# 9000 Series Kernel 12.X

## Industrial Managed Ethernet Switch

## (POE / Layer2 / Layer3)

# GUI Manual

# V1.4

# Table of Content

# Management

The switch can be controlled via a built-in web server which supports Internet Explorer (Internet Explorer 5.0 or above versions) and other Web browsers such as Chrome. Therefore, you can manage and configure the switch easily and remotely. You can also upgrade firmware via a web browser. The Web management function not only reduces network bandwidth consumption, but also enhances access speed and provides a user-friendly viewing screen.

By default, IE5.0 or later version do not allow Java applets to open sockets. You need to modify the browser setting separately in order to enable Java applets for network ports.

## Preparing for Web Management

You can access the management page of the switch via the following default values:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

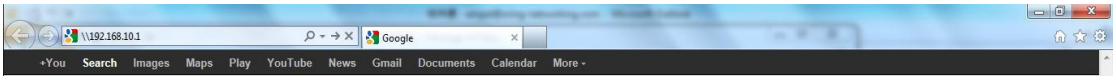
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

## System Login

1. Launch the Internet Explorer.
2. Type http:// and the IP address of the switch. Press **Enter**.




3. A login screen appears.
4. Type in the username and password. The default username and password is **admin**.
5. Click **Enter** or **OK** button, the management Web page appears.

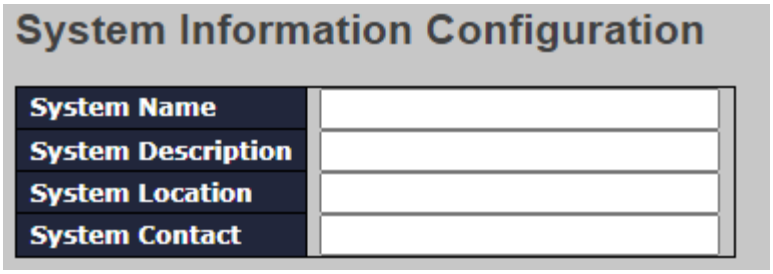

After logging in, you can see the information of the switch as below.

# 1.1 Basic Settings

Basic Settings allow you to configure the basic functions of the switch.

## 1.1.1 System Information

This page shows the general information of the switch.




.

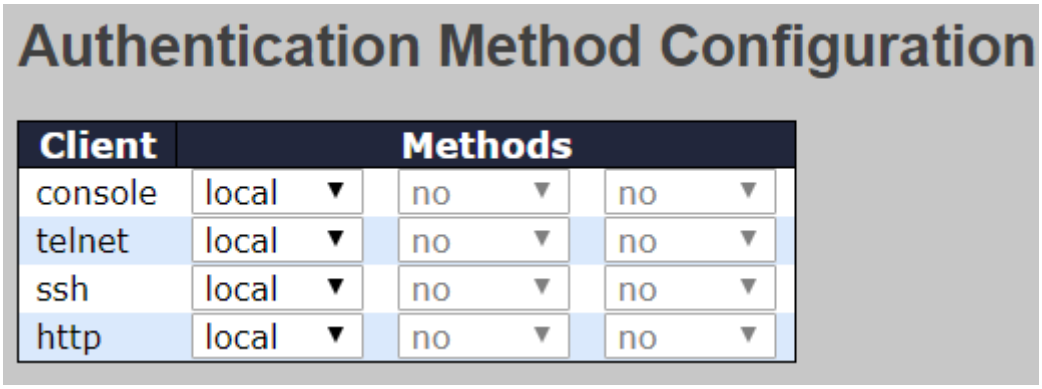
| Label | Description |
|---|---|
| **System Name** | An administratively assigned name for the managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string consisting of alphabets (A-Z, a-z), digits (0-9), and minus sign (-). Space is not allowed to be part of the 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 Description** | Description of the device |
| **System Location** | The physical location of the node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed. |
| **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 only ASCII characters from 32 to 126 are allowed. |
| **Save** | Click to save changes. |
| **Reset** | Click to undo any changes made locally and revert to previously saved values. |

## 1.1.2 Auth Method

### Authentication Method Configuration

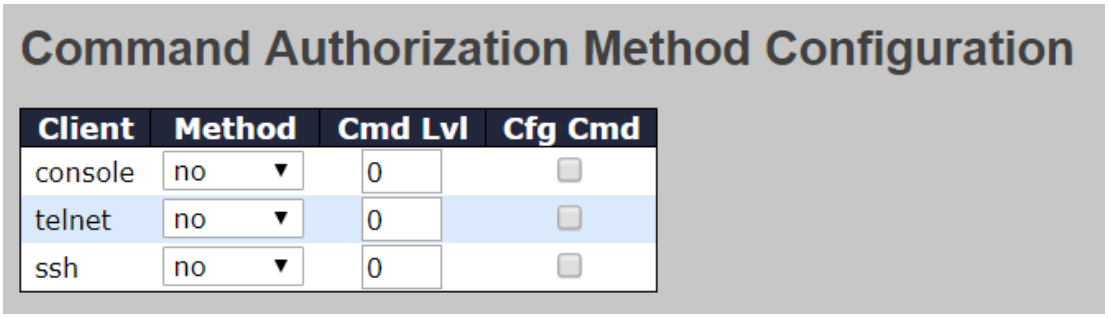
The authentication section allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.




| Label | Description |
|---|---|
| **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. |

## Command Authorization Method Configuration

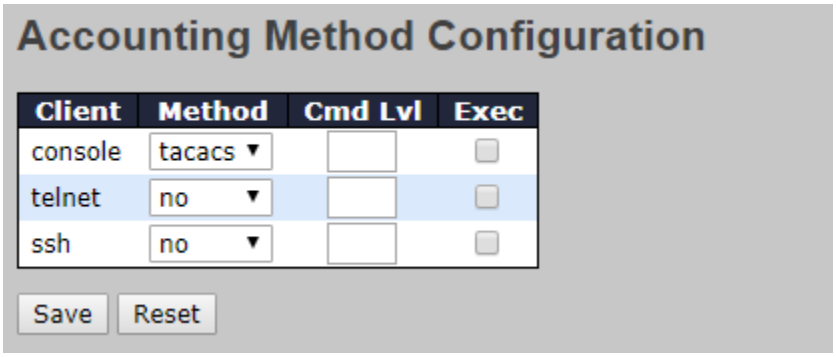
The command authorization section allows you to limit the CLI commands available to a user.




| Label | Description |
|---|---|
| **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. |

## Accounting Method Configuration

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



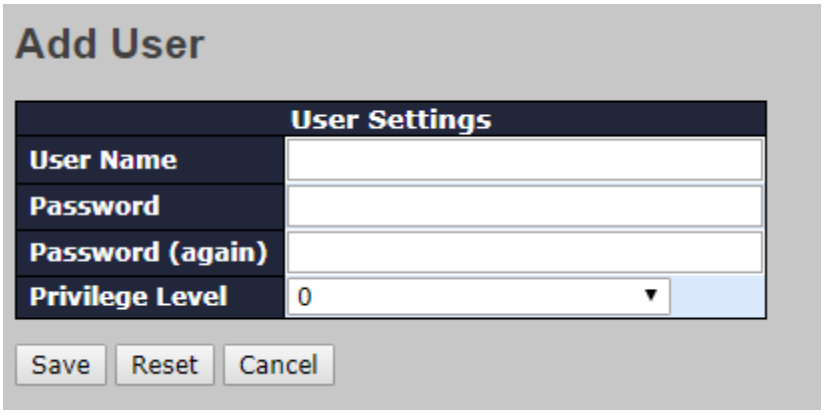

| Label | Description |
|---|---|
| **Client** | The management client for which the configuration below applies. |
| **Methods** | Method can be set to one of the following values:<br>· **no**: Accounting is disabled.<br>· **tacacs**: Use remote TACACS+ server(s) for accounting. |
| **Cmd Lvl** | Enable accounting of all commands with a privilege level higher than or equal to this level. Valid values are in the range of 0 to 15. |

| | |
|---|---|
| | Leave the field empty to disable command accounting. |
| **Exec** | Enable exec (login) accounting. |

### 1.1.3 Users

#### Configuration

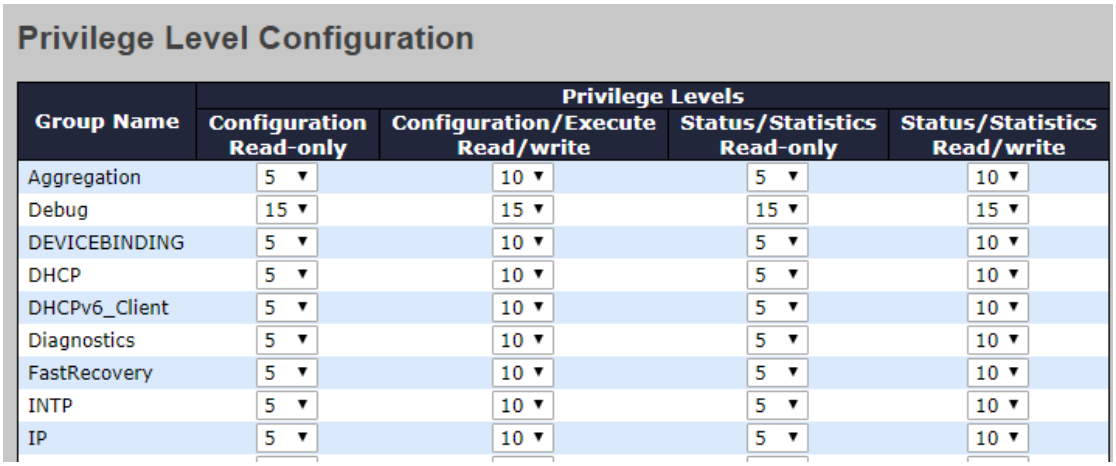
This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.




| Label | 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 can be letters, numbers and underscores. |
| **Password** | The password of the user. The allowed string length is 0 to 31. Any printable characters including space are 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 other values need to refer to each group privilege level. User's privilege should be the same or greater than the group privilege level to have the access of that group. By default, the group privilege level of 5 has the read-only access and the privilege level of 10 has the read-write access. System maintenance (software upload, factory defaults and etc.) requires the user privilege level of 15. Generally, the privilege level of 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account. |

#### Privilege Levels

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 |
| Debug | 15 | 15 | 15 | 15 |
| DEVICEBINDING | 5 | 10 | 5 | 10 |
| DHCP | 5 | 10 | 5 | 10 |
| DHCPv6_Client | 5 | 10 | 5 | 10 |
| Diagnostics | 5 | 10 | 5 | 10 |
| FastRecovery | 5 | 10 | 5 | 10 |
| INTP | 5 | 10 | 5 | 10 |
| IP | 5 | 10 | 5 | 10 |

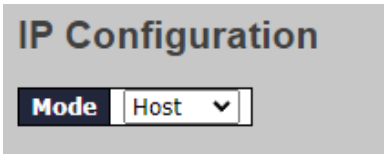
| Label | Description |
|---|---|
| **Group Name** | The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details: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

## 1.1.4 IP Settings

This page allows you to configure IP information for the switch. You can configure the settings of the device operating in host or router mode.

### IP Configuration (only for Layer 3 Model)

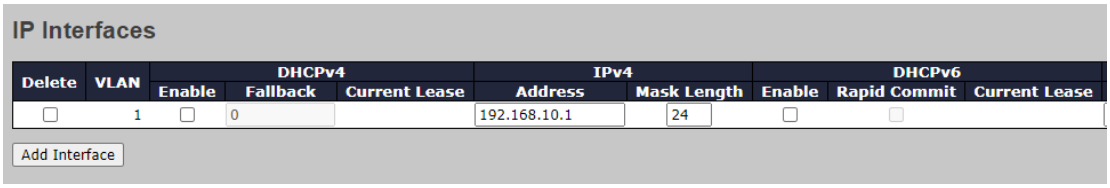
the item provides user setting switch mode .




| Label | Description |
|---|---|
| **Mode** | Configure whether the IP stack should act as a Host or a Router.<br>***In Host mode*** = IP traffic between interfaces will not be routed.<br>***In Router mode*** = traffic is routed between all interfaces. |

### IP Interface

This page provides an overview of the privilege levels.



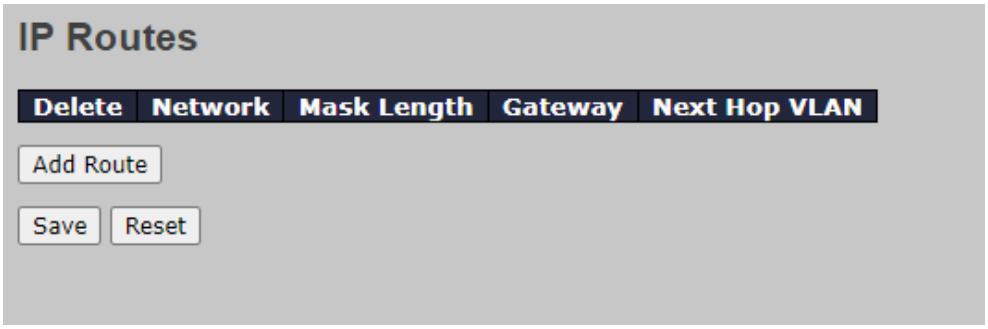

| Label | Description |
|---|---|
| **VLAN** | The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface. |
| **IPv4 DHCP Enabled** | Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup. |
| **IPv4 DHCP Fallback Timeout** | The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds. |

| | |
|---|---|
| **IPv4 DHCP Current Lease** | For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server. |
| **IPv4 Address** | The IPv4 address of the interface in dotted decimal notation.<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 an 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. An 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>This 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 an IPv6 address.<br>This 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. |
| **Gateway** | Input gateway address . |
| **Add Interface (only for Layer 3 model)** | Click to add a new IP interface. A maximum of 128 interfaces is supported. |

## IP Routes (only for Layer 3 Model)

This page provides user setting static route entry

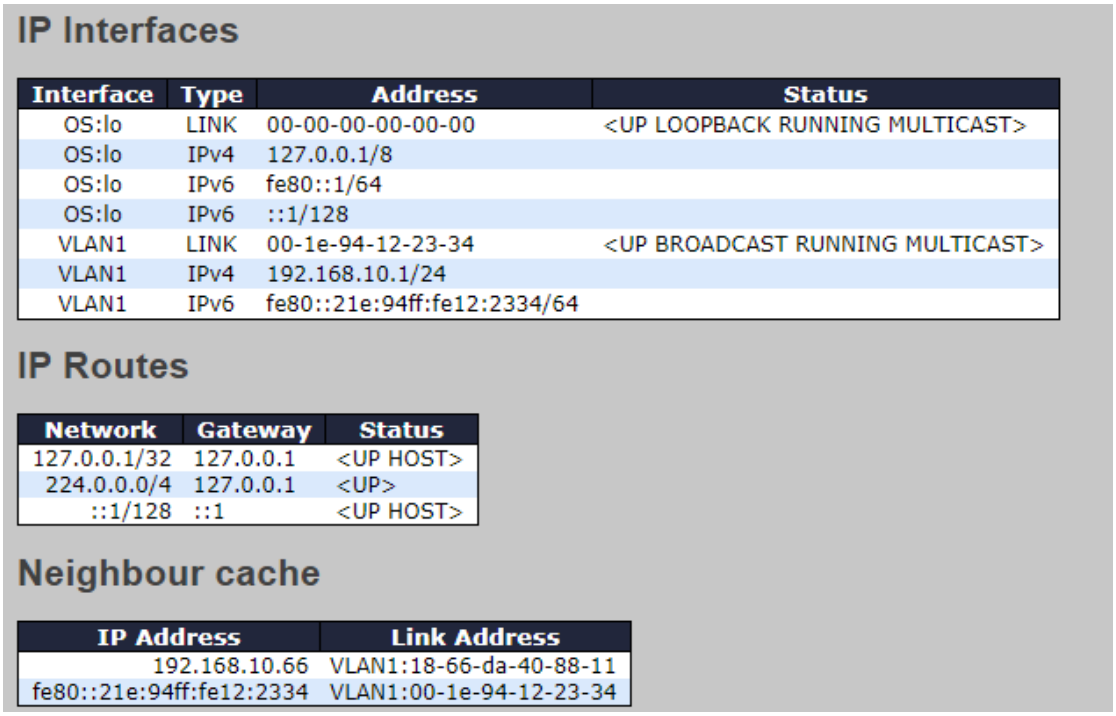



| Label | Description |
|---|---|
| **Delete** | Select this option to delete an existing IP route. |
| **Network** | The destination IP network or host address of this route. Valid format is dotted decimal notationor a valid IPv6 notation. A default route can use the value 0.0.0.0or IPv6 :: notation. |
| **Mask Length** | The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything). |
| **Gateway** | The IP address of the IP gateway. Valid format is dotted decimal |

| | |
|---|---|
| | notationor a valid IPv6 notation. Gateway and Network must be of the same type. |
| **Next Hop VLAN (only for IPv6)** | The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.<br>The given VID ranges from 1 to 4095 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. |

## 1.1.5 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.



IP Interfaces

| Interface | Type | Address | Status |
|---|---|---|---|
| OS:lo | LINK | 00-00-00-00-00-00 | <UP LOOPBACK RUNNING MULTICAST> |
| OS:lo | IPv4 | 127.0.0.1/8 | |
| OS:lo | IPv6 | fe80::1/64 | |
| OS:lo | IPv6 | ::1/128 | |
| VLAN1 | LINK | 00-1e-94-12-23-34 | <UP BROADCAST RUNNING MULTICAST> |
| VLAN1 | IPv4 | 192.168.10.1/24 | |
| VLAN1 | IPv6 | fe80::21e:94ff:fe12:2334/64 | |

IP Routes

| Network | Gateway | Status |
|---|---|---|
| 127.0.0.1/32 | 127.0.0.1 | <UP HOST> |
| 224.0.0.0/4 | 127.0.0.1 | <UP> |
| ::1/128 | ::1 | <UP HOST> |

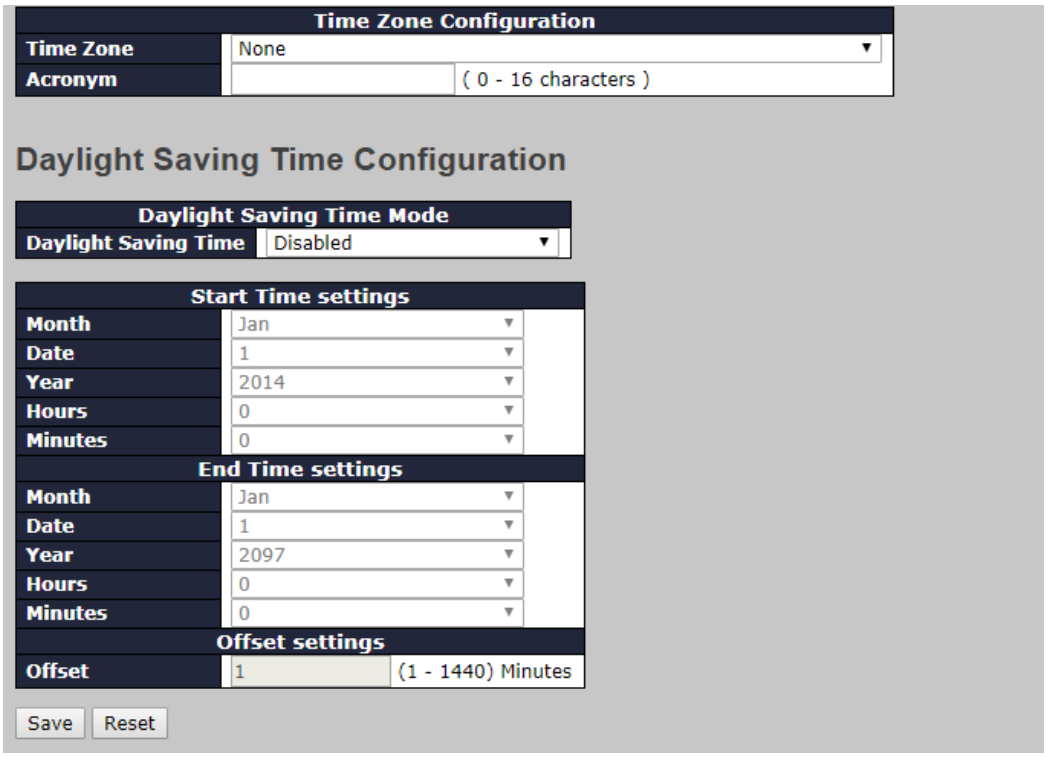
Neighbour cache

| IP Address | Link Address |
|---|---|
| 192.168.10.66 | VLAN1:18-66-da-40-88-11 |
| fe80::21e:94ff:fe12:2334 | VLAN1:00-1e-94-12-23-34 |

| Label | Description |
|---|---|
| **IP Interface** | |
| **Interface** | The name of the interface. |
| **Type** | The address type of the entry. This may be LINK or IPv4. |
| **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. |

## 1.1.6 Daylight Saving Time




| Label | Description |
|---|---|
| **Time Zone Configuration** | **Time Zone**: Set the switch location time zone. The following table lists the different location time zone for your reference. **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 alpha-numeric characters and can contain '-', '_' or '.'). |
| **Daylight Saving Time Configuration** | **Daylight Saving Time Mode**: Enable or disable daylight saving time function. This is used to set the clock forward or backward according to the configurations set below for a |

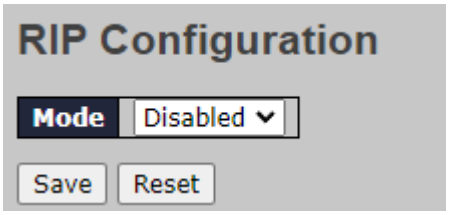
| | |
|---|---|
| | defined daylight saving time duration. Select **'Disable'** to disable the daylight saving time configuration. Select **'Recurring'** and configure the Daylight Saving Time duration to repeat the configuration every year. Select '**Non-Recurring**' and configure the daylight saving time duration for single time configuration. ( Default : Disabled ).<br>Start Time Settings: Set up the start time of the daylight saving time period.<br>End Time Settings: Set up the ending time of the daylight saving time period.<br>Offset Settings: Set up the offset time. |

| Local Time Zone | Conversion from UTC | Time at 12:00 UTC |
|---|---|---|
| November Time Zone | - 1 hour | 11 am |
| Oscar Time Zone | -2 hours | 10 am |
| ADT - Atlantic Daylight | -3 hours | 9 am |
| AST - Atlantic Standard<br>EDT - Eastern Daylight | -4 hours | 8 am |
| EST - Eastern Standard<br>CDT - Central Daylight | -5 hours | 7 am |
| CST - Central Standard<br>MDT - Mountain Daylight | -6 hours | 6 am |
| MST - Mountain Standard<br>PDT - Pacific Daylight | -7 hours | 5 am |
| PST - Pacific Standard<br>ADT - Alaskan Daylight | -8 hours | 4 am |
| ALA - Alaskan Standard | -9 hours | 3 am |
| HAW - Hawaiian Standard | -10 hours | 2 am |
| Nome, Alaska | -11 hours | 1 am |

| | | |
|---|---|---|
| CET - Central European<br>FWT - French Winter<br>MET - Middle European<br>MEWT - Middle European Winter<br>SWT - Swedish Winter | +1 hour | 1 pm |
| EET - Eastern European, USSR Zone 1 | +2 hours | 2 pm |
| BT - Baghdad, USSR Zone 2 | +3 hours | 3 pm |
| ZP4 - USSR Zone 3 | +4 hours | 4 pm |
| ZP5 - USSR Zone 4 | +5 hours | 5 pm |
| ZP6 - USSR Zone 5 | +6 hours | 6 pm |
| WAST - West Australian Standard | +7 hours | 7 pm |
| CCT - China Coast, USSR Zone 7 | +8 hours | 8 pm |
| JST - Japan Standard, USSR Zone 8 | +9 hours | 9 pm |
| EAST - East Australian Standard<br>GST<br>Guam Standard, USSR Zone 9 | +10 hours | 10 pm |
| IDLE - International Date Line<br>NZST - New Zealand Standard<br>NZT - New Zealand | +12 hours | Midnight |

## 1.1.7 RIP (only for Layer 3 Model)

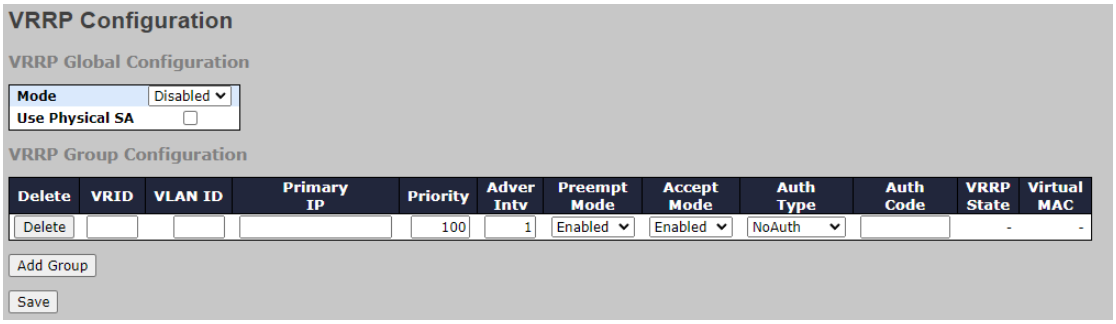
Configure RIP on this page.




| Label | Description |
|---|---|
| **Mode** | Indicates the RIP mode operation. Possible modes are:<br>Enabled: Enable RIP mode operation.<br>Disabled: Disable RIP mode operation. |

## 1.1.8 VRRP (only for Layer 3 Model)

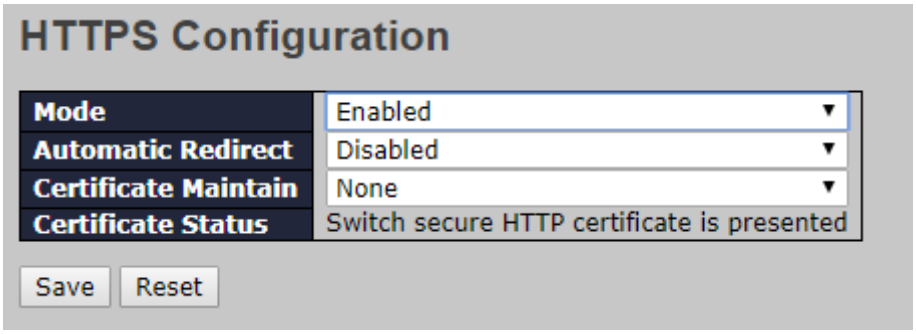
Configure VRRP on this page.




| Label | Description |
|---|---|
| **VRRP Global Configuration** | |
| **Mode** | Enable / Disable VRRP Function |
| **Use Physical SA** | Use physical source MAC address for ARP reply. |
| **VRRP Group Configuration** | |
| **Delete** | Delete the group |
| **VRID** | Virtual Router ID, from 1 to 254 |
| **VLAN ID** | VLAN interface ID |
| **Primary IP** | Primary interface for a VRRP Group |
| **Priority** | Priority, from 1 to 254 |
| **Adver Intv** | Advertisement Interval (0 - 10) |
| **Accept Mode** | Preemption of a backup VRRP device acting as a master device is allowed when another backup device has a higher priority |
| **Auth Mode** | Enabling accept mode allows a backup VRRP device to respond to ping, if the backup device becomes the master VRRP device |
| **Auth Type** | A simple text password can be used for interface authentication in a network |
| **Auth Code** | Password, 8 characters |
| **VRRP State** | Show the role of group |
| **Virtual MAC** | If device is master, this shows the Virtual MAC of group |

## 1.1.9 HTTPS

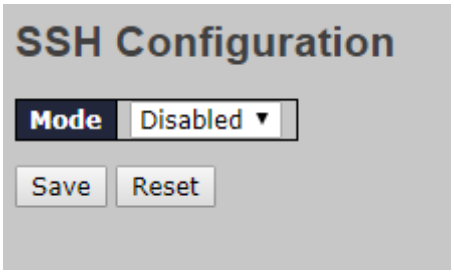
You can configure the HTTPS mode in this page.




| Label | Description |
|---|---|
| **Mode** | Enables or disables HTTPS mode. |
| **Automatic Redirect** | Enables or disables automatic redirect function. It is only significant when HTTPS mode is enabled. When the redirect mode is enabled, the HTTP connection will be redirected to HTTPS connection automatically. Notice that the browser may not allow redirection due to security considerations unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually for this case. |
| **Certificate Maintain** | The operation of certificate maintenance including:<br>**None**: No operation.<br>**Delete**: Delete the current certificate.<br>**Upload**: Upload a certificate PEM file through a Web browser or URL.<br>**Generate**: Generate a new self-signed RSA certificate. |
| **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**. |

## 1.1.10 SSH

You can configure the SSH mode in this page.




| Label | Description |
|---|---|
| **Mode** | Enable or disable SSH. |
| **Save** | Click to save changes |
| **Reset** | Click to undo any changes made locally and revert to previously saved values. |

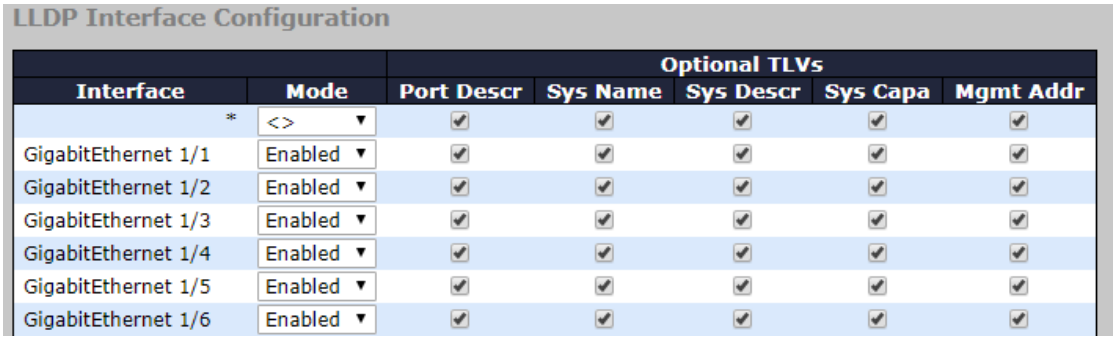
## 1.1.11 LLDP

### LLDP Configurations

This page allows you to examine and configure current LLDP port settings.


| Label | Description |
|---|---|
| **Tx Interval** | The switch periodically transmits LLDP frames to its neighbors to update the network discovery information. The interval between each LLDP frame is determined by the Tx Interval value which must be between 5 - 32768 seconds. |
| **Tx Hold** | Each LLDP frame contains information about how long time the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values must be between 2 - 10 times. |
| **Tx Delay** | When a setting 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 must be between 1 - 8192 seconds. |
| **Tx Reinit** | When an interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values must be between 1 - 10 seconds. |




| Label | Description |
|---|---|
| **Interface** | The switch interface name of the logical LLDP interface. |
| **Mode** | Select a LLDP mode from the drop down list.<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. |
| **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. |

## LLDP Neighbor Information

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

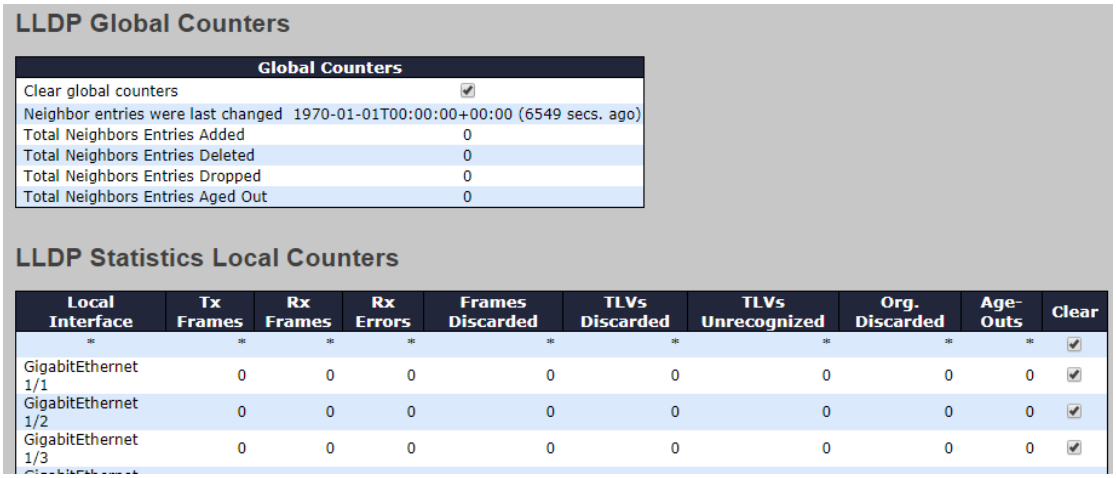
Auto-refresh ☐ Refresh

| Local Port | Chassis ID | Remote Port ID | System Name | Port Description | System Capabilities | Management Address |
|---|---|---|---|---|---|---|
| Port 8 | 00-1E-94-12-45-78 | 7 | IGS-9812GP | Port #7 | Bridge(+) | 192.168.10.14 (IPv4) |

| Label | Description |
|---|---|
| **Local Port** | The port that you use to transmits and receives LLDP frames. |
| **Chassis ID** | The identification number of the neighbor sending out the LLDP frames. |
| **Remote Port ID** | The identification of the neighbor port |
| **System Name** | The name advertised by the neighbor. |
| **Port Description** | The description of the port advertised by the neighbor. |
| **System Capabilities** | Description of the neighbor's capabilities. The capabilities include:<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, a (+) will be displayed. If the capability is disabled, a (-) will be displayed. |
| **Management Address** | The neighbor's address which can be used to help network management. This may contain the neighbor's IP address. |
| **Refresh** | Click to refresh the page immediately. |
| **Auto-refresh** | Check to enable an automatic refresh of the page at regular intervals. |

## Port Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters will apply settings to the whole switch stack, while local counters will apply settings to specified switches.




## Global Counters

| Label | Description |
|---|---|
| **Clear Global Counters** | If checked the global counters are cleared when **Clear** is pressed. |
| **Neighbor entries were last changed** | 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 full entry table |
| **Total Neighbors Entries Aged Out** | Shows the number of entries deleted due to expired time-to-live |

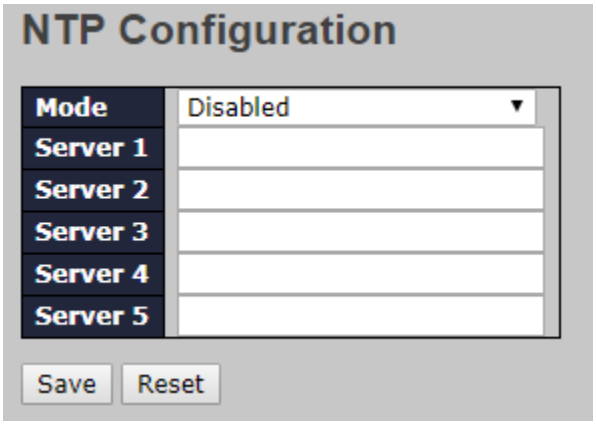
## Local Counters

| Label | Description |
|---|---|
| **Local Port** | The port that receives or transmits LLDP frames |
| **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 errors |
| **Frames Discarded** | If a port receives an LLDP frame, and the switch's internal table is full, the LLDP frame will be counted and discarded. This situation is known as "too many neighbors" in the LLDP standard. LLDP frames require a new entry in the table if Chassis ID or Remote Port ID is not included in the table. Entries are removed from the |

| | |
|---|---|
| | table when a given port links 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 (Type Length Value). If a TLV is malformed, it will be counted and discarded. |
| **TLVs Unrecognized** | The number of well-formed TLVs, but with an unknown type value |
| **Org. Discarded** | The number of organizationally TLVs received |
| **Age-Outs** | Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received during the age-out time, the LLDP information will be removed, and the value of the age-out counter will be incremented. |
| **Clear** | If checked the counters for the specific interface are cleared when **Clear** is pressed. |

## 1.1.12 NTP

The function allows you to specify the Network Time Protocol (NTP) servers to query for the current time to maintain an accurate time on the switch, ensuring the system log record meaningful dates and times for event entries. With NTP, the switch can set its internal clock periodically according to an NTP time server. Otherwise, the switch will only record the time from the factory default set at the last bootup. When the NTP client is enabled, the switch regularly sends a request for a time update to a configured time server. A maximum of five time servers are supported. The switch will attempt to poll each server in the configured sequence.

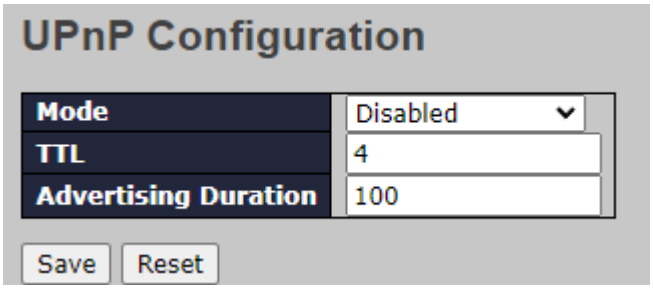



| Label | Description |
|---|---|
| **Mode** | Select a NTP mode from the drop down list. |
| **Server** | Sets the IP address for up to five time servers. The switch will update the time from the servers, starting from the first to the |

| | |
|---|---|
| | fifth in sequence if any of them fails. The polling interval is fixed at 15 minutes. |

### 1.1.13 UPnP

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

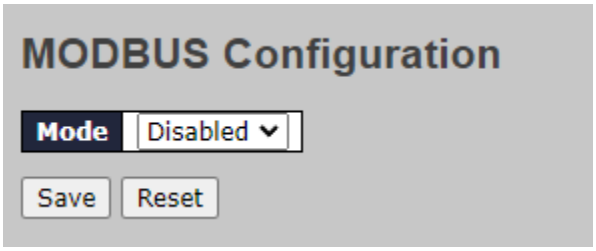



| Label | Description |
|---|---|
| **Mode** | Indicates the UPnP operation mode. Possible modes are:<br><br>Enabled: Enable UPnP mode operation.<br><br>Disabled: Disable UPnP mode operation.<br><br>When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled. |
| **TTL** | The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255. |
| **Advertising Duration** | The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid |

| | |
|---|---|
| | values are in the range 100 to 86400. |

### 1.1.14 Modus TCP

Support Modbus TCP. (About Modbus please reference http://www.modbus.org/)

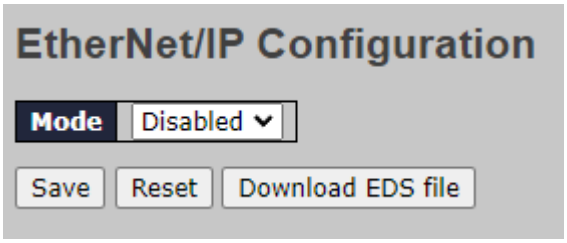



The following table describes the labels in this screen.

| Label | Description |
|---|---|
| **Mode** | Enable or Disalble Modbus TCP function |

### 1.1.15 Ethernet/IP

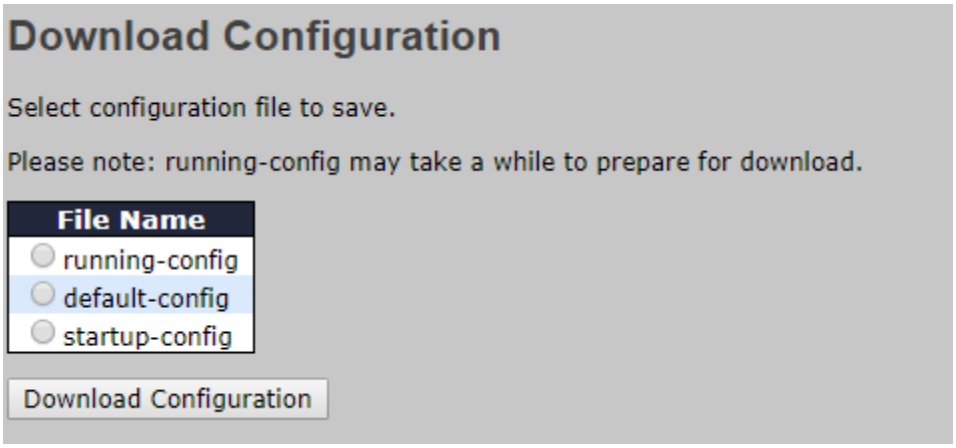
EtherNet/IP is an industrial network protocol that adapts the Common Industrial Protocol to standard Ethernet.[1] EtherNet/IP is one of the leading industrial protocols in the United States and is widely used in a range of industries including factory, hybrid and process.

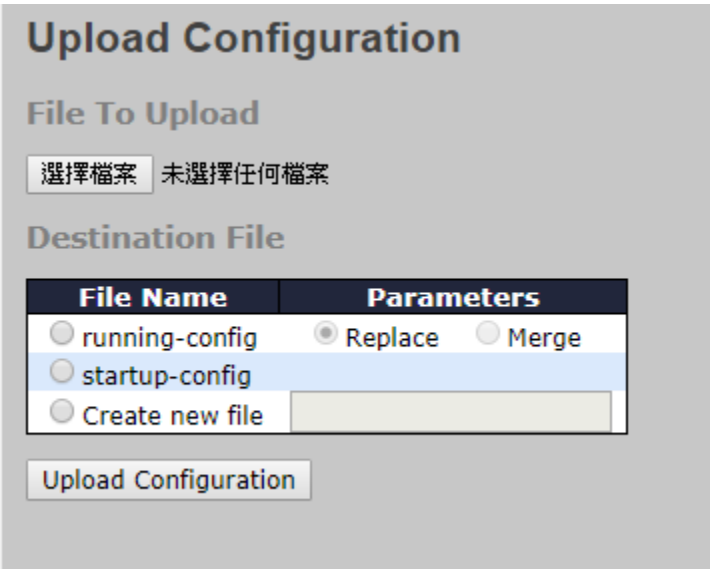



| Label | Description |
|---|---|
| **Mode** | Indicates the EtherNet/IP mode operation. Possible modes are:<br><br>Enabled: Enable EtherNet/IP mode operation.<br><br>Disabled: Disable EtherNet/IP mode operation. |

### 1.1.16 Backup/Restore Configurations

You can save/view or load switch configurations.




### 1.1.17 Firmware Update

This page allows you to update the firmware of the switch.

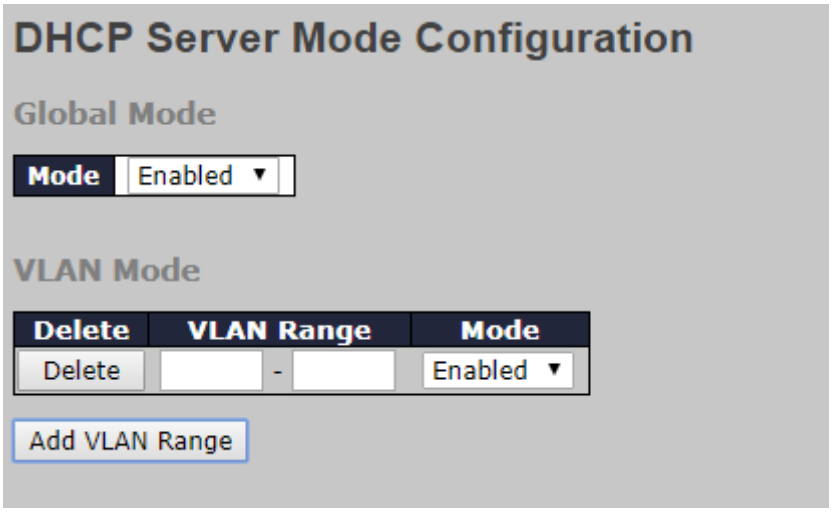

## 1.2 DHCP

### 1.2.1 DHCP Server

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

and per VLAN.and per VLAN.

## Mode

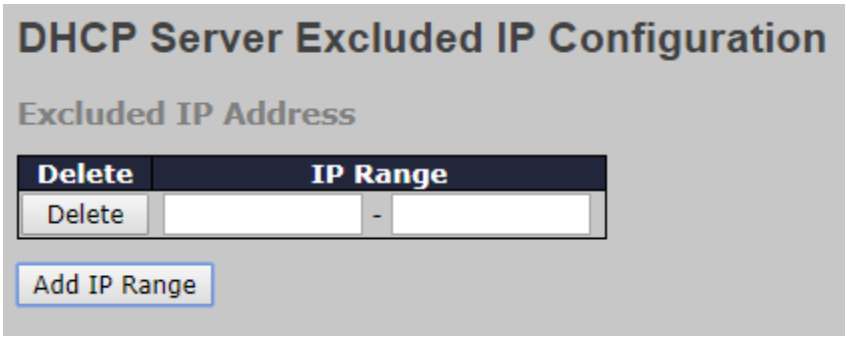



| Label | Description |
|---|---|
| **Global Mode** | |
| **Mode** | Configure the operation mode per system. Possible modes are:<br>**Enabled**: Enable DHCP server per system.<br>**Disabled**: Disable DHCP server pre system. |
| **VLAN Mode** | |
| **VLAN Range** | Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both.<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** | Indicate the operation mode per VLAN. Possible modes are:<br>**Enabled:** Enable DHCP server per VLAN. |

| | |
|---|---|
| | **Disabled**: Disable DHCP server pre VLAN. |

## Excluded IP

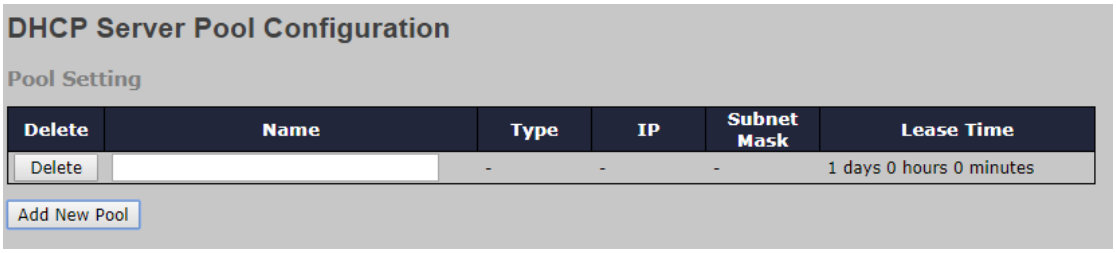
This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client




| Label | 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. |

## Pool

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

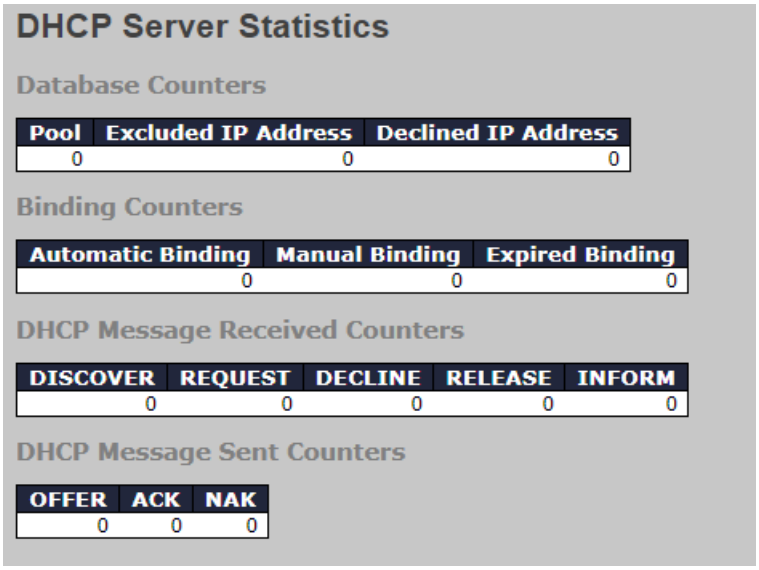



| Label | Description |
|---|---|
| Name | Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page. |
| **Type** | Display which type of the pool is.<br>**Network**: 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. 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. |
| **Lease Time** | Display lease time of the pool. |

## Statistics

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

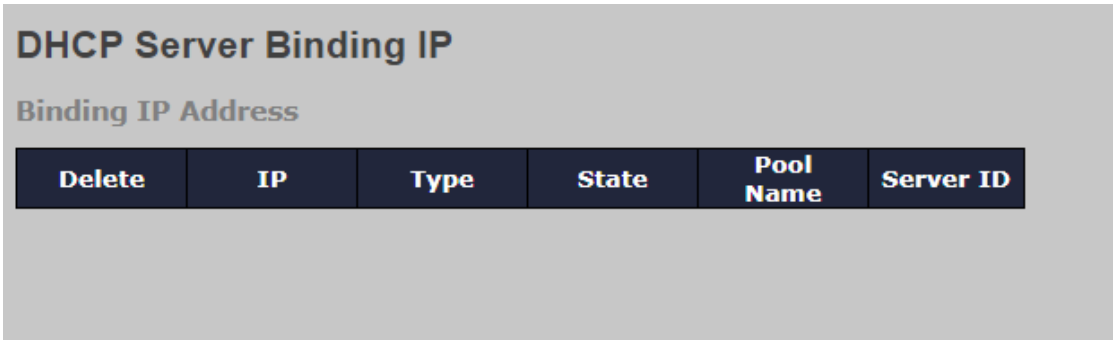



| Label | Description |
|---|---|
| **Database Counters** | |
| **Pool** | Number of pools. |
| **Excluded IP Address** | Number of excluded IP address ranges. |
| **Declined IP Address** | Number of declined IP addresses. |
| **Binding Counters** | |
| **Automatic Binding** | Number of bindings with 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. |

## Binding

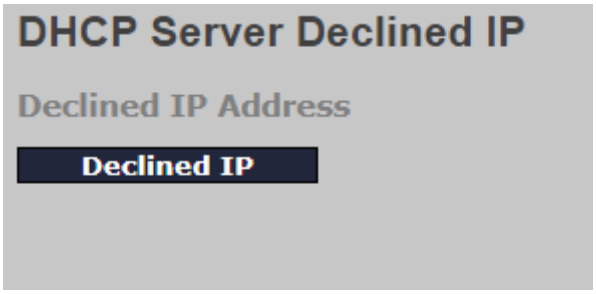
This page displays bindings generated for DHCP clients.




| Label | 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 ID** | Server IP address to service the binding. |

## Declined IP

Display IP addresses declined by DHCP clients.

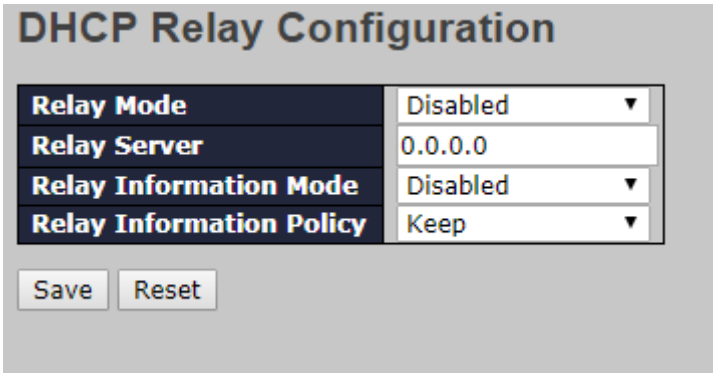



| Label | Description |
|---|---|

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

## 1.2.2 DHCP Relay

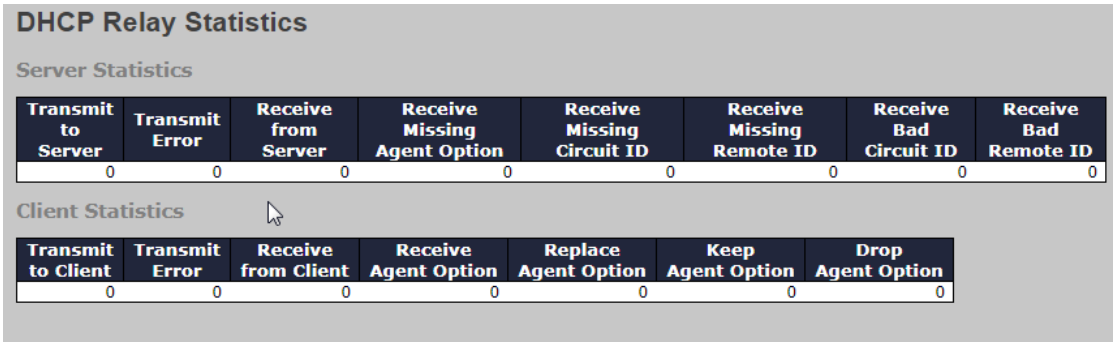
DHCP relay is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain. You can configure the function in this page.




| Label | Description |
|---|---|
| **Relay Mode** | Indicates the existing DHCP relay mode. The modes include:<br>**Enabled**: activate DHCP relay. When DHCP relay is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain to prevent the DHCP broadcast message from flooding for security considerations.<br>**Disabled**: disable DHCP relay |
| **Relay Server** | Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain. |
| **Relay Information Mode** | Indicates the existing DHCP relay information mode. The format of DHCP option 82 circuit ID format is "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, and the fifth and sixth characters are the module ID. In stand-alone devices, the module ID always equals to 0; in stacked devices, it means switch ID. The last two characters are the port number. For example, "00030108" means the DHCP message received form VLAN ID 3, switch ID 1, and port No. 8. The option 82 remote ID value equals to the switch MAC address.<br>The modes include:<br>**Enabled**: activate DHCP relay information. When DHCP relay information is enabled, the agent inserts specific information |

| | |
|---|---|
| | (option 82) into a DHCP message when forwarding to a DHCP server and removes it from a DHCP message when transferring to a DHCP client. It only works when DHCP relay mode is enabled.<br>**Disabled**: disable DHCP relay information |
| **Relay Information Policy** | Indicates the policies to be enforced when receiving DHCP relay information. When DHCP relay information mode is enabled, if the agent receives a DHCP message that already contains relay agent information, it will enforce the policy. The Replace option is invalid when relay information mode is disabled. The policies includes:<br>**Replace**: replace the original relay information when a DHCP message containing the information is received.<br>**Keep**: keep the original relay information when a DHCP message containing the information is received.<br>**Drop**: drop the package when a DHCP message containing the information is received. |

The relay statistics shows the information of relayed packets of the switch.



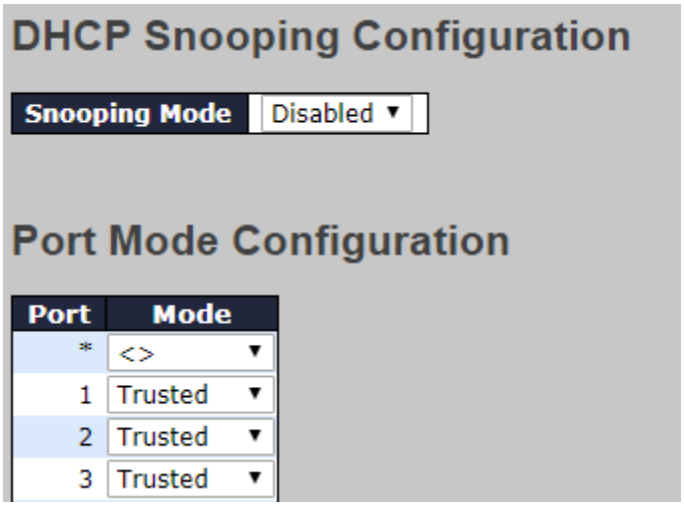

| Label | Description |
|---|---|
| **Transmit to Sever** | The number of packets relayed from the client to the server |
| **Transmit Error** | The number of packets with errors when being sent to clients |
| **Receive from Server** | The number of packets received from the server |
| **Receive Missing Agent Option** | The number of packets received without agent information |
| **Receive Missing Circuit ID** | The number of packets received with Circuit ID |
| **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 do not match the known circuit ID |
| **Receive Bad Remote ID** | The number of packets whose Remote ID do not match the |

| | |
|---|---|
| | known Remote ID |
| **Transmit to Client** | The number of packets relayed from the server to the client |
| **Transmit Error** | The number of packets with errors when being sent to servers |
| **Receive from Client** | The number of packets received from the server |
| **Receive Agent Option** | The number of received packets containing relay agent information |
| **Replace Agent Option** | The number of packets replaced when received messages contain relay agent information. |
| **Keep Agent Option** | The number of packets whose relay agent information is retained |
| **Drop Agent Option** | The number of packets dropped when received messages contain relay agent information. |

## 1.2.3 DHCP Snooping

### Snooping

Configure DHCP Snooping on this page.

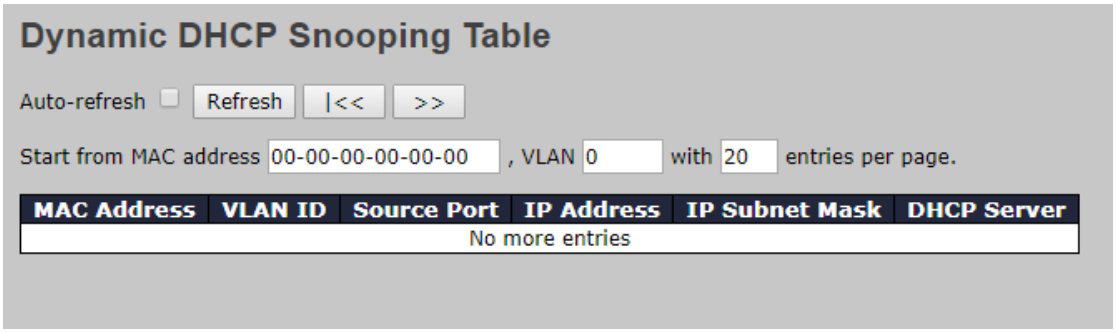



| Label | Description |
|---|---|
| **Snooping Mode** | Indicates the DHCP snooping mode operation. Possible modes are:<br>**Enabled**: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.<br>**Disabled**: Disable DHCP snooping mode operation. |
| **Port Mode Configuration** | Indicates the DHCP snooping port mode. Possible port modes are: |

| | |
|---|---|
| | **Trusted**: Configures the port as trusted source of the DHCP messages.<br>**Untrusted**: Configures the port as untrusted source of the DHCP messages. |

## Snooping Table

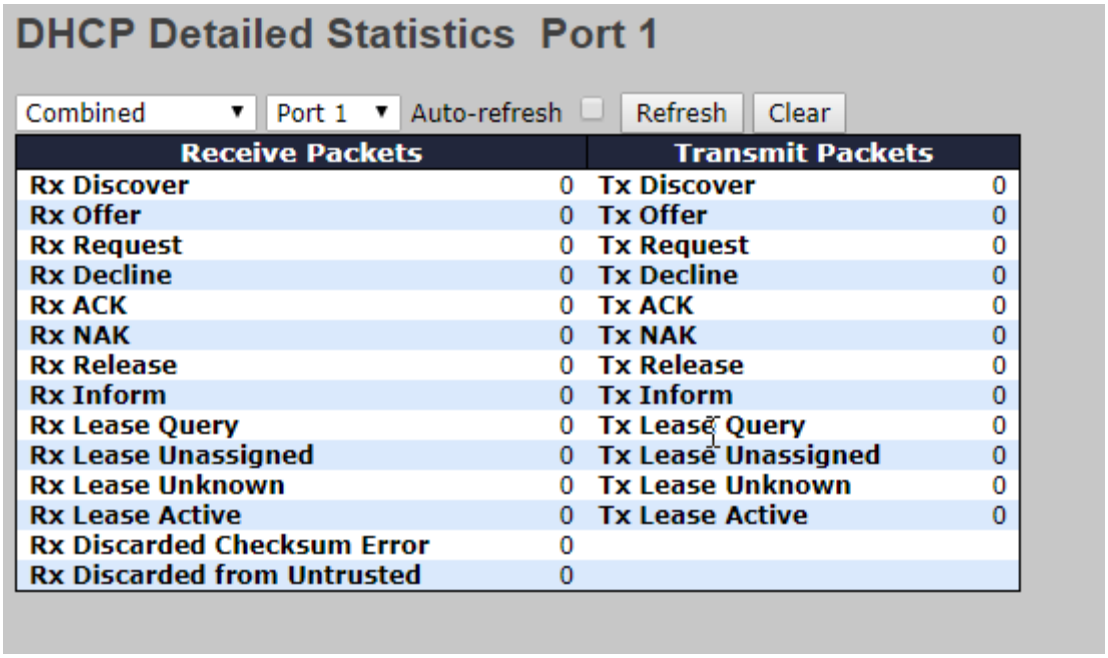
This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.




| Label | 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. |

## 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.




| Label | 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 Decline** | The number of decline (option 53 with value 4) packets received and transmitted. |
| **Rx and Tx ACK** | The number of ACK (option 53 with value 5) packets received and transmitted. |
| **Rx and Tx NAK** | The number of NAK (option 53 with value 6) packets received and transmitted. |
| **Rx and Tx Release** | The number of release (option 53 with value 7) packets received and transmitted. |
| **Rx and Tx Inform** | The number of inform (option 53 with value 8) packets received and transmitted. |
| **Rx and Tx Lease Query** | The number of lease query (option 53 with value 10) packets received and transmitted. |
| **Rx and Tx Lease Unassigned** | The number of lease unassigned (option 53 with value 11) packets received and transmitted. |
| **Rx and Tx Lease** | The number of lease unknown (option 53 with value 12) packets |

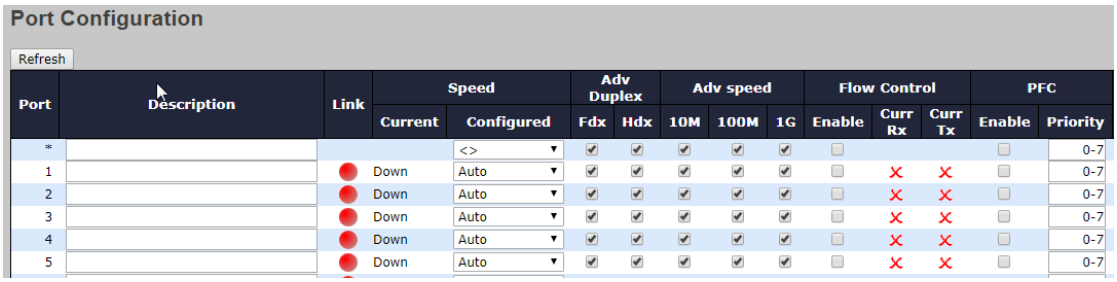
| | |
|---|---|
| **Unknown** | received and transmitted. |
| **Rx and Tx Lease Active** | The number of lease active (option 53 with value 13) packets received and transmitted. |
| **Rx Discarded checksum error** | The number of discard packet that IP/UDP checksum is error. |
| **Rx Discarded from Untrusted** | The number of discarded packet that are coming from untrusted port. |

# 1.3 Port Setting

Port Setting allows you to manage individual ports of the switch, including traffic, power, and trunks.

## 1.3.1 Port Control

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




| Label | Description |
|---|---|
| **Port** | This is the logical port number for this row. |
| **Description** | The description of the port. It is an ASCII string no longer than 256 characters. |
| **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 are 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 |

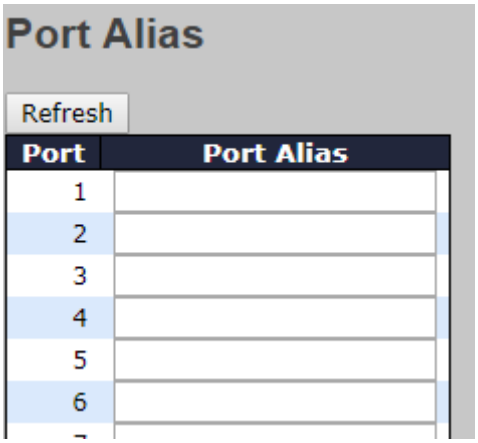
| | |
|---|---|
| | duplex mode.<br>**10Mbps FDX** - Forces the cu port in 10Mbps full duplex mode.<br>**100Mbps HDX** - Forces the cu port in 100Mbps half duplex mode.<br>**100Mbps FDX** - Forces the cu port in 100Mbps full duplex mode.<br>**1Gbps FDX** - Forces the port in 1Gbps full duplex<br>**2.5Gbps FDX** - Forces the Serdes port in 2.5Gbps full duplex mode.<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 have Cu port preferred.<br>Ports in AMS mode with 1000-X speed have fiber port preferred.<br>Ports in AMS mode with 100-FX speed have 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 Hdxto** 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**) 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 doesn't 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 Flow control 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 doesn't 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 |

## 1.3.2 Port Alias

This page is available to let users add descriptions on the port.




| Label | Description |
|---|---|
| **Port** | This is the logical port number for this row. |
| **Port Alias** | Add descriptions on the port. |

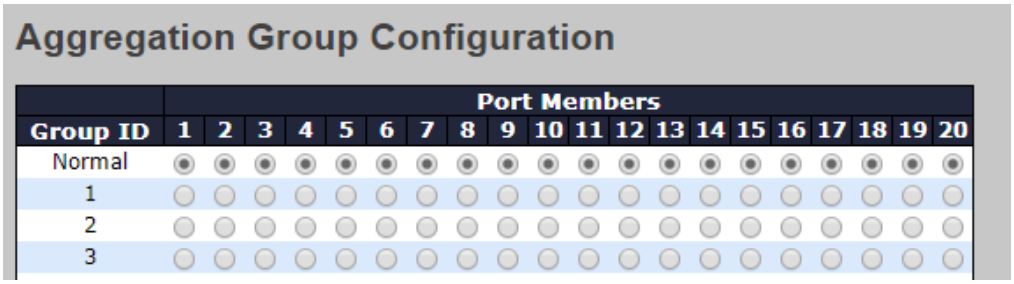
## 1.3.3 Port Trunk

A port trunk is a group of ports that have been grouped together to function as one logical path. This method provides an economical way for you to increase the bandwidth between the switch and another networking device. In addition, it is useful when a single physical link between the devices is insufficient to handle the traffic load. This page allows you to configure the aggregation hash mode and the aggregation group.

### Configurations


| Label | Description |
|---|---|

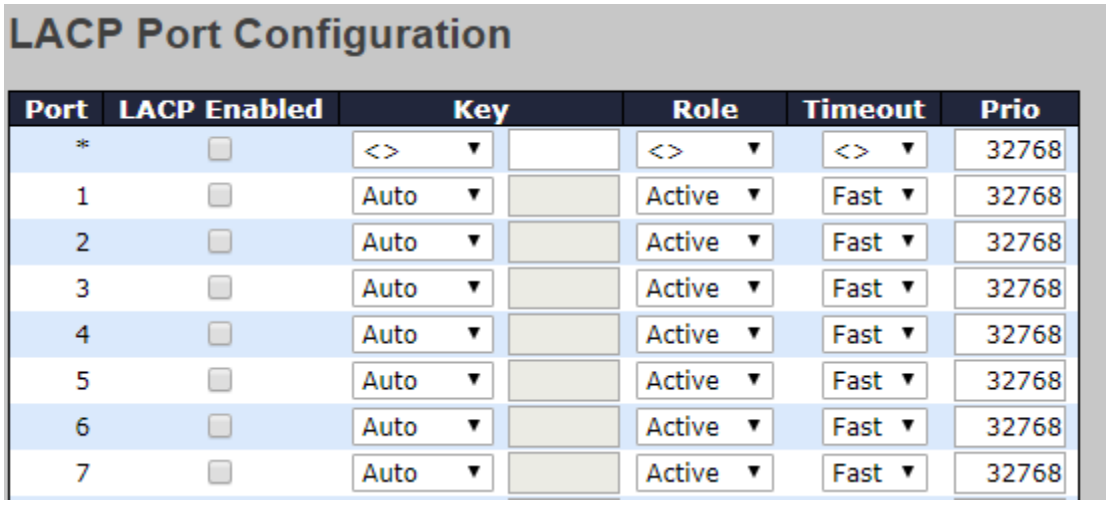
| | |
|---|---|
| **Source MAC Address** | Calculates the destination port of the frame. You can check this box to enable the source MAC address, or uncheck to disable. By default, **Source MAC Address** is enabled. |
| **Destination MAC Address** | Calculates the destination port of the frame. You can check this box to enable the destination MAC address, or uncheck to disable. By default, **Destination MAC Address** is disabled. |
| **IP Address** | Calculates the destination port of the frame. You can check this box to enable the IP address, or uncheck to disable. By default, **IP Address** is enabled. |
| **TCP/UDP Port Number** | Calculates the destination port of the frame. You can check this box to enable the TCP/UDP port number, or uncheck to disable. By default, **TCP/UDP Port Number** is enabled. |




| Label | Description |
|---|---|
| **Group ID** | Indicates the ID of each aggregation group. **Normal** means no aggregation. Only one group ID is valid per port. |
| **Port Members** | Lists each switch port 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 the ports must be in the same speed in each group. |

## LACP

LACP (Link Aggregation Control Protocol) trunks are similar to static port trunks, but they are more flexible because LACP is compliant with the IEEE 802.3ad standard. Hence, it is interoperable with equipment from other vendors that also comply with the standard. This page allows you to enable LACP functions to group ports together to form single virtual links and change associated settings, thereby increasing the bandwidth between the switch and other LACP-compatible devices.

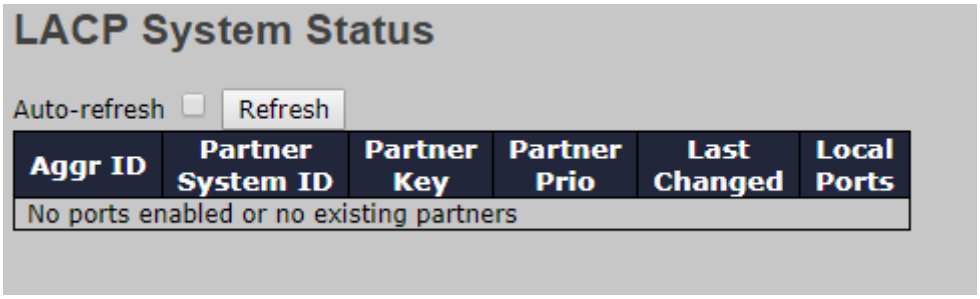



| Label | Description |
|---|---|
| **Port** | Indicates the ID of each aggregation group. **Normal** indicates there is no aggregation. Only one group ID is valid per port. |
| **LACP Enabled** | Lists each switch port for each group ID. Check to include a port in an aggregation, or clear the box to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and the ports must be in the same speed in each group. |
| **Key** | The **Key** value varies with the port, ranging from 1 to 65535. **Auto** will set the key according to the physical link speed (10Mb = 1, 100Mb = 2, 1Gb = 3). **Specific** allows you to enter a user-defined value. Ports with the same key value can join in the same aggregation group, while ports with different keys cannot. |
| **Role** | Indicates LACP activity status. **Active** will transmit LACP packets every 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. |
| **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. |

## LACP System Status

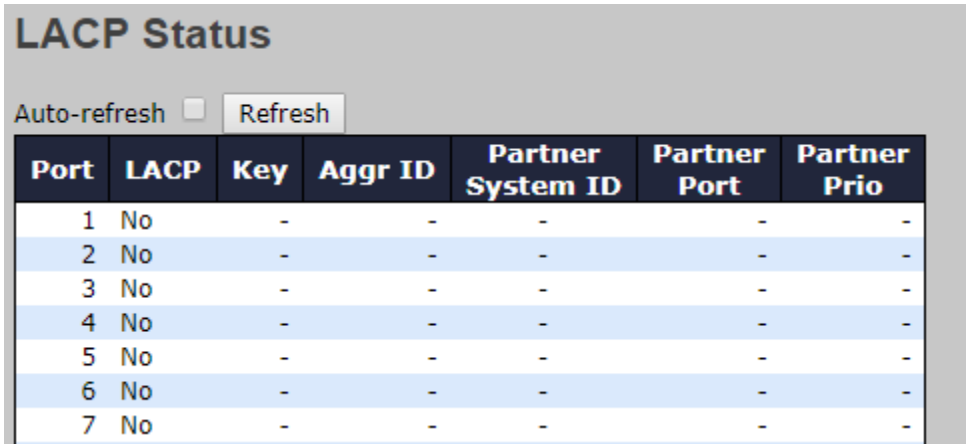
This page provides a status overview for all LACP instances.




| Label | Description |
|---|---|
| **Aggr ID** | The aggregation ID is associated with the aggregation instance. For LLAG, the ID is shown as '**isid:aggr-id**' and for GLAGs as '**aggr-id**' |
| **Partner System ID** | System ID (MAC address) of the aggregation partner |
| **Partner Key** | When connecting the device to other manufactures' devices, you may need to configure LACP partner key. Partner key is the operational key value assigned to the port associated with this link by the Partner. |
| **Last Changed** | The time since this aggregation is changed. |
| **Local Ports** | Indicates which ports belong to the aggregation of the switch/stack. The format is: "**Switch ID:Port**". |
| **Refresh** | Click to refresh the page immediately |
| **Auto-refresh** | Check to enable an automatic refresh of the page at regular intervals |

## LACP Port Status

This page provides an overview of the LACP status for all ports.

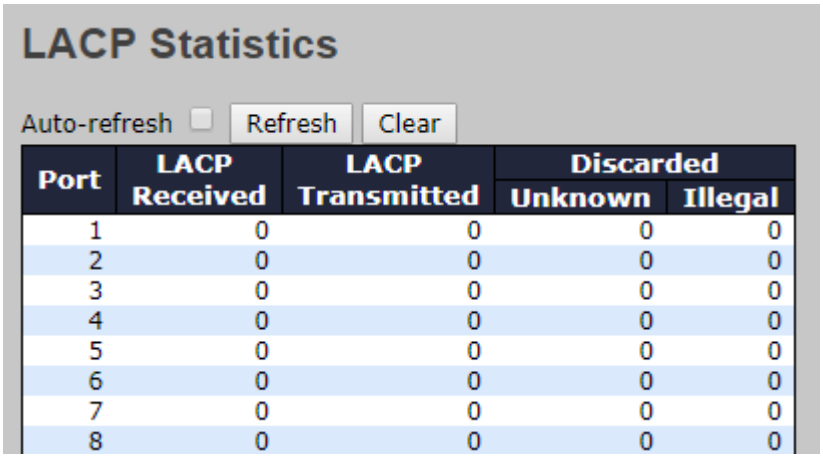



| Port | LACP | Key | Aggr ID | Partner System ID | Partner Port | Partner Prio |
|---|---|---|---|---|---|---|
| 1 | No | - | - | - | - | - |
| 2 | No | - | - | - | - | - |
| 3 | No | - | - | - | - | - |
| 4 | No | - | - | - | - | - |
| 5 | No | - | - | - | - | - |
| 6 | No | - | - | - | - | - |
| 7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

| Label | Description |
|---|---|
| **Port** | Switch port number |
| **LACP** | **Yes** means LACP is enabled and the port link is up. **No** means LACP is not enabled or the port link is down. **Backup** means the port cannot join in the aggregation group unless other ports are removed. The LACP status is disabled. |
| **Key** | The key assigned to the port. Only ports with the same key can be aggregated |
| **Aggr ID** | The aggregation ID assigned to the aggregation group |
| **Partner System ID** | The partner’s system ID (MAC address) |
| **Partner Port** | The partner’s port number associated with the port |
| **Partner Prio** | The partner's port priority. |
| **Refresh** | Click to refresh the page immediately |
| **Auto-refresh** | Check to enable an automatic refresh of the page at regular intervals |

## LACP Port Statistics

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



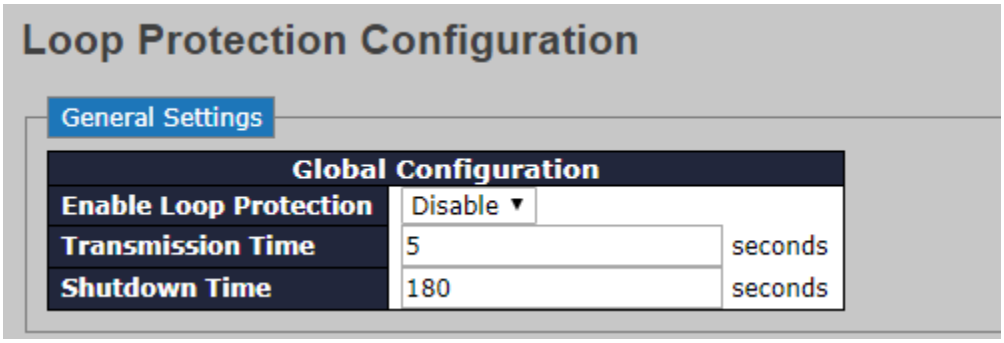

| Port | LACP Received | LACP Transmitted | Discarded | |
|---|---|---|---|---|
| | | | Unknown | Illegal |
| 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 |

| Label | Description |
|---|---|
| **Port** | Switch port number |
| **LACP Transmitted** | The number of LACP frames sent from each port |
| **LACP Received** | The number of LACP frames received at each port |
| **Discarded** | The number of unknown or illegal LACP frames discarded at each port. |
| **Refresh** | Click to refresh the page immediately |
| **Auto-refresh** | Check to enable an automatic refresh of the page at regular intervals |
| **Clear** | Click to clear the counters for all ports |

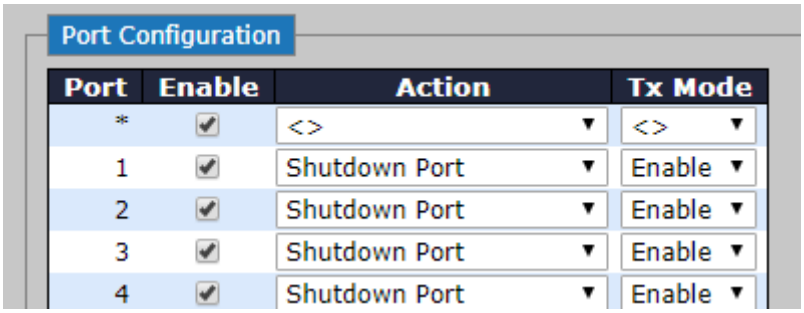
## 1.3.4 Loop Protection

This feature prevents loop attack. When receiving loop packets, the port will be disabled automatically, preventing the loop attack from affecting other network devices.

### Configuration



| Label | Description |
|---|---|
| **Enable Loop Protection** | Activate loop protection functions (as a whole) |
| **Transmission Time** | The interval between each loop protection PDU sent on each port. The valid value is 1 to 10 seconds. |
| **Shutdown Time** | The period (in seconds) for which a port will be kept disabled when a loop is detected (shutting down the port). The valid value is 0 to 604800 seconds (7 days). A value of zero will keep a port disabled permanently (until the device is restarted). |

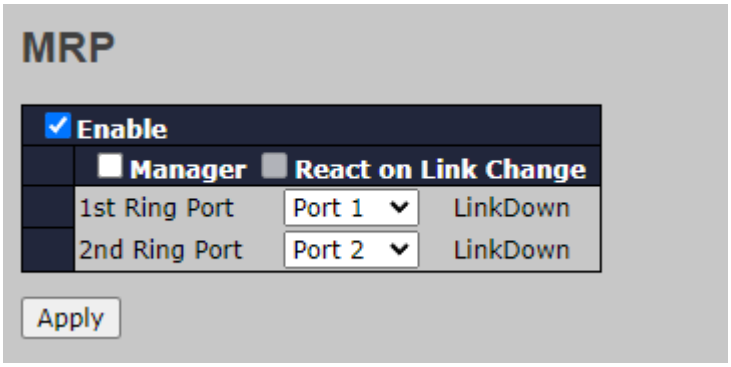



| Label | Description |
|---|---|
| **Port** | Switch port number |
| **Enable** | Activate loop protection functions (as a whole) |
| **Action** | Configures the action to take when a loop is detected. Valid values include **Shutdown Port**, **Shutdown Port**, and **Log or Log Only**. |
| **Tx Mode** | Controls whether the port is actively generating loop protection PDUs or only passively look for looped PDUs. |

# 1.4 Redundancy

## 1.4.1.1 MRP

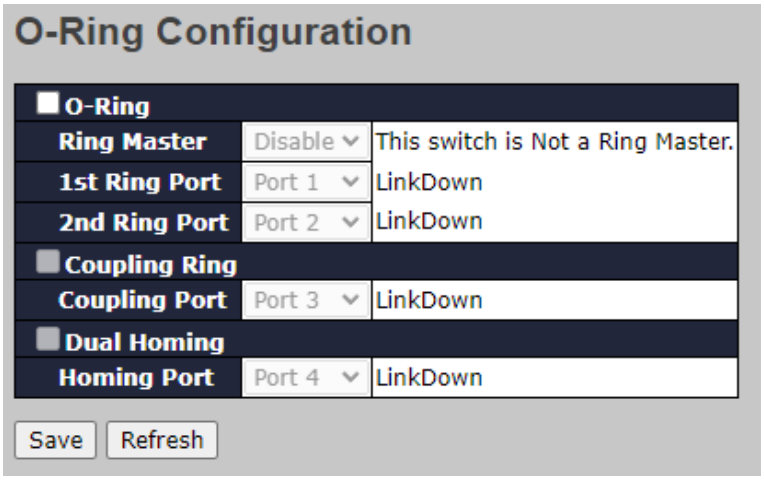
MRP (Media Redundancy Protocol) is an industry standard for high-availability Ethernet networks. MRP allowing Ethernet switches in ring configuration to recover from failure rapidly to ensure seamless data transmission. A MRP ring (IEC 62439) can support up to 50 devices and will enable a back-up link in 80ms (adjustable to max. 200ms/500ms).




| Label | Description |
|---|---|
| **Enable** | Enables the MRP function |
| **Manager** | Every MRP topology needs a MRP manager. One MRP topology can only have a Manager. If two or more switches are set to be Manager, the MRP topology will fail. |
| **React on Link Change (Advanced mode)** | Faster mode. Enabling this function will cause MRP topology to converge more rapidly. This function only can be set in MRP manager switch. |
| **1st Ring Port** | Chooses the port which connects to the MRP ring |
| **2nd Ring Port** | Chooses the port which connects to the MRP ring |

## 1.4.1.2 O-Ring

Ring is the most powerful Ring in the world. The recovery time of Ring is less than 30 ms. It can reduce unexpected damage caused by network topology change. Ring Supports 3 Ring topology: Ring, Coupling Ring and Dual Homing.



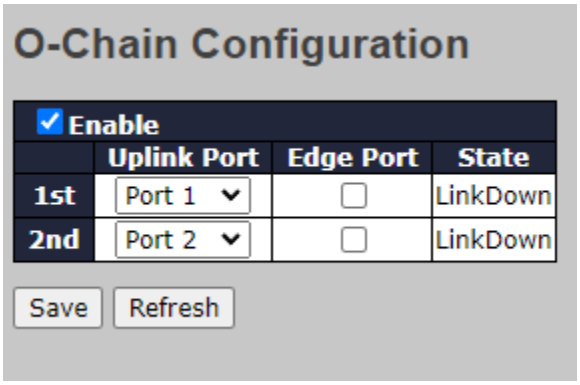

The following table describes the labels in this screen.

| Label | Description |
|---|---|
| **Redundant Ring** | Mark to enable Ring. |
| **Ring Master** | There should be one and only one Ring Master in a ring. However if there are two or more switches which set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters. |
| **1st Ring Port** | The primary port, when this switch is Ring Master. |
| **2nd Ring Port** | The backup port, when this switch is Ring Master. |
| **Coupling Ring** | Mark to enable Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller rings to avoid effecting all switches when network topology change. It is a good application for connecting two Rings. |
| **Coupling Port** | Link to Coupling Port of the switch in another ring. Coupling Ring need four switch to build an active and a backup link. Set a port as coupling port. The coupled four ports of four switches will be run at active/backup mode. |
| **Dual Homing** | Mark to enable Dual Homing. By selecting Dual Homing mode, Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each Ring to the normal switches in RSTP mode. |
| **Apply** | Click "**Apply**" to set the configurations. |

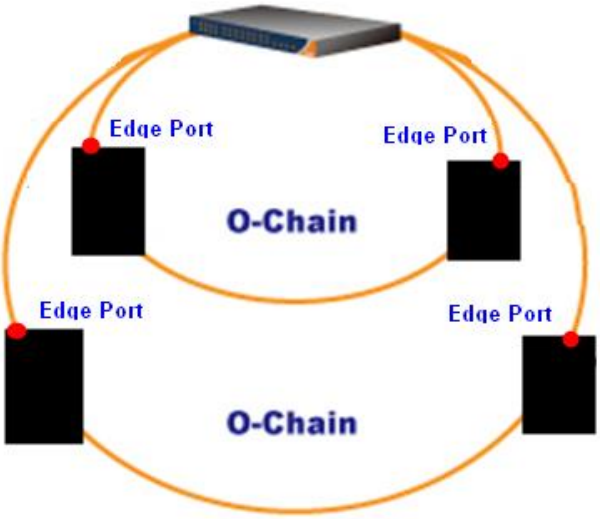
**Note:** We don't suggest you to set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load.

### 1.4.1.3 O-Chain

O-Chain is the revolutionary network redundancy technology that provides the add-on network redundancy topology for any backbone network, providing ease-of-use while maximizing fault-recovery swiftness, flexibility, compatibility, and cost-effectiveness in one set of network redundancy topologies O-Chain allows multiple redundant network rings of different redundancy protocols to join and function together as a larger and more robust compound network topology, i.e. the creation of multiple redundant networks beyond the limitations of current redundant ring technology.



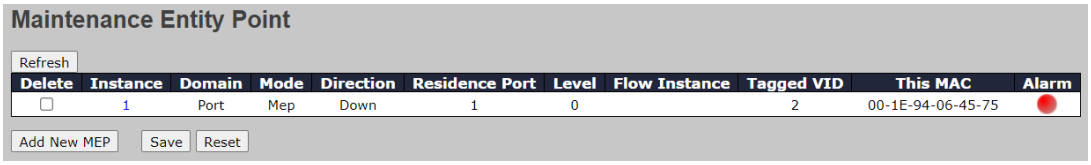

| Label | Description |
|---|---|
| **Enable** | Enabling the O-Chain function |
| **1st Ring Port** | Choosing the port which connect to the ring |
| **2nd Ring Port** | Choosing the port which connect to the ring |
| **Edge Port** | In the O-Chain application, the head and tail of two Switch Port, must start the Edge,MAC smaller Switch, Edge port will be the backup and RM LED Light. |



### 1.4.1.4 G.8032

#### 1.4.1.4.1 MEP

The Maintenance Entity Point instances are configured here.




| Label | 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. |
| **Domain** | **Port:** This is a MEP in the Port Domain. 'Flow Instance' is a Port.<br>**Esp:** Future use<br>**Evc:** This is a MEP in the EVC Domain. 'Flow Instance' is a EVC<br>**Mpls:** Future use |
| **Mode** | **MEP:** This is a Maintenance Entity End Point.<br>**MIP:** This is a Maintenance Entity Intermediate Point. |
| **Direction** | **Ingress:** This is a Ingress (down) MEP - monitoring ingress traffic on 'Residence Port'.<br>**Egress:** This is a Egress (up) MEP - monitoring egress traffic on 'Residence Port'. |
| **Residence Port** | The port where MEP is monitoring - see 'Direction'. |
| **Level** | The MEG level of this MEP. |
| **Flow Instance** | The MEP is related to this flow - See 'Domain'. |
| **Tagged VID** | **Port MEP:** An outer C/S-tag (depending on VLAN Port Type) is added with this VID.<br>Entering '0' means no TAG added. |
| **This MAC** | The MAC of this MEP - can be used by other MEP when unicast is selected (Info only). |
| **Alarm** | There is an active alarm on the MEP. |

### MEP Configuration –Instance Data

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

**Instance Data**

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|---|---|---|---|---|---|---|---|---|
| 1 | Port | Mep | Down | 1 | | 2 | 0 | 00-1E-94-06-45-75 |

| Label | Description |
|---|---|
| **MEP Instance** | MEP Instance |
| **Domain** | Show domain info . |
| **Mode** | Show mode info |
| **Direction** | Show direction info . |
| **Residence Port** | Show residence port info |
| **Flow Instance** | Show flow instance info |
| **Tagged VID** | Show the MEP Tagged VID Value . |
| **This MAC** | Show the switch MAC |

### MEP Configuration –Instance Data

**Instance Configuration**

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSD | aTSF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | ITU ICC | | ICC000MEG0000 | 1 | 2 | ☐ | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |

**Peer MEP Configuration**

| Delete | Peer MEP ID | Unicast Peer MAC | | cLOC | cRDI | cPeriod | cPriority | cDEG |
|---|---|---|---|---|---|---|---|---|
| | No Peer MEP Added | | | | | | | |
| Delete | 0 | 00-00-00-00-00-00 | | | | | | |

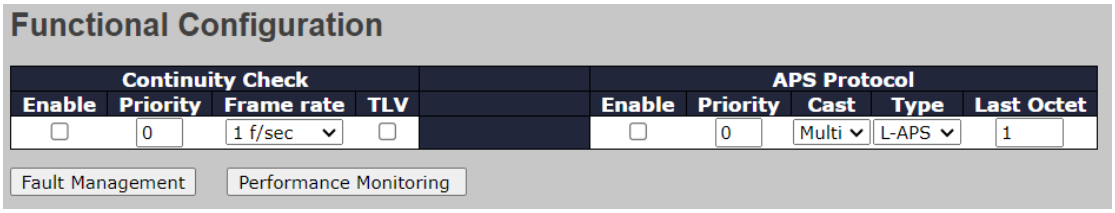
Add New Peer MEP

| Label | Description |
|---|---|
| **Level** | See help on MEP create WEB. |
| **Format** | This is the configuration of the two possible Maintenance Association Identifier formats.<br>**ITU ICC:** This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char.<br><br>**IEEE String:** This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char.<br><br>**ITU CC ICC:** This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char. |

| | |
|---|---|
| **Domain Name** | This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char. |
| **MEG Id** | This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be max 16 char. |
| **MEP Id** | This value will become the transmitted two byte CCM MEP ID. |
| **Tagged VID** | This value will be the VID of a TAG added to the OAM PDU. |
| **VOE** | This will attempt to utilize VOE HW for MEP implementation. Not all platforms support VOE. |
| **cLevel** | Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP. |
| **cMEG** | Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP. |
| **cMEP** | Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP. |
| **cAIS** | Fault Cause indicating that AIS PDU is received. |
| **cLCK** | Fault Cause indicating that LCK PDU is received. |
| **cDEG** | Fault Cause indicating that server layer is indicating Signal Degraded. |
| **cSSF** | Fault Cause indicating that server layer is indicating Signal Fail. |
| **aBLK** | The consequent action of blocking service frames in this flow is active. |
| **aTSD** | The consequent action of indicating Trail Signal Degrade is calculated. |
| **aTSF** | The consequent action of indicating Trail Signal Fail to-wards protection is active. |
| **Delete** | This box is used to mark a Peer MEP for deletion in next Save operation. |
| **Peer MEP ID** | This value will become an expected MEP ID in a received CCM - see 'cMEP'. |
| **Unicast Peer MAC** | This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP. |
| **cLOC** | Fault Cause indicating that no CCM has been received (in 3,5 |

| | |
|---|---|
| | periods) - from this peer MEP. |
| **cRDI** | Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP. |
| **cPeriod** | Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP. |
| **cPriority** | Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP. |

**MEP Configuration –Functional Configuration**




| Label | Description |
|---|---|
| | **Continuity Check** |
| **Enable** | Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1. |
| **Priority** | The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same. |
| **Frame rate** | Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has the following uses:<br>* The transmission rate of the CCM PDU.<br><br>* Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'.<br><br>* Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'.<br><br>Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame |

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

### TLV Configuration

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


| Label | Description |
|---|---|
| **OUI First** | The transmitted first value in the OS TLV OUI field. |
| **Format** | This is the configuration of the two possible Maintenance Association Identifier formats.<br>**ITU ICC:** This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char.<br><br>**IEEE String:** This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char. |

| | |
|---|---|
| | **ITU CC ICC:** This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char. |

### TLV Status

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | | | CC Port Status | | | CC Interface Status | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | | Value | Last RX | | Value | Last RX |
| No Peer MEP Added | | | | | | | | | | | | |

| Label | Description |
|---|---|
| **Level** | See help on MEP create WEB. |
| **Format** | This is the configuration of the two possible Maintenance Association Identifier formats.<br>**ITU ICC:** This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char.<br><br>**IEEE String:** This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char.<br><br>**ITU CC ICC:** This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char. |

### Link State Tracking

Link State Tracking

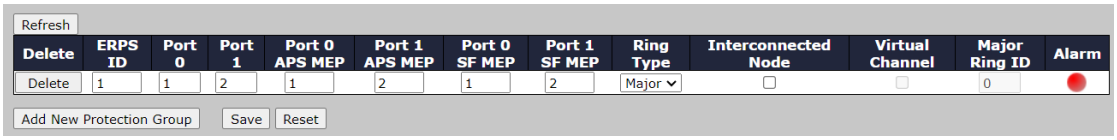
Enable

| Label | Description |
|---|---|
| **Level** | See help on MEP create WEB. |
| **Format** | This is the configuration of the two possible Maintenance Association Identifier formats.<br>**ITU ICC:** This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char.<br><br>**IEEE String:** This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char. |

| | |
|---|---|
| | **ITU CC ICC:** This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char. |

### 1.4.1.4.2 ERPS

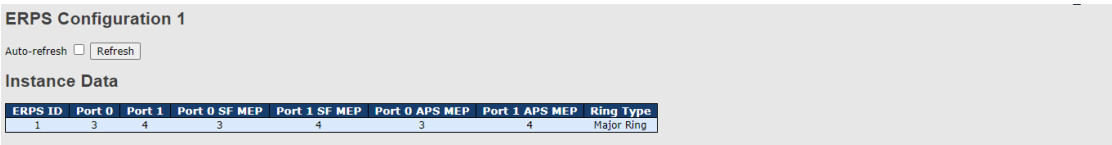
The Ethernet Ring Protection Switch instances are configured here.




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

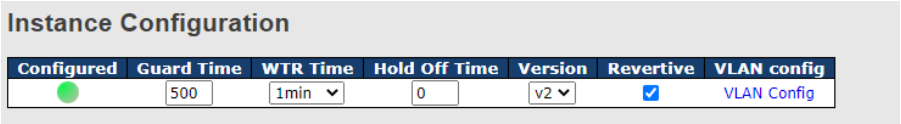
| | |
|---|---|
| | checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel. |
| **Major Ring ID** | Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring. |
| **Alarm** | There is an active alarm on the ERPS. |

### ERPS Configuration-Instance Data




| Label | Description |
|---|---|
| **ERPS ID** | The ID of the Protection group. |
| **Port 0** | See help on ERPS create WEB. |
| **Port 1** | See help on ERPS create WEB. |
| **Port 0 SF MEP** | See help on ERPS create WEB. |
| **Port 1 SF MEP** | See help on ERPS create WEB. |
| **Port 0 APS MEP** | See help on ERPS create WEB. |
| **Port 1 APS MEP** | See help on ERPS create WEB. |
| **Ring Type** | Type of Protecting ring. It can be either major ring or sub-ring. |

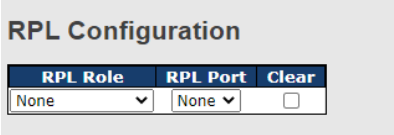
### ERPS Configuration-Instance Configuration




| Label | Description |
|---|---|
| **Configured** | Red: This ERPS is only created and has not yet been configured - is not active.<br>Green: This ERPS is configured - is active. |
| **Guard Time** | Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. |

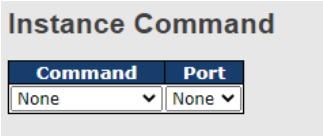
| | |
|---|---|
| | The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms |
| **WTR Time** | The Wait To Restore timing value to be used in revertive switching.<br><br>The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes. |
| **Hold Off Time** | The timing value to be used to make persistent check on Signal Fail before switching.<br><br>The range of the hold off timer is 0 to 10 seconds in steps of 100 ms |
| **Version** | ERPS Protocol Version - v1 or v2 |
| **Revertive** | In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL.<br><br>In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared. |
| **VLAN config** | VLAN configuration of the Protection Group. Click on the "VLAN Config" link to confure VLANs for this protection group. |

**ERPS Configuration-RPL Configuration**



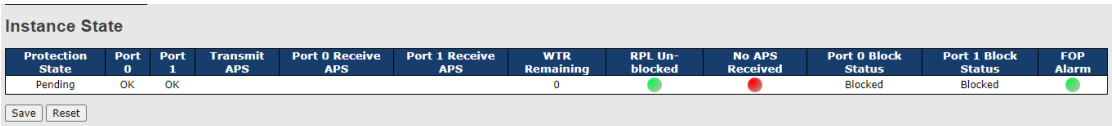

| Label | Description |
|---|---|
| **RPL Role** | It can be either RPL owner or RPL Neighbour. |
| **RPL Port** | This allows to select the east port or west port as the RPL block. |
| **Clear** | If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.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

**ERPS Configuration- Instance Command**




| Label | Description |
|---|---|
| **orced Switch** | Forced Switch command forces a block on the ring port where the command is issued. |
| **Manual Switch** | In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued. |
| **Clear** | The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch). |
| **Port** | Port selection - Port0 or Port1 of the protection Group on which the command is applied. |

**ERPS Configuration- Instance Command**



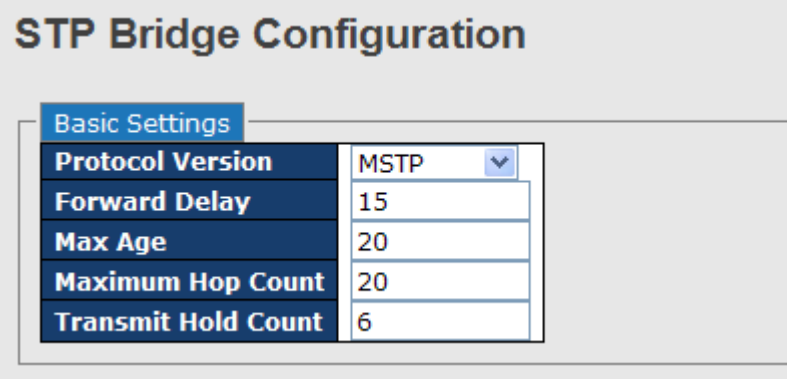

| Label | Description |
|---|---|
| **Protection State** | ERPS state according to State Transition Tables in G.8032. |
| **Port 0** | OK: State of East port is ok<br>SF: State of East port is Signal Fail |
| **Port 1** | OK: State of West port is ok<br>SF: State of West port is Signal Fail |
| **Transmit APS** | The transmitted APS according to State Transition Tables in G.8032. |
| **Port 0 Receive APS** | The received APS on Port 0 according to State Transition Tables in G.8032. |
| **Port 1 Receive APS** | The received APS on Port 1 according to State Transition Tables in G.8032. |
| **WTR Remaining** | Remaining WTR timeout in milliseconds. |
| **RPL Un-blocked** | APS is received on the working flow. |
| **No APS Received** | RAPS PDU is not received from the other end. |
| **Port 0 Block Status** | Block status for Port 0 (Both traffic and R-APS block status).<br>R-APS channel is never blocked on sub-rings without virtual |

| | |
|---|---|
| | channel. |
| **Port 1 Block Status** | Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel. |
| **FOP Alarm** | Failure of Protocol Defect(FOP) status. If FOP is detected, red LED glows; else green LED glows. |

### 1.4.1.5 MSTP

#### Bridge Settings

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

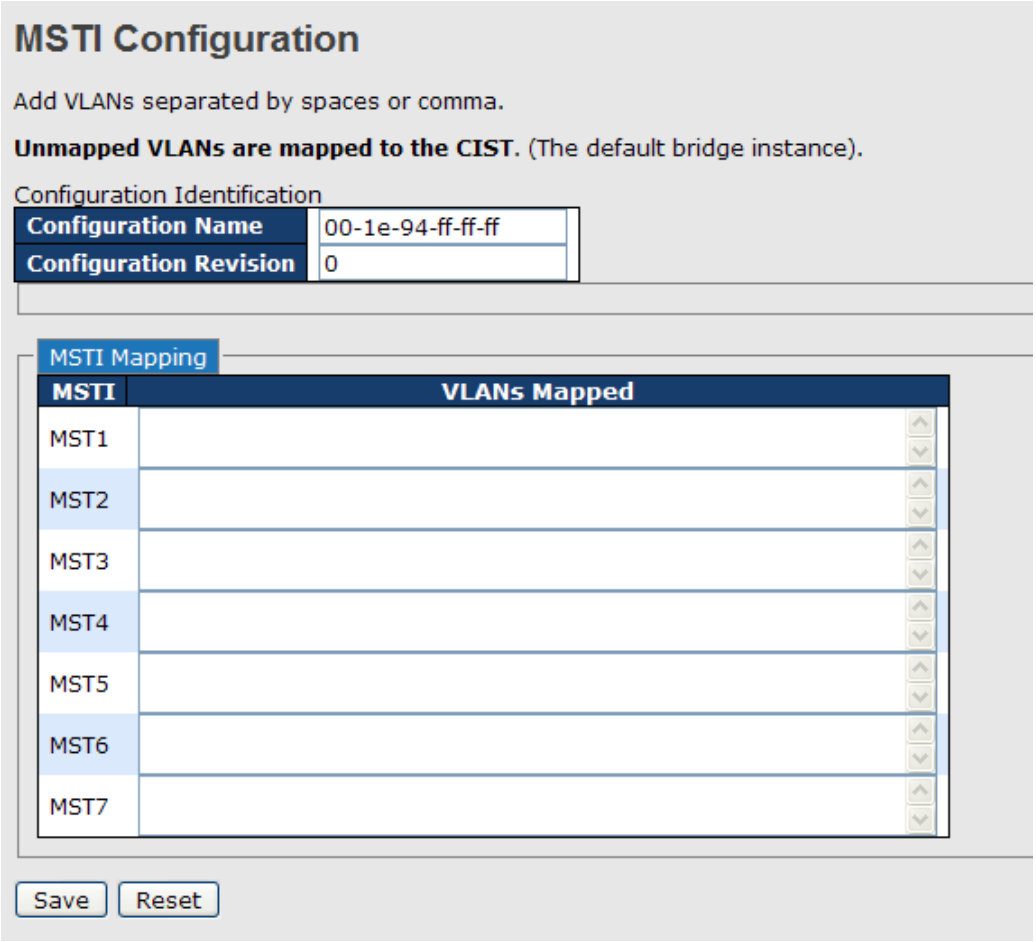



| Label | Description |
|---|---|
| **Protocol Version** | The STP protocol version setting. Valid values are STP, RSTP and MSTP. |
| **Forward Delay** | The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 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 remainingHops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 4 to 30 seconds, and MaxAge must be <= (FwdDelay-1)*2. |
| **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. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## MSTI Mapping

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

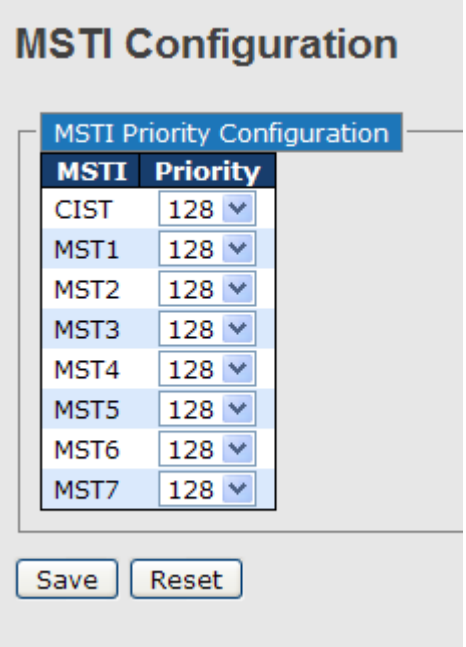



| Label | Description |
|---|---|
| **Configuration Name** | The name identifiying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters. |
| **Configuration** | The revision of the MSTI configuration named above. This must |

| | |
|---|---|
| **Revision** | be an integer between 0 and 65535. |
| **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 VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## MSTI Priorities

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

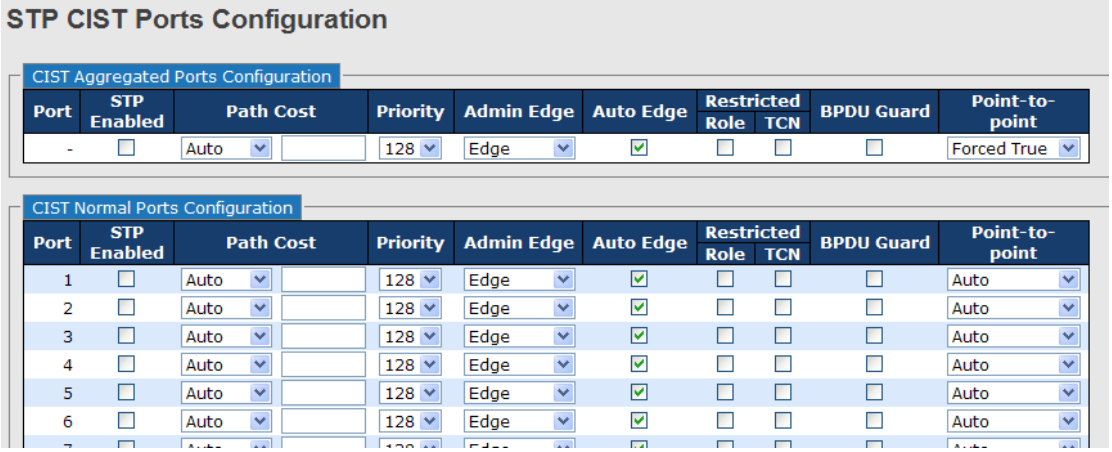



| Label | Description |
|---|---|
| **MSTI** | The bridge instance. The CIST is the default instance, which is always active. |
| **Priority** | Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC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

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

## 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. The aggregation settings are stack global.



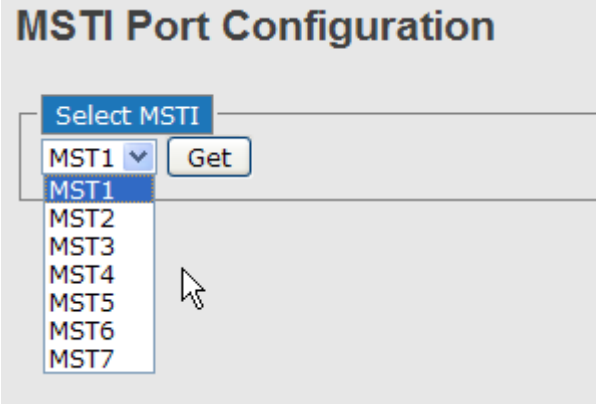

| Label | Description |
|---|---|
| **Port** | The switch port number of the logical STP port. |
| **STP Enabled** | Controls whether STP is enabled on this switch port. |
| **Path Cost** | Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical 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 favor of higher path cost ports. Valid values are in the range 1 to 200000000. |
| **Priority** | Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). |
| **OpenEdge(setate flag)** | Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transitioning to the forwarding state is faster for edge ports (having operEdge true) |

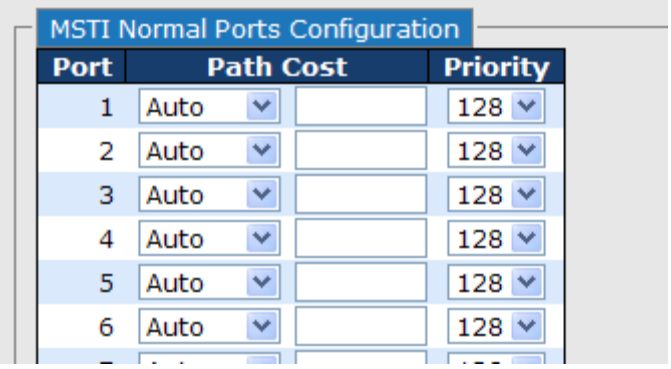
| | |
|---|---|
| | than for other ports. |
| **AdminEdge** | Controls whether the operEdge flag should start as beeing set or cleared. (The initial operEdge state when a port is initialized). |
| **AutoEdge** | Controls whether the bridge should enable automatic edge detection on the bridge port. This 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 influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also know 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 trees active topology as a result of persistent incorrectly 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 is the physical link state for the attached LANs transitions frequently. |
| **Point2Point** | Controls whether the port connects to a point-to-point LAN rather than 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. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

## MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. A MSTI port is a virtual port, which is instantiated seperately for each

active CIST (physical) port for each MSTI instance configured and applicable for 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. The aggregation settings are stack global.



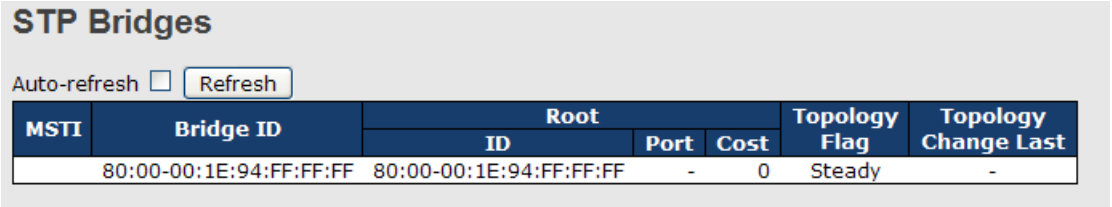

| Label | Description |
|---|---|
| **Port** | The switch port number of the corresponding STP CIST (and MSTI) port. |
| **Path Cost** | Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. |
| **Priority** | Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). |

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

## STP Bridges

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

The displayed table contains a row for each STP bridge instance, where the column displays the following information:



STP Bridges

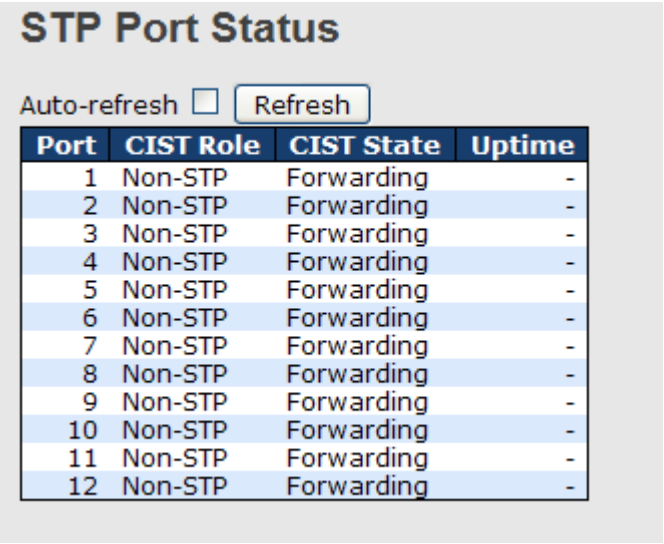
Auto-refresh ☐ Refresh

| MSTI | Bridge ID | Root | | | Topology Flag | Topology Change Last |
|---|---|---|---|---|---|---|
| | | ID | Port | Cost | | |
| | 80:00-00:1E:94:FF:FF:FF | 80:00-00:1E:94:FF:FF:FF | - | 0 | Steady | - |

| Label | Description |
|---|---|
| **MSTI** | The Bridge Instance. This is also a link to the STP Detailed Bridge Status. |
| **Bridge ID** | The Bridge ID of this Bridge instance. |
| **Root ID** | The Bridge ID of the currently elected root bridge. |
| **Root Port** | The switch port currently assigned the root port role. |
| **Root Cost** | Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge. |
| **Topology Flag** | The current state of the Topology Change Flag for this Bridge instance. |
| **Topology Change Last** | The time since last Topology Change occurred. |
| Refresh | Click to refresh the page immediately. |
| Auto-refresh ☐ | Check this box to enable an automatic refresh of the page at regular intervals. |

## STP Port Status

This page displays the STP CIST port status for port physical ports in the currently selected switch.

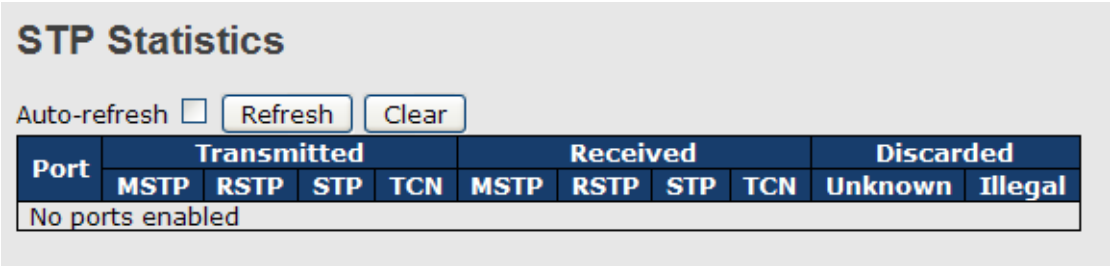



| Port | CIST Role | CIST State | Uptime |
|---|---|---|---|
| 1 | Non-STP | Forwarding | - |
| 2 | Non-STP | Forwarding | - |
| 3 | Non-STP | Forwarding | - |
| 4 | Non-STP | Forwarding | - |
| 5 | Non-STP | Forwarding | - |
| 6 | Non-STP | Forwarding | - |
| 7 | Non-STP | Forwarding | - |
| 8 | Non-STP | Forwarding | - |
| 9 | Non-STP | Forwarding | - |
| 10 | Non-STP | Forwarding | - |
| 11 | Non-STP | Forwarding | - |
| 12 | Non-STP | Forwarding | - |

| Label | 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. |
| **State** | The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding. |
| **Uptime** | The time since the bridge port was last initialized. |
| Refresh | Click to refresh the page immediately. |
| Auto-refresh | Check this box to enable an automatic refresh of the page at regular intervals. |

## STP Statistics

This page displays the RSTP port statistics counters for bridge ports in the currently selected switch.

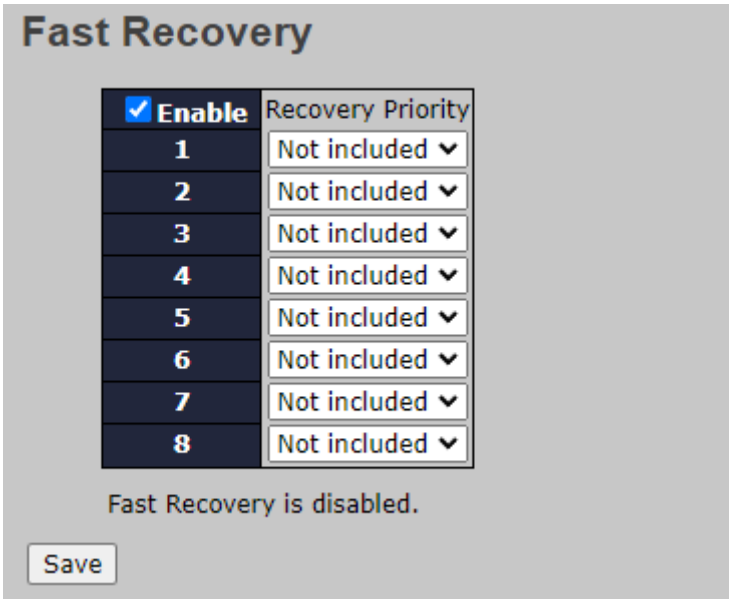



| Port | Transmitted | | | | Received | | | | Discarded | |
|---|---|---|---|---|---|---|---|---|---|---|
| | MSTP | RSTP | STP | TCN | MSTP | RSTP | STP | TCN | Unknown | Illegal |
| No ports enabled | | | | | | | | | | |

| Label | Description |
|---|---|
| **Port** | The switch port number of the logical RSTP port. |
| **RSTP** | The number of RSTP Configuration BPDU's received/transmitted on the port. |
| **STP** | The number of legacy STP Configuration BPDU's received/transmitted on the port. |
| **TCN** | The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port. |
| **Discarded Unknown** | The number of unknown Spanning Tree BPDU's received (and discarded) on the port. |
| **Discarded Illegal** | The number of illegal Spanning Tree BPDU's received (and discarded) on the port. |
| Refresh | Click to refresh the page immediately. |
| Auto-refresh ☐ | Check this box to enable an automatic refresh of the page at regular intervals. |

### 1.4.1.6 Fast Recovery Mode

The Fast Recovery Mode can be set to connect multiple ports to one or more switches. The IGPS-9084GP-LA with its fast recovery mode will provide redundant links. Fast Recovery mode supports 12 priorities, only the first priority will be the act port, the other ports configured with other priority will be the backup ports.



The following table describes the labels in this screen.

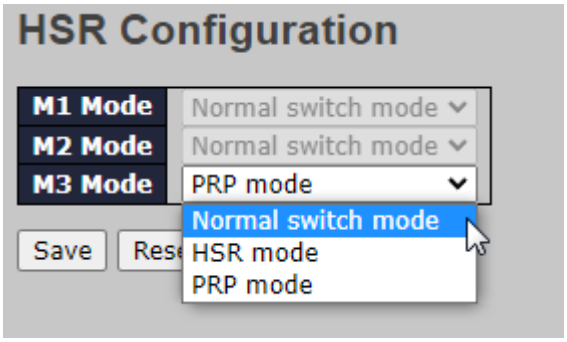
| Label | Description |
|---|---|
| **Active** | Activate the fast recovery mode. |
| **port** | Port can be configured as 12 priorities. Only the port with highest priority will be the active port. 1st Priority is the highest. |
| **Apply** | Click "**Apply**" to activate the configurations. |

## 1.4.1.7 HSR/PRP(only for HSR/PRP Model )

### HSR Config

The page will auto detect HSR/PRP Module , if your slot connect HSR /PRP Module .

Will can select the module work mode




| Label | Description |
|---|---|
| **Normal Switch Mode** | The module G1/G2 Port = Normal Switch port . |
| **PRP Mode** | The module G1/G2 Port will run PRP . |
| **HSR Mode** | The module G1/G2 Port will run HSR |

### Module Information

This pager will show HSR Module status and Module Port status .

## Module Information

Auto-refresh ☐ Refresh

## Module Status

| Slot Information | | | |
|---|---|---|---|
| **Module #** | **Mode** | **Status** | **Address** |
| M#1 | -- | Other | -- |
| M#2 | -- | Other | -- |
| M#3 | prp | Ready | 00-1E-94-FF-FF-FF |

## Module Port Status

| Module # | Port | Link | Autoneg | Speed | Duplex |
|---|---|---|---|---|---|
| M#1 | Port A | -- | -- | -- | -- |
| M#1 | Port B | -- | -- | -- | -- |
| M#2 | Port A | -- | -- | -- | -- |
| M#2 | Port B | -- | -- | -- | -- |
| M#3 | Port A | Down | Yes | 1Gbps | Half |
| M#3 | Port B | Down | Yes | 1Gbps | Half |

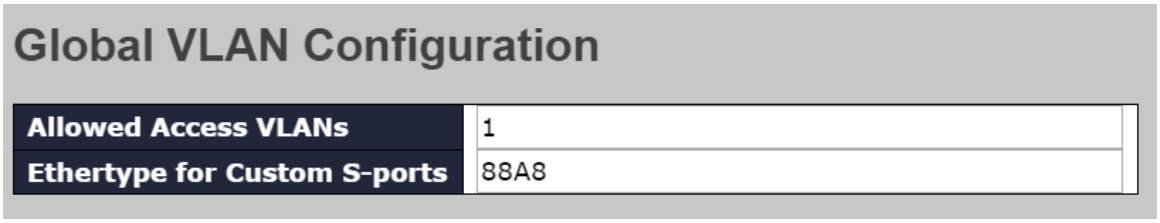
| Label | Description |
|---|---|
| **Module Status** | |
| **Mode** | Show Module status ( None / PRP / HSR) |
| **Status** | Other = no module connected<br>Ready = Module connect and ready . |
| **Address** | Show HSR(PRP) Module MAC Address ( not is switch MAC) |
| **Module Port Status** | |
| **Link** | Show Link status (Up / Down) |
| **Autonego** | Show Auto-negotiation status |
| **Speed** | Display Port link speed (100M/1G) |
| **Duplex** | Display port link duplex status ( Full / Half) |

# 1.5 VLAN

## 1.5.1 VLAN Membership

A VLAN is a group of end devices with a common set of requirements, independent of physical location. With the same attributes as a physical LAN, VLANs enable you to group end devices even if they are not located physically on the same LAN segment. By splitting up a network into sets of VLANs, assigning ports to individual VLANs, and defining criteria for VLAN membership for workstations connected to those ports, traffic for the same VLAN can be sent between switches.

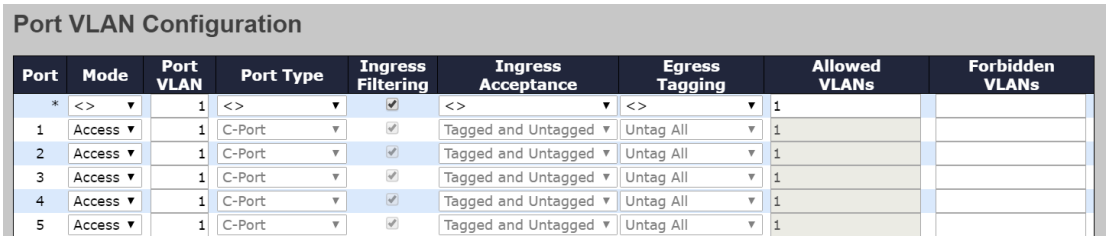
### Global VLAN Configuration




| Label | Description |
|---|---|
| Allowed Access VLANs | This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of the VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.<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. |
| **Ethertype for Custom** | This field specifies the ethertype/TPID (specified in |

| | |
|---|---|
| **S-ports** | 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 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 | |

| Label | Description |
|---|---|
| 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><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 not classified to the Access VLAN<br>• On egress all frames are transmitted untagged |

| | |
|---|---|
| | **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><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><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><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 |

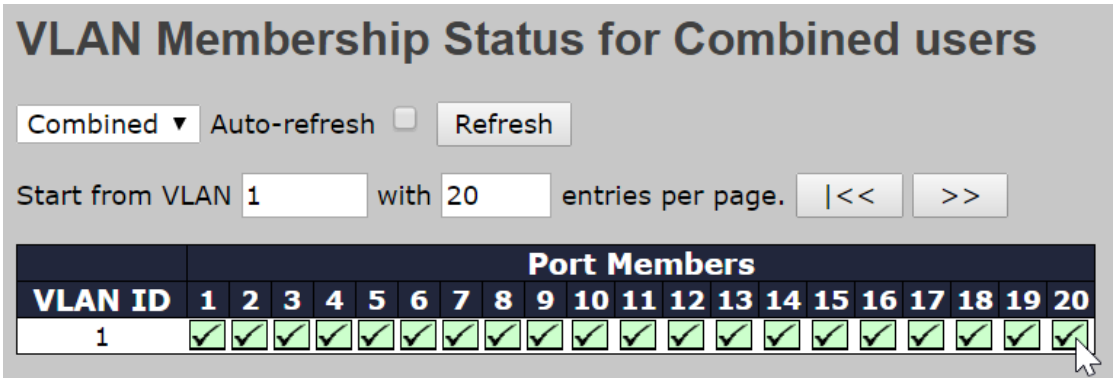
| | |
|---|---|
| | tagged if Egress Tagging configuration is set to untag Port VLAN.<br>The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode. |
| **Port Type** | Ports in hybrid mode allow for changing the port type, that is, whether a frame's 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.<br>If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN.<br>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 = 0x88A8 get classified to the VLAN ID embedded in the tag.<br>Priority-tagged frames are classified to the Port VLAN.<br>If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped.<br>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 equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag.<br>Priority-tagged frames are classified to the Port VLAN.<br>If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. |

| | |
|---|---|
| | 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. See Port Type for a description of when a frame is considered tagged.<br>**Tagged Only**<br>Only frames tagged with the corresponding Port Type tag are accepted on ingress.<br>**Untagged Only**<br>Only untagged frames are accepted on ingress. See Port Typefor a description of when a frame is considered untagged. |
| **Egress Tagging** | Ports in Trunk and Hybrid mode may control the tagging of frames on egress.<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.<br>This option is only available for ports in Hybrid mode. |
| **Allowed VLANs** | Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. |

| | |
|---|---|
| | The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to **1-4095**.<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 become member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.<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. |

## 1.5.2 Membership Status

This page provides an overview of membership status of VLAN users.




| Label | 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. |

| | |
|---|---|
| | 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: ✗c. The port will not be a member of the VLAN in this case. |

## 1.5.3 Port Status

This page provides VLAN Port Status

**VLAN Port Status for Combined users**

Combined ▾ Auto-refresh ☐ Refresh

| 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 |

| Label | 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 VLAN 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. |

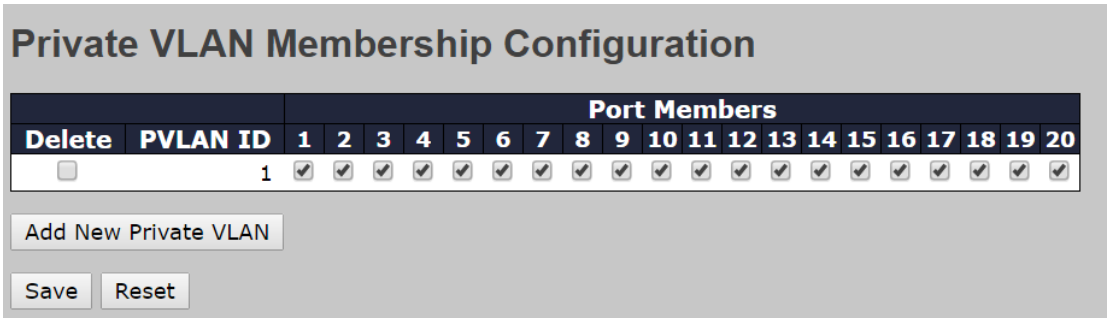
### 1.5.4 Private VLAN

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

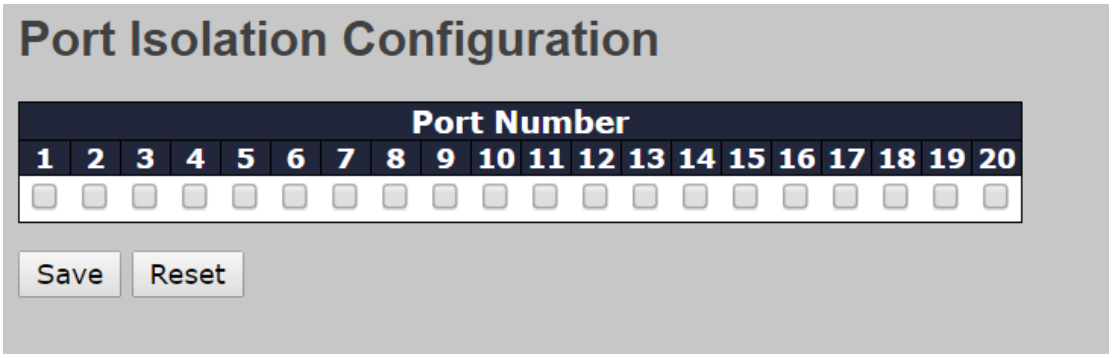
be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and private VLAN IDs can be identical.

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.




| Label | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Private VLAN ID** | Indicates the ID of this particular private VLAN. |
| **MAC Address** | The MAC address for the entry. |
| **Port Members** | A row of check boxes for each port is displayed for each private VLAN ID. You can check the box to include a port in a private VLAN. 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 Static Entry** | Click **Add New Private WLAN** 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. |



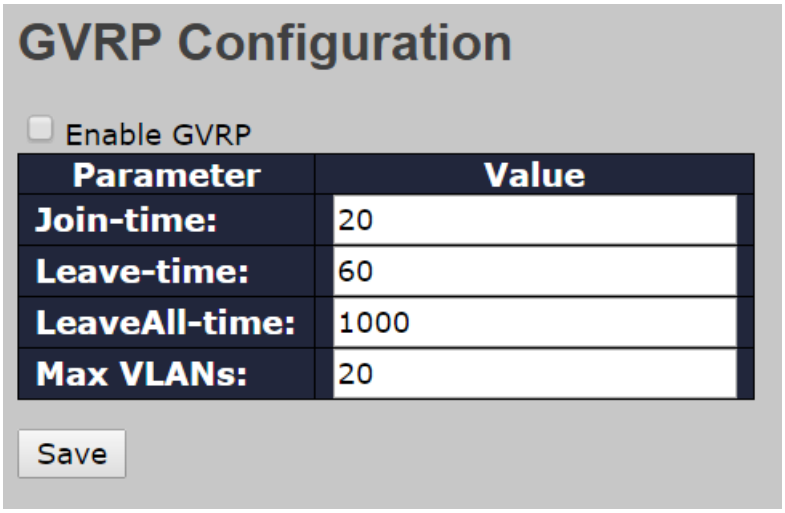

| Label | Description |
|---|---|
| **Port Members** | A check box is provided for each port of a private VLAN.<br>When checked, port isolation is enabled for that port.<br>When unchecked, port isolation is disabled for that port.<br>By default, port isolation is disabled for all ports. |

## 1.5.5 GVRP

GVRP is an acronym for **G**ARP **V**LAN **R**egistration **P**rotocol. It is a protocol for dynamicaly registering VLANs on ports, and is specified in IEEE 802.1Q-2005, clause 11. GVRP is an example of the use of GARP, hence the G in GVRP.

### GVRP Config

This page allows you to configure the global GVRP configuration settings that are commonly applied to all GVRP enabled ports.

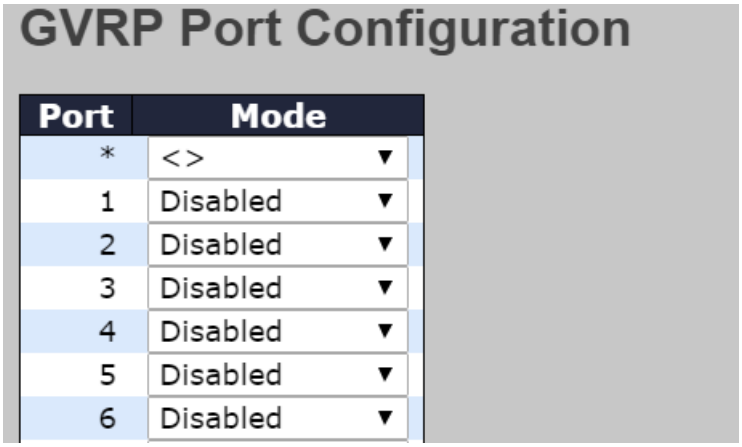



| Label | Description |
|---|---|

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

## Port Config

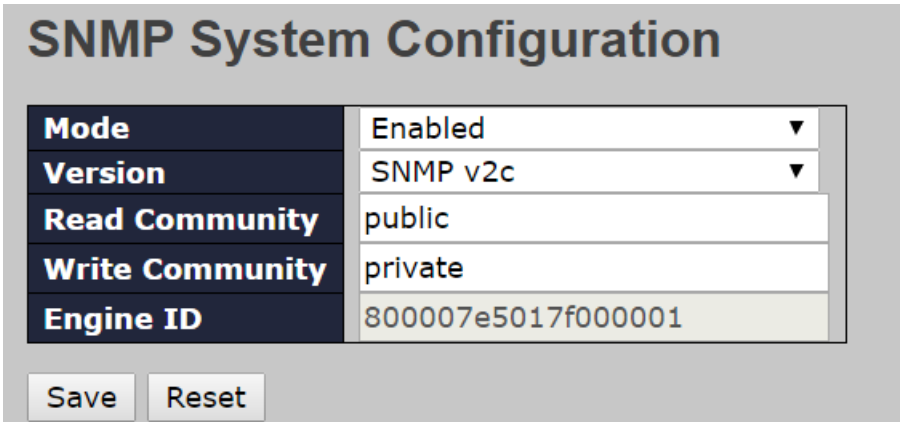
This page allows you to enable or disable a port for GVRP operation. This configuration can be performed either before or after GVRP is configured globally - the protocol operation will be the same.




| Label | 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. |

# 1.6 SNMP

## 1.6.1 SNMP System Configurations




| Label | Description |
|---|---|
| **Mode** | Indicates existing SNMP mode. Possible modes include:<br>**Enabled**: enable SNMP mode<br>**Disabled**: disable SNMP mode |
| **Version** | Indicates the supported SNMP version. Possible versions include:<br>**SNMP v1**: supports SNMP version 1.<br>**SNMP v2c**: supports SNMP version 2c.<br>**SNMP v3**: supports SNMP version 3. |
| **Read Community** | Indicates the read community string to permit access to SNMP agent. The allowed string length is 0 to 255, and only ASCII characters from 33 to 126 are allowed.<br>The field only suits to SNMPv1 and SNMPv2c. SNMPv3 uses USM for authentication and privacy and the community string will be associated with SNMPv3 community table. |
| **Write Community** | Indicates the write community string to permit access to SNMP agent. The allowed string length is 0 to 255, and only ASCII characters from 33 to 126 are allowed.<br>The field only suits to SNMPv1 and SNMPv2c. SNMPv3 uses USM |

| | |
|---|---|
| | for authentication and privacy and the community string will be associated with SNMPv3 community table. |
| **Engine ID** | Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users. |

## 1.6.2 Trap

### SNMP Trap Detailed Configuration

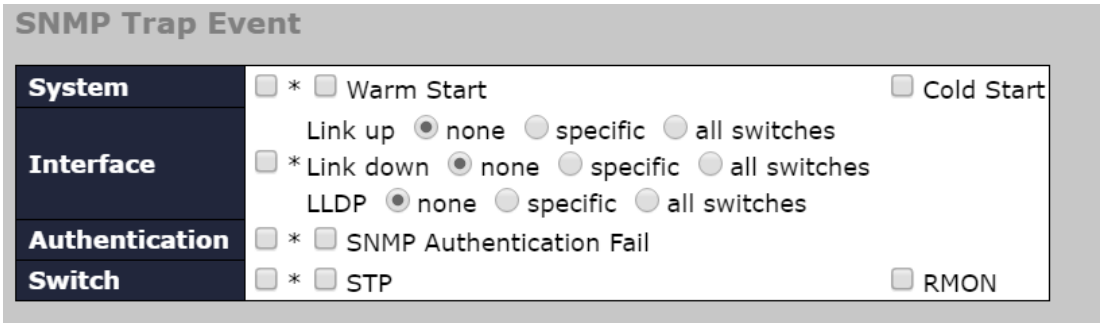
| | |
|---|---|
| **Trap Config Name** | |
| **Trap Mode** | Disabled ▼ |
| **Trap Version** | SNMP v2c ▼ |
| **Trap Community** | Public |
| **Trap Destination Address** | |
| **Trap Destination Port** | 162 |
| **Trap Inform Mode** | Disabled ▼ |
| **Trap Inform Timeout (seconds)** | 3 |
| **Trap Inform Retry Times** | 5 |
| **Trap Probe Security Engine ID** | Enabled ▼ |
| **Trap Security Engine ID** | |
| **Trap Security Name** | None ▼ |

| Label | Description |
|---|---|
| **Trap Config Name** | Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. |
| **Trap Mode** | Indicates existing SNMP trap mode. Possible modes include:<br>**Enabled**: enable SNMP trap mode<br>**Disabled**: disable SNMP trap mode |
| **Trap Version** | Indicates the supported SNMP trap version. Possible versions include:<br>**SNMP v1**: supports SNMP trap version 1<br>**SNMP v2c**: supports SNMP trap version 2c<br>**SNMP v3**: supports SNMP trap version 3 |
| **Trap Community** | Indicates the community access string when sending SNMP trap packets. The allowed string length is 0 to 255, and only ASCII characters from 33 to 126 are allowed. |

| | |
|---|---|
| **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 allows 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'. |
| **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. Possible modes include:<br>**Enabled**: enable SNMP trap inform mode<br>**Disabled**: disable SNMP trap inform mode |
| **Trap Inform Timeout(seconds)** | Configures the SNMP trap inform timeout. The allowed range is 0 to 2147. |
| **Trap Inform Retry Times** | Configures the retry times for SNMP trap inform. The allowed range is 0 to 255. |
| **Trap Probe Secuirty 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** | Indicates the SNMP trap security name. SNMPv3 traps and informs |

| | |
|---|---|
| **Name** | using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled. |

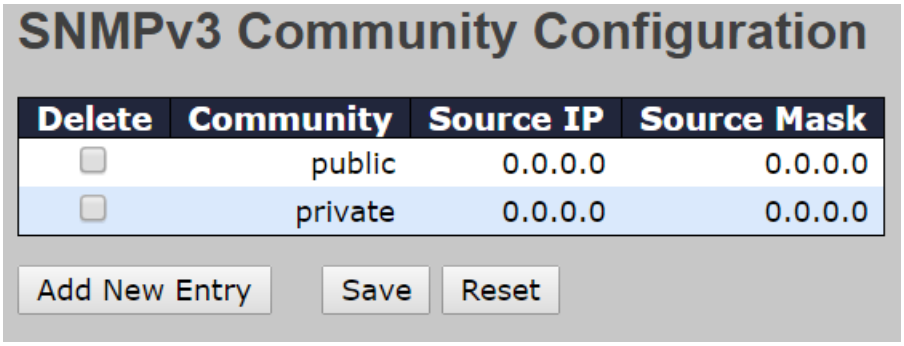
### SNMP Trap Event




| Label | Description |
|---|---|
| **System** | Enable/disable that the Interface group's traps. Possible traps are:<br>**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 the Switch group's traps. Possible traps are:<br>**STP**: Enable/disable STP trap.<br>**RMON**: Enable/disable RMON trap. |

## 1.6.3 SNMP Community Configurations

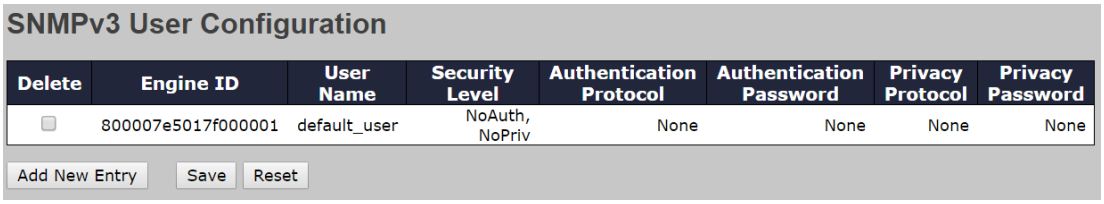
This page allows you to configure SNMPv3 community table. The entry index key is **Community**.




| Label | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Community** | Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed. |
| **Source IP** | Indicates the SNMP source address |
| **Source Mask** | Indicates the SNMP source address mask |

## 1.6.4 SNMP User Configurations

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

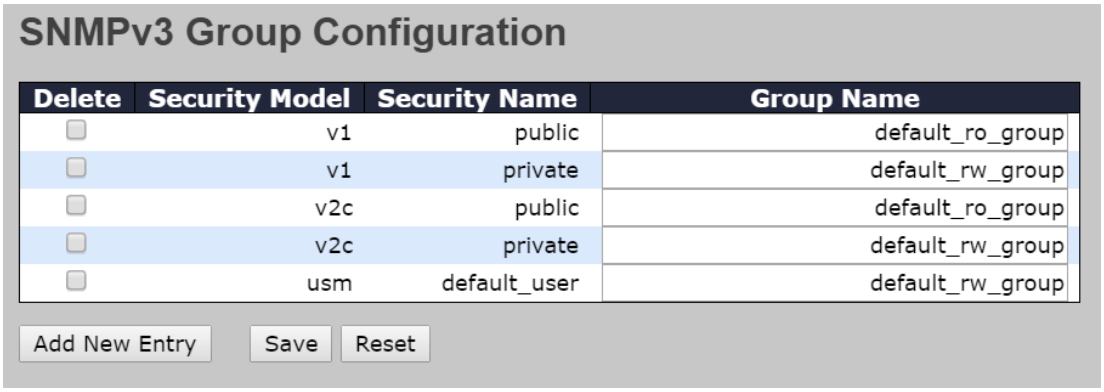



| Label | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Engine ID** | An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses User-based Security Model (USM) for message security and View-based Access Control Model (VACM) for access control. For the USM entry, the **usmUserEngineID** and **usmUserName** are the entry 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 is the same as 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 only ASCII characters from 33 to 126 are allowed. |
| **Security Level** | Indicates the security model that this entry should belong to. Possible security models include:<br>**NoAuth, NoPriv**: no authentication and none privacy<br>**Auth, NoPriv**: Authentication and no privacy<br>**Auth, Priv**: Authentication and privacy<br>The value of security level cannot be modified if the entry already exists, which means the value must be set correctly at the time of entry creation. |
| **Authentication Protocol** | Indicates the authentication protocol that this entry should belong to. Possible authentication protocols include:<br>**None**: no authentication protocol<br>**MD5**: an optional flag to indicate that this user is using MD5 authentication protocol<br>**SHA**: an optional flag to indicate that this user is using SHA authentication protocol<br>The value of security level cannot be modified if the entry already exists, which means the value must be set correctly at the time of entry creation. |
| **Authentication Password** | A string identifying the authentication pass 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. Only ASCII characters from 33 to 126 are allowed. |
| **Privacy Protocol** | Indicates the privacy protocol that this entry should belong to. Possible privacy protocols include:<br>**None**: no privacy protocol<br>**DES**: an optional flag to indicate that this user is using DES authentication protocol |
| **Privacy Password** | A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and only ASCII characters from 33 to 126 are allowed. |

### 1.6.5 SNMP Group Configurations

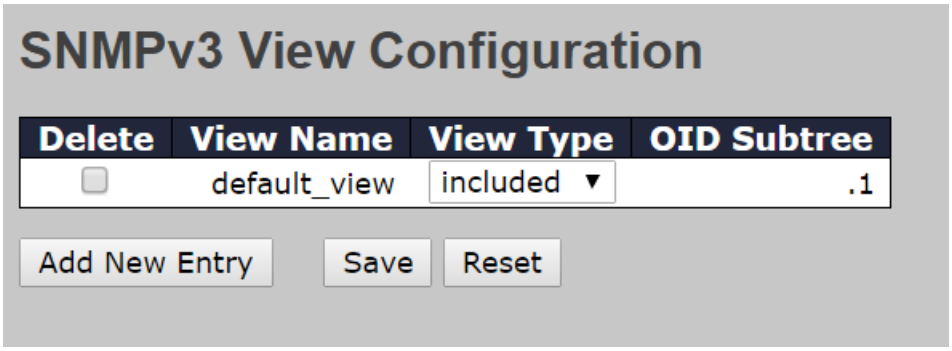
This page allows you to configure SNMPv3 group table. The entry index keys are **Security Model** and **Security Name**.




| Label | 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 included:<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 only ASCII characters from 33 to 126 are allowed. |
| **Group Name** | A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed. |

### 1.6.6 SNMP View Configurations

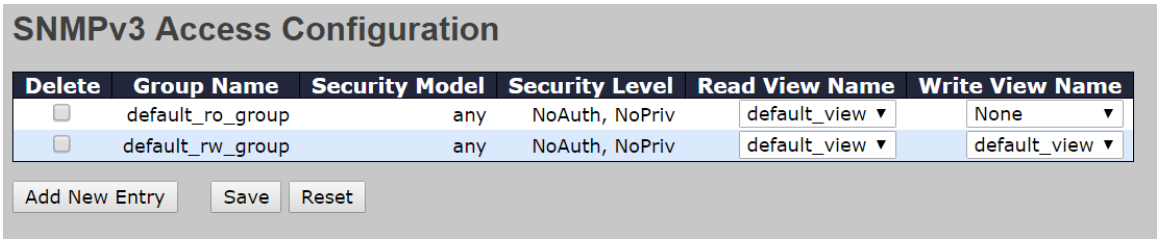
This page allows you to configure SNMPv3 view table. The entry index keys are **View Name** and **OID Subtree**.



| Label | 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 only ASCII characters from 33 to 126 are allowed. |
| **View Type** | Indicates the view type that this entry should belong to. Possible view types include:<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>Generally, if an entry's view type is **Excluded**, it should exist another entry whose view type is **Included, and** its OID subtree oversteps the **Excluded** 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 (*). |

## 1.6.7 SNMP Access Configurations

This page allows you to configure SNMPv3 access table. The entry index keys are **Group Name**, **Security Model**, and **Security Level**.

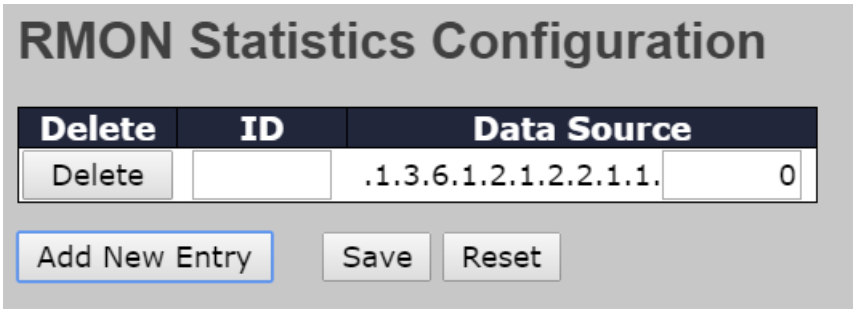



| Label | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Group Name** | A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed. |
| **Security Model** | Indicates the security model that this entry should belong to. Possible security models include:<br>**any**: Accepted any security model (v1\|v2c\|usm). |

| | |
|---|---|
| | **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 include:<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 only ASCII characters from 33 to 126 are allowed. |
| **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 only ASCII characters from 33 to 126 are allowed. |

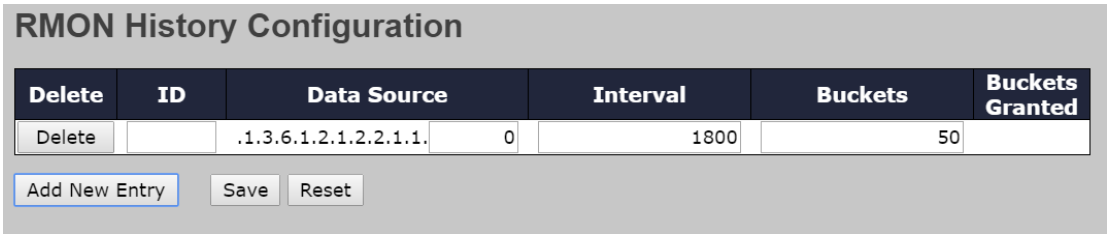
## 1.6.8 RMON

### Statistics Configuration




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

### History Configuration




| Label | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **ID** | Indicates the index of the entry. The range is from 1 to 65535. |
| **Data Source** | Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005. |
| **Interval** | Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds. |
| **Buckets** | Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50. |
| **Buckets Granted** | The number of data shall be saved in the RMON. |

## Alarm Configuration

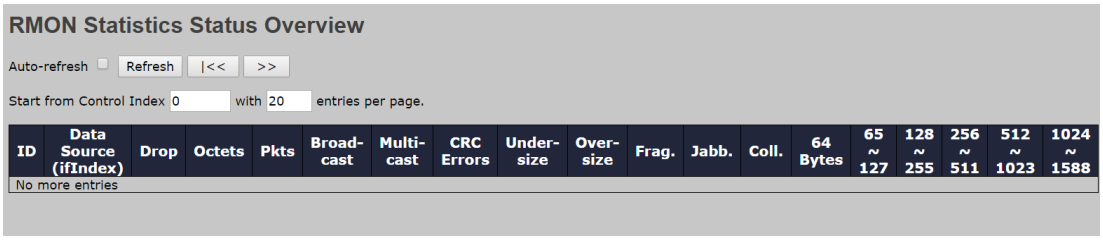

| Label | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **ID** | Indicates the index of the entry. The range is from 1 to 65535. |
| **Interval** | Indicates the interval in seconds for sampling and comparing the rising and falling threshold. 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 even the packets are 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). |
| **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** | Rising event index (1-65535). |
| **Falling Threshold** | Falling threshold value (-2147483648-2147483647) |
| **Falling Index** | Falling event index (1-65535). |

## Event Configuration


| Label | 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** | 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. |

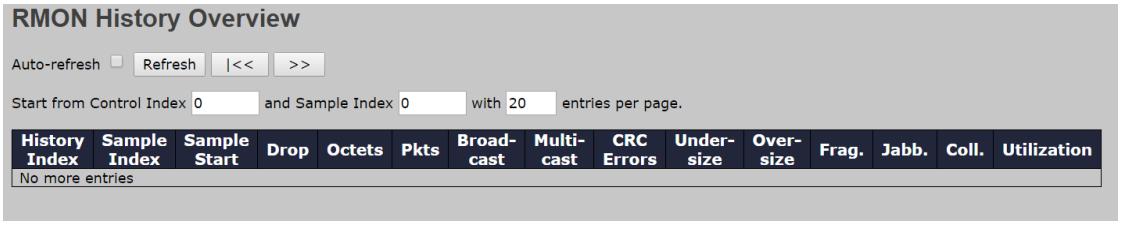
## Statistics Stauts




| Label | Description |
|---|---|
| **ID** | Indicates the index of Statistics entry. |
| **Data Source** | The port ID which wants to be monitored. |
| **Octets** | The total number of events in which packets were dropped by the probe due to lack of resources. |
| **Pkts** | The total number of packets (including bad packets, broadcast packets, and multicast packets) received. |

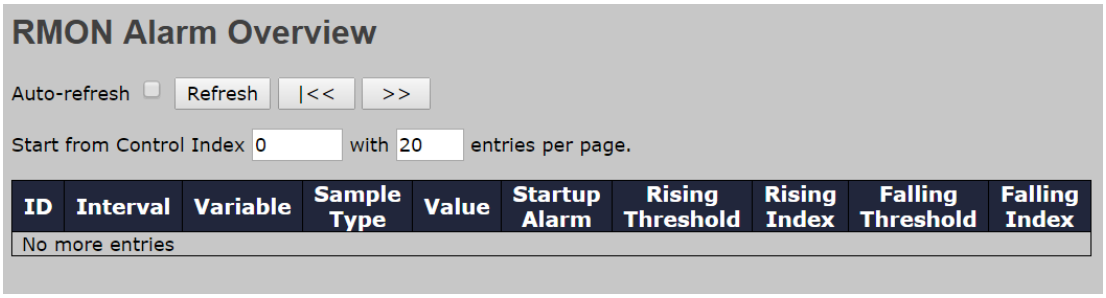
| | |
|---|---|
| **Broad-Cast** | The total number of good packets received that were directed to the broadcast address. |
| **Muulti-Cast** | The total number of good packets received that were directed to a multicast address. |
| **CRC Errors** | The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). |
| **Under-size** | The total number of packets received that were less than 64 octets. |
| **Over-size** | The total number of packets received that were longer than 1518 octets. |
| **Frag** | The number of frames which size is less than 64 octets received with invalid CRC. |
| **Jabb** | The number of frames which size is larger than 64 octets received with invalid CRC. |
| **Coll.** | The best estimate of the total number of collisions on this Ethernet segment. |
| **64** | The total number of packets (including bad packets) received that were 64 octets in length. |
| **65~127** | The total number of packets (including bad packets) received that are between 65 to 127 octets in length. |
| **128~255** | The total number of packets (including bad packets) received that are between 128 to 255 octets in length. |
| **256~511** | The total number of packets (including bad packets) received that are between 256 to 511 octets in length. |
| **512~1023** | The total number of packets (including bad packets) received that are between 512 to 1023 octets in length. |
| **1024~1588** | The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length. |

## History Status



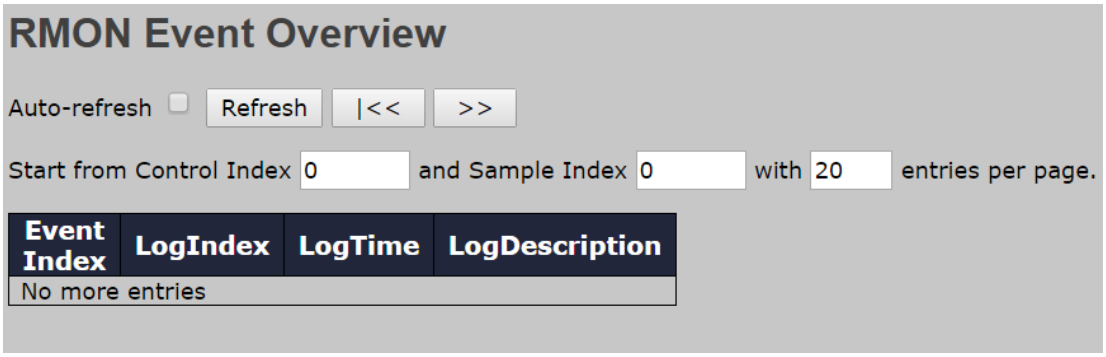
| Label | Description |
|---|---|
| **History Index** | Indicates the index of History control entry. |
| **Sample Index** | Indicates the index of the data entry associated with the control entry. |
| **Sample Start** | The value of sysUpTime at the start of the interval over which this sample was measured. |
| **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. |
| **CRC Error** | The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). |
| **Undersize** | The total number of packets received that were less than 64 octets. |
| **Oversize** | The total number of packets received that were longer than 1518 octets. |
| **Frag.** | The number of frames which size is less than 64 octets received with invalid CRC. |
| **Jabb.** | The total number of packets received that were longer than 1518 octets. |
| **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. |

## Alarm Status




| Label | 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 threshold value. |
| **Filing Threshold** | Falling threshold value. |
| **Falling Index** | Falling event index. |

## Event Status




| Label | 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 |
| **LogDescripi** | Indicates the Event description. |

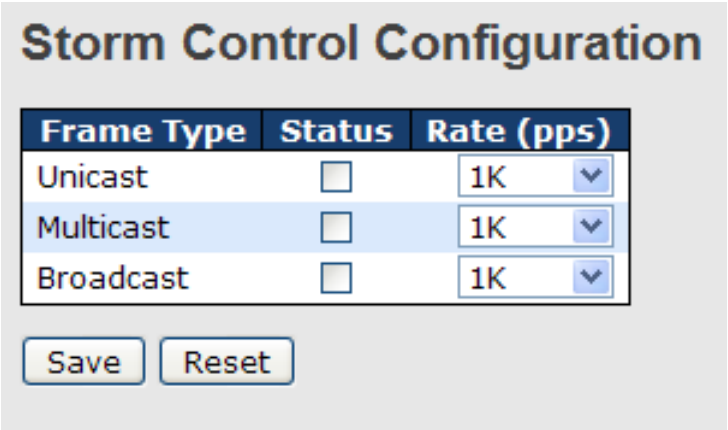
# 1.7 Traffic Prioritization

## 1.7.1 Storm Control

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 rate is 2^n, where n is equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilopackets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

Note: frames sent to the CPU of the switch are always limited to approximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.

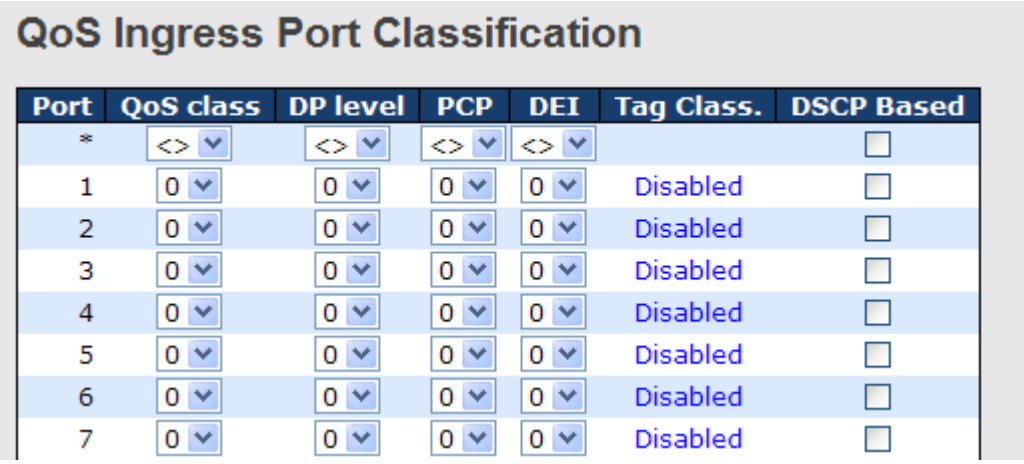



| Label | Description |
|---|---|
| **Frame Type** | The settings in a particular row apply to the frame type listed here: **unicast**, **multicast**, or **broadcast**. |
| **Status** | Enable or disable the storm control status for the given frame type. |

| | |
|---|---|
| **Rate** | The rate unit is packet per second (pps), configure the rate as 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K.<br>The 1 kpps is actually 1002.1 pps. |

## 1.7.2 Port Classification

QoS is an acronym for Quality of Service. It is a method to achieve efficient bandwidth utilization between individual applications or protocols.




| Label | Description |
|---|---|
| **Port** | The port number for which the configuration below applies |
| **QoS Class** | Controls the default QoS class<br>All frames are classified to a QoS class. There is a one to one mapping between QoS class, queue, and priority. A QoS class of 0 (zero) has the lowest priority.<br>If the port is VLAN aware and the frame is tagged, then the frame is classified to a QoS class that is based on the PCP value in the tag as shown below. Otherwise the frame is classified to the default QoS class.<br>PCP value: 0 1 2 3 4 5 6 7<br>QoS class: 1 0 2 3 4 5 6 7<br>If the port is VLAN aware, the frame is tagged, and Tag Class is enabled, then the frame is classified to a QoS class that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default QoS class.<br>The classified QoS class can be overruled by a QCL entry.<br>Note: if the default QoS class has been dynamically changed, then the actual default QoS class is shown in parentheses after |

| | |
|---|---|
| | the configured default QoS class. |
| **DP level** | Controls the default Drop Precedence Level<br>All frames are classified to a DP level.<br>If the port is VLAN aware and the frame is tagged, then the frame is classified to a DP level that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DP level.<br>If the port is VLAN aware, the frame is tagged, and Tag Class is enabled, then the frame is classified to a DP level that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DP level.<br>The classified DP level 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. |
| **Tag Class** | Shows the classification mode for tagged frames on this port<br>**Disabled**: Use default QoS class and DP level for tagged frames<br>**Enabled**: Use mapped versions of PCP and DEI for tagged frames<br>Click on the mode 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 QoS class and DP level. |
| **DSCP Based** | Click to enable DSCP Based QoS Ingress Port Classification |

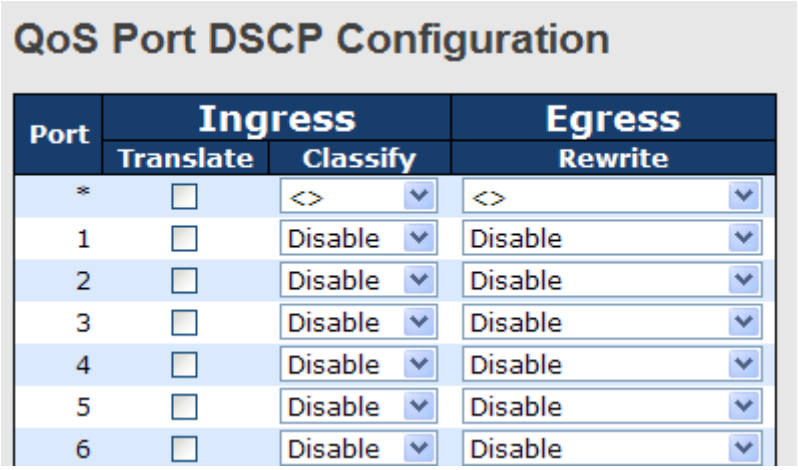
### 1.7.3 Port Tag Remaking

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


| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied. Click on the port number 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 |

## 1.7.4 Port DSCP

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

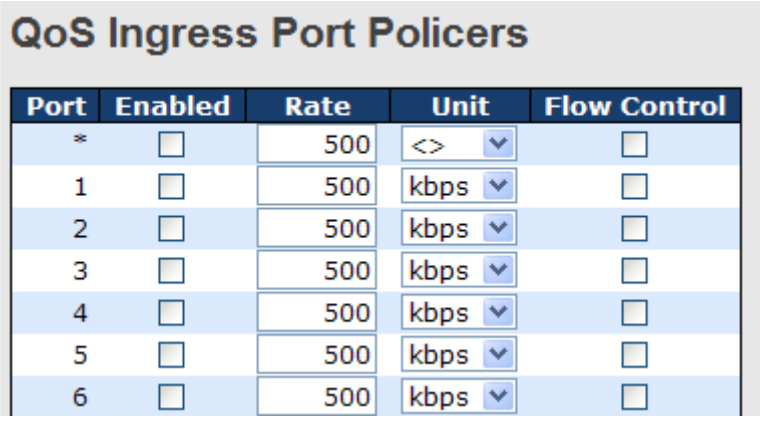



| Label | Description |
|---|---|
| **Port** | Shows the list of ports for which you can configure DSCP Ingress and Egress settings. |
| **Ingress** | In **Ingress** settings you can change ingress translation and classification settings for individual ports.<br>There are two configuration parameters available in Ingress:<br>1. **Translate**<br>2. **Classify** |

| | |
|---|---|
| **1. Translate** | Check to enable ingress translation |
| **2. Classify** | Classification has 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 whose 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 the following options:<br>**Disable**: no Egress rewrite<br>**Enable**: rewrite enabled without remapping<br>**Remap DP Unaware**: DSCP from the analyzer is remapped and the frame is remarked with a remapped DSCP value. The remapped DSCP value is always taken from the '**DSCP Translation->Egress Remap DP0**' table.<br>**Remap DP Aware**: DSCP from the analyzer is remapped and the frame is remarked with a remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the '**DSCP Translation->Egress Remap DP0**' table or from the '**DSCP Translation->Egress Remap DP1**' table. |

## 1.7.5 Port Policing

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

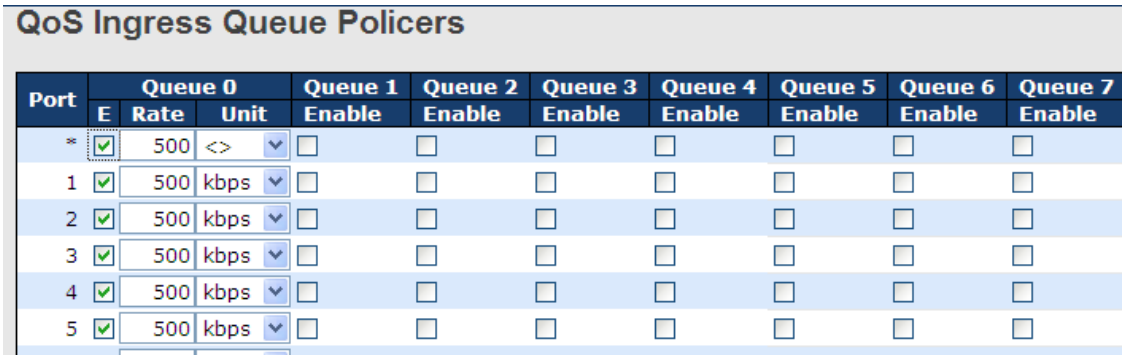



| Label | Description |
|---|---|

| | |
|---|---|
| **Port** | The port number for which the configuration below applies |
| **Enable** | Check to enable the policer for individual switch ports |
| **Rate** | Configures the rate of each policer. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps** or **fps**, and is restricted to 1 to 3300 when the **Unit** is **Mbps** or **kfps**. |
| **Unti** | Configures the unit of measurement for each 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 being discarded. |

## 1.7.6 Queue Policing

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

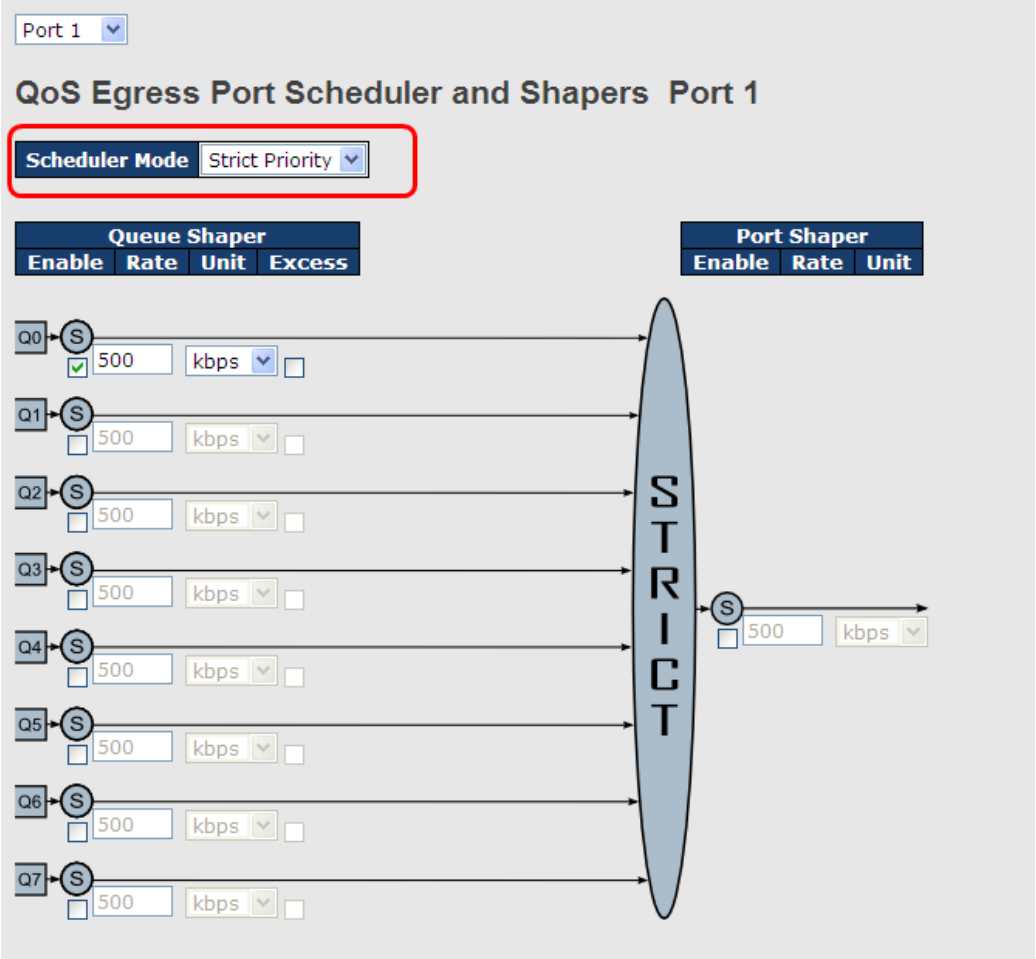



| Label | Description |
|---|---|
| **Port** | The port number for which the configuration below applies. |
| **Enable(E)** | Check to enable queue policer for individual switch ports |
| **Rate** | Configures the rate of each queue policer. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and is restricted to 1 to 3300 when the **Unit** is **Mbps**.<br>This field is only shown if at least one of the queue policers is enabled. |
| **Unit** | Configures the unit of measurement for each queue policer rate as kbps or Mbps. The default value is **kbps**.<br>This field is only shown if at least one of the queue policers is enabled. |

## 1.7.7 QoS Egress Port Scheduler and Shapers

This page allows you to configure Scheduler and Shapers for a specific port.

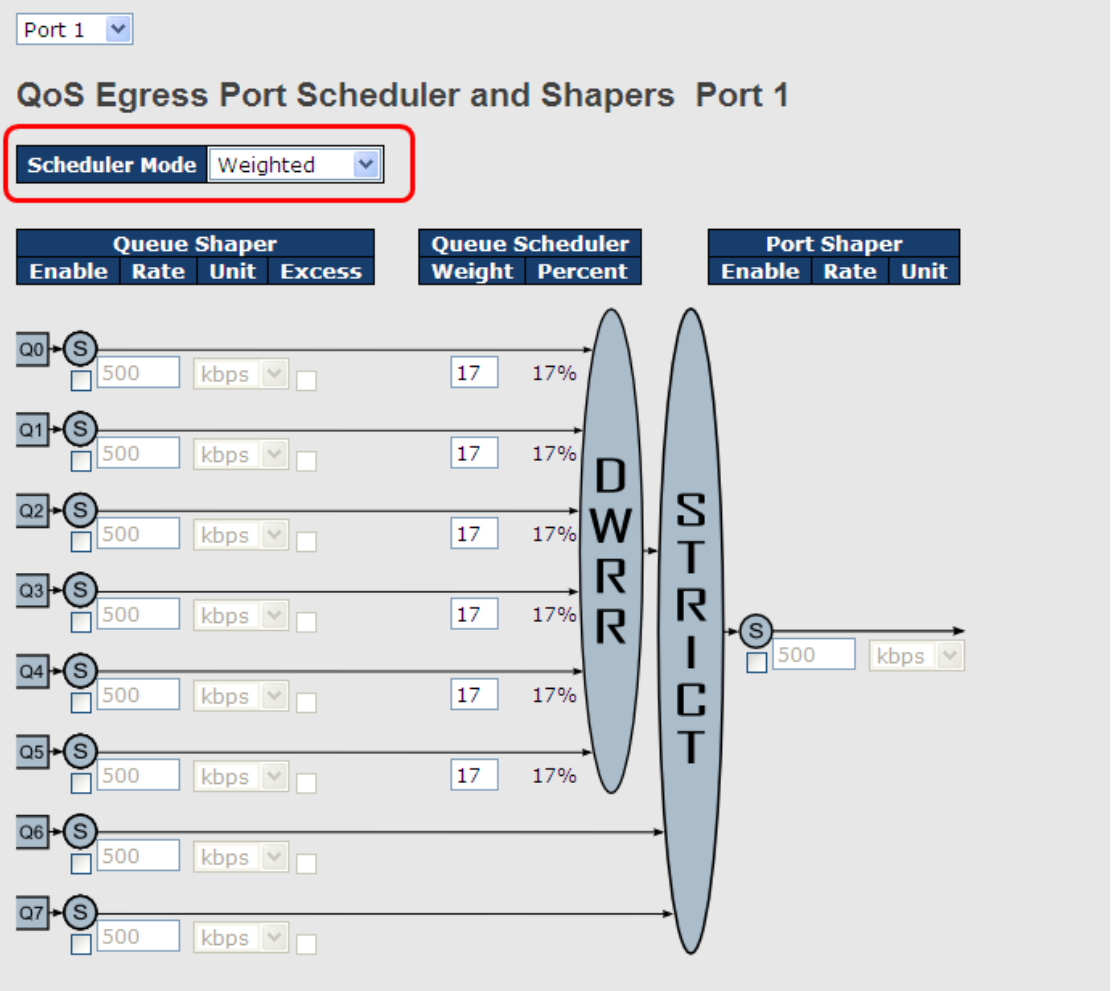
## Strict Priority




| Label | Description |
|---|---|
| **Scheduler Mode** | Controls whether the scheduler mode is **Strict Priority** or **Weighted** on this switch port |
| **Queue Shaper Enable** | Check to enable queue shaper for individual switch ports |
| **Queue Shaper Rate** | Configures the rate of each queue shaper. The default value is **500**. This value is restricted to 100 to 1000000 whn the **Unit** is **kbps**", and it is restricted to 1 to 3300 when the **Unit** is **Mbps**. |
| **Queues Shaper Unit** | Configures the rate for each queue shaper. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**. |
| **Queue Shaper Excess** | Allows the queue to use excess bandwidth |

| | |
|---|---|
| **Port Shaper Enable** | Check to enable port shaper for individual switch ports |
| **Port Shaper Rate** | Configures the rate of each port shaper. The default value is **500** This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**. |
| **Port Shaper Unit** | Configures the unit of measurement for each port shaper rate as **kbps** or **Mbps**. The default value is **kbps**. |

## Weighted

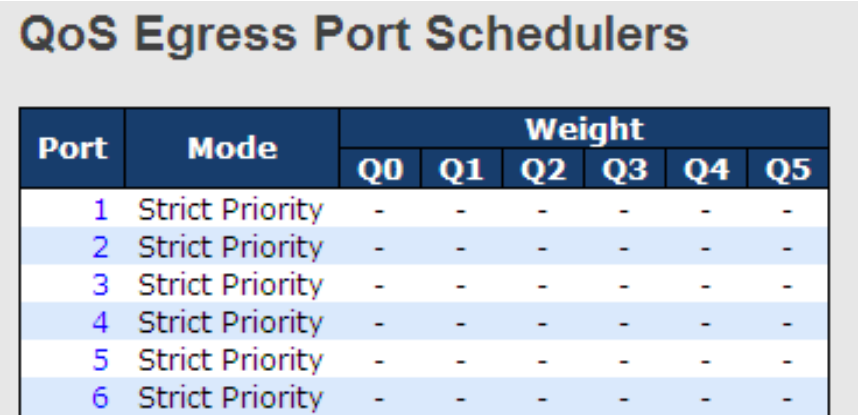



| Label | Description |
|---|---|
| **Scheduler Mode** | Controls whether the scheduler mode is **Strict Priority** or **Weighted** on this switch port |
| **Queue Shaper Enable** | Check to enable queue shaper for individual switch ports |
| **Queue Shaper Rate** | Configures the rate of each queue shaper. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is |

| | |
|---|---|
| | **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**. |
| **Queues Shaper Unit** | Configures the rate of each queue shaper. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit**" is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**. |
| **Queue Shaper Excess** | Allows the queue to use excess bandwidth |
| **Queue Scheduler Weight** | Configures the weight of each queue. The default value is **17**. This value is restricted to 1 to 100. This parameter is only shown if **Scheduler Mode** is set to **Weighted**. |
| **Queue Scheduler Percent** | Shows the weight of the queue in percentage. This parameter is only shown if **Scheduler Mode** is set to **Weighted**. |
| **Port Shaper Enable** | Check to enable port shaper for individual switch ports |
| **Port Shaper Rate** | Configures the rate of each port shaper. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**. |
| **Port Shaper Unit** | Configures the unit of measurement for each port shaper rate as **kbps** or **Mbps**. The default value is **kbps**. |

## 1.7.8 Port Scheduler

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



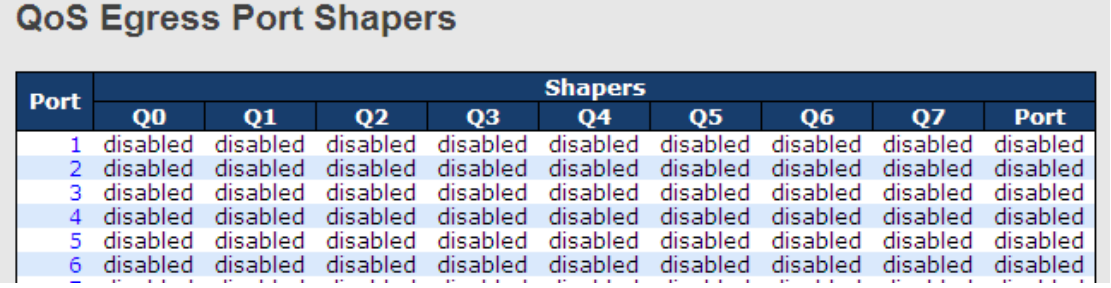
QoS Egress Port Schedulers

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

| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied.<br>Click on the port number to configure the schedulers |
| **Mode** | Shows the scheduling mode for this port |
| **Qn** | Shows the weight for this queue and port |

## 1.7.9 Port Shaping

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



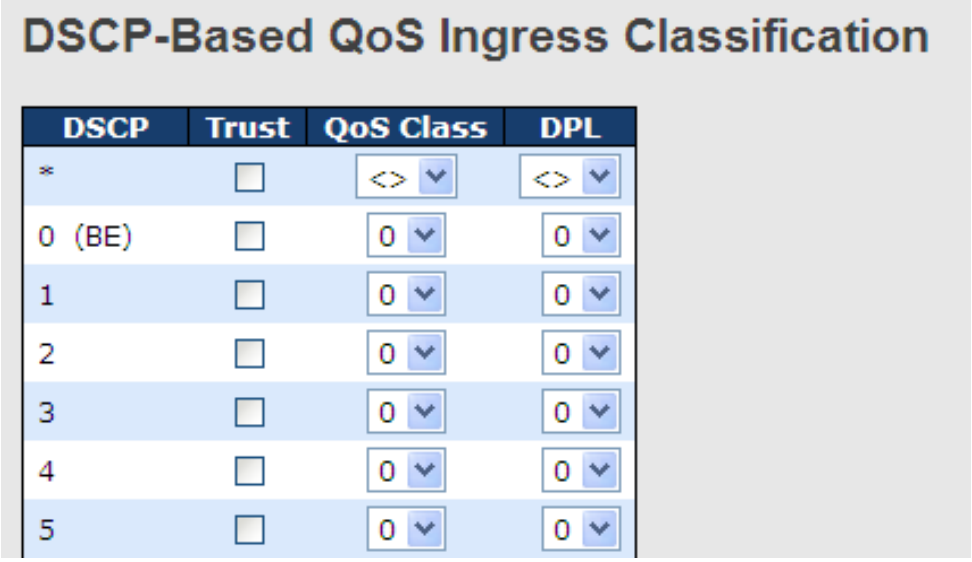
QoS Egress Port Shapers

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

| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied. Click on the port number to configure the shapers |
| **Mode** | Shows **disabled** or actual queue shaper rate - e.g. "800 Mbps" |
| **Qn** | Shows **disabled** or actual port shaper rate - e.g. "800 Mbps" |

## 1.7.10 DSCP-Based QoS

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



DSCP-Based QoS Ingress Classification

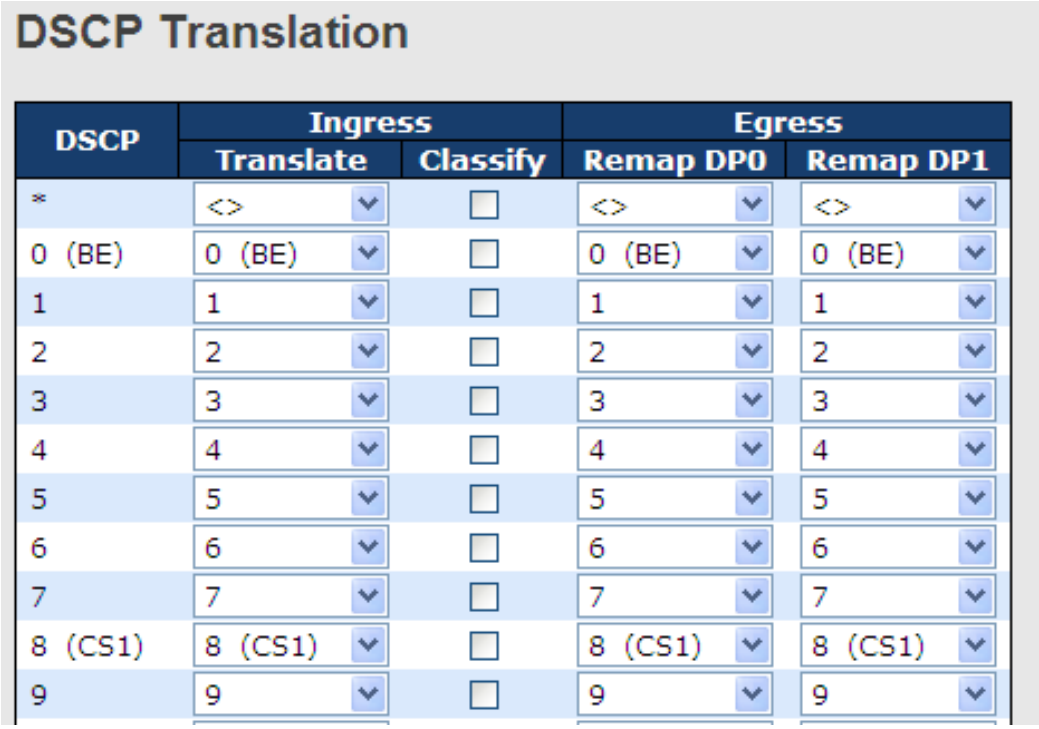
| DSCP | Trust | QoS Class | DPL |
|---|---|---|---|
| * | ☐ | <> | <> |
| 0 (BE) | ☐ | 0 | 0 |
| 1 | ☐ | 0 | 0 |
| 2 | ☐ | 0 | 0 |
| 3 | ☐ | 0 | 0 |
| 4 | ☐ | 0 | 0 |
| 5 | ☐ | 0 | 0 |

| Label | Description |
|---|---|
| **DSCP** | Maximum number of supported DSCP values is 64 |
| **Trust** | Check to trust a specific DSCP value. Only frames with trusted DSCP values are mapped to a specific QoS class and drop precedence level. Frames with untrusted DSCP values are treated as a non-IP frame. |

| | |
|---|---|
| **QoS Class** | QoS class value can be any number from 0-7. |
| **DPL** | Drop Precedence Level (0-1) |

## 1.7.11 DSCP Translation

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

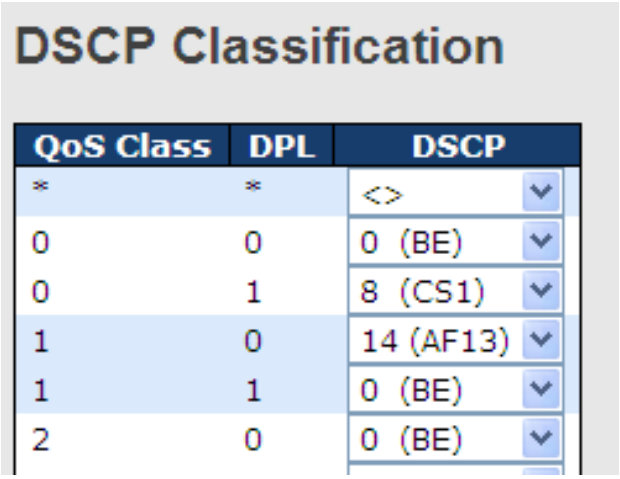



| Label | Description |
|---|---|
| **DSCP** | Maximum number of supported DSCP values is 64 and valid DSCP value ranges from 0 to 63. |
| **Ingress** | Ingress DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.<br>There are two configuration parameters for DSCP Translation -<br>1. **Translate:** DSCP can be translated to any of (0-63) DSCP values.<br>2. **Classify:** check to enable ingress classification |
| **Egress** | Configurable engress parameters include;<br>**Remap DP0**: controls the remapping for frames with DP level 0. You can select the DSCP value from a selected menu to |

| | |
|---|---|
| | which you want to remap. DSCP value ranges from 0 to 63.<br>**Remap DP1**: controls the remapping for frames with DP level 1. You can select the DSCP value from a selected menu to which you want to remap. DSCP value ranges from 0 to 63. |

## 1.7.12 DSCP Classification

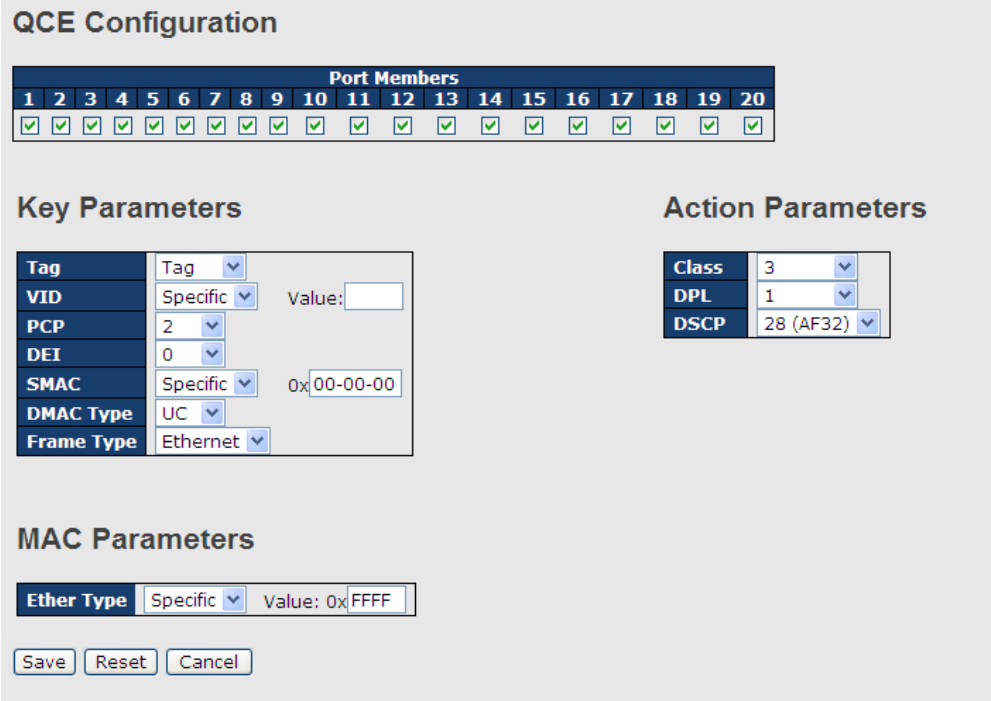
This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.




| Label | Description |
|---|---|
| **QoS Class** | Actual QoS class |
| **DPL** | Actual Drop Precedence Level |
| **DSCP** | Select the classified DSCP value (0-63) |

## 1.7.13 QoS Control List

This page allows you to edit or insert a single QoS control entry at a time. A QCE consists of several parameters. These parameters vary with the frame type you select.



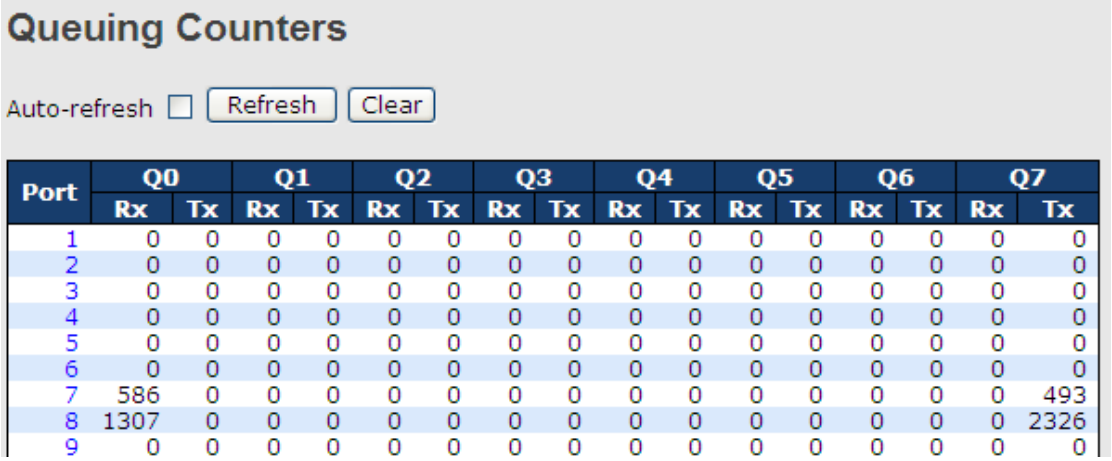

| Label | Description |
|---|---|
| Port Members | Check to include the port in the QCL entry. By default, all ports are included. |
| Key Parameters | Key configurations include:<br>**Tag**: value of tag, can be **Any**, **Untag** or **Tag**.<br>**VID**: valid value of VLAN ID, can be any value from 1 to 4095 **Any**: user can enter either a specific value or a range of VIDs.<br>**PCP**: Priority Code Point, can be specific numbers (0, 1, 2, 3, 4, 5, 6, 7), a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or **Any**<br>**DEI**: Drop Eligible Indicator, can be any of values between 0 and 1 or **Any**<br>**SMAC**: Source MAC Address, can be 24 MS bits (OUI) or **Any**<br>**DMAC Type**: Destination MAC type, can be **unicast** (**UC**), **multicast** (**MC**), **broadcast** (**BC**) or **Any**<br>Frame Type can be the following values:<br>**Any**<br>**Ethernet**<br>**LLC**<br>**SNAP**<br>**IPv4** |

| | |
|---|---|
| | **IPv6**<br>Note: all frame types are explained below. |
| Any | Allow all types of frames |
| Ethernet | Valid Ethernet values can range from 0x600 to 0xFFFF or Any' but excluding 0x800(IPv4) and 0x86DD(IPv6). The default value is **Any**. |
| LLC | SSAP Address: valid SSAP (Source Service Access Point) values can range from 0x00 to 0xFF or **Any**. The default value is **Any**.<br>DSAP Address: valid DSAP (Destination Service Access Point) values can range from 0x00 to 0xFF or **Any**. The default value is **Any**.<br>Control Valid Control: valid values can range from 0x00 to 0xFF or **Any**. The default value is **Any**. |
| SNAP | PID: valid PID (a.k.a ethernet type) values can range from 0x00 to 0xFFFF or Any. The default value is Any. |
| 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 of x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the 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>DSCP (Differentiated Code Point): can be a specific value, a range, or **Any**. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.<br>IP Fragment: Ipv4 frame fragmented options include **'yes'**, **'no'**, and **'any'**.<br>Sport Source TCP/UDP Port: (0-65535) or **Any**, specific value or port range applicable for IP protocol UDP/TCP<br>Dport Destination TCP/UDP Port: (0-65535) or **Any**, specific value or port range applicable for IP protocol UDP/TCP |
| IPv6 | Protocol IP protocol number: (0-255, TCP or UDP) or **Any**<br>Source IP IPv6 source address: (a.b.c.d) or **Any**, 32 LS bits<br>DSCP (Differentiated Code Point): can be a specific value, a range, 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 |

| | |
|---|---|
| | value or port range applicable for IP protocol UDP/TCP<br>Dport Destination TCP/UDP port: (0-65535) or **Any**, specific value or port range applicable for IP protocol UDP/TCP |
| Action Parameters | Class QoS class: (0-7) or **Default**<br>Valid Drop Precedence Level value can be (0-1) or **Default**.<br>Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or **Default**.<br>Default means that the default classified value is not modified by this QCE. |

## 1.7.14 QoS Statistics

This page provides the statistics of individual queues for all switch ports.



Queuing Counters

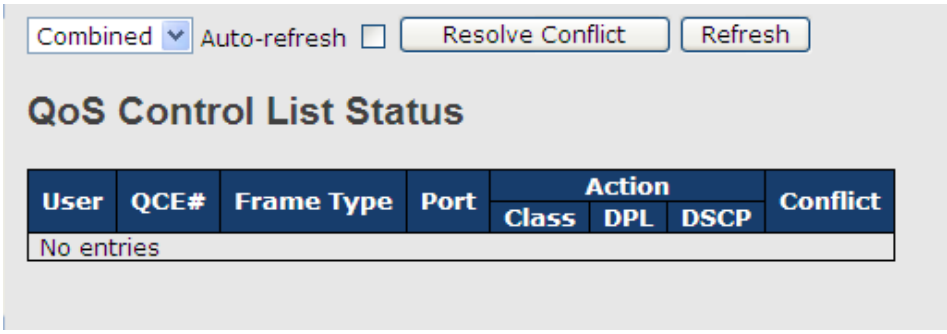
Auto-refresh ☐ Refresh Clear

| 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 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 586 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 493 |
| 8 | 1307 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2326 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied. |
| **Qn** | There are 8 QoS queues per port. Q0 is the lowest priority |
| **Rx / Tx** | The number of received and transmitted packets per queue |

## 1.7.15 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.

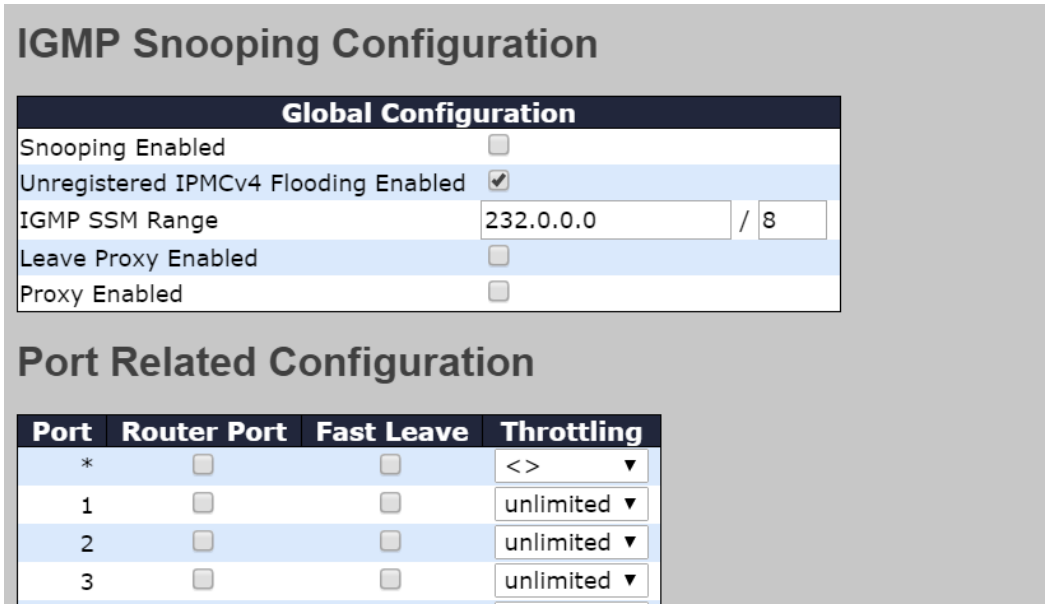



| Label | Description |
|---|---|
| **User** | Indicates the QCL user |
| **QCE#** | Indicates the index of QCE |
| **Frame Type** | Indicates the type of frame to look for incoming frames. Possible frame types are:<br>**Any**: the QCE will match all frame type.<br>**Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.<br>**LLC**: Only (LLC) frames are allowed.<br>**SNAP**: Only (SNAP) frames are allowed.<br>**IPv4**: the QCE will match only IPV4 frames.<br>**IPv6**: the QCE will match only IPV6 frames. |
| **Port** | Indicates the list of ports configured with the QCE. |
| **Action** | Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.<br>There are three action fields: **Class**, **DPL**, and **DSCP**.<br>**Class**: Classified QoS; if a frame matches the QCE, it will be put in the queue.<br>**DPL**: Drop Precedence Level; if a frame matches the QCE, then DP level will set to a value displayed under DPL column.<br>**DSCP**: if a frame matches the QCE, then DSCP will be classified with the value displayed under DSCP column. |
| **Conflict** | Displays the conflict status of QCL entries. As hardware resources are shared by multiple applications, 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 hardware resources required to add the QCL entry by pressing Resolve Conflict button. |

# 1.8 Multicast

## 1.8.1 IGMP Snooping

This page provides IGMP Snooping related configurations.




| Label | Description |
|---|---|
| **Snooping Enabled** | Check to enable global IGMP snooping |
| **Unregistered IPMCv4Flooding 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.<br>Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range. |
| **Leaver Proxy Enabled** | Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side. |
| **Proxy Enable** | Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side. |
| **Router Port** | Specifies 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** | Check to enable fast leave on the port |

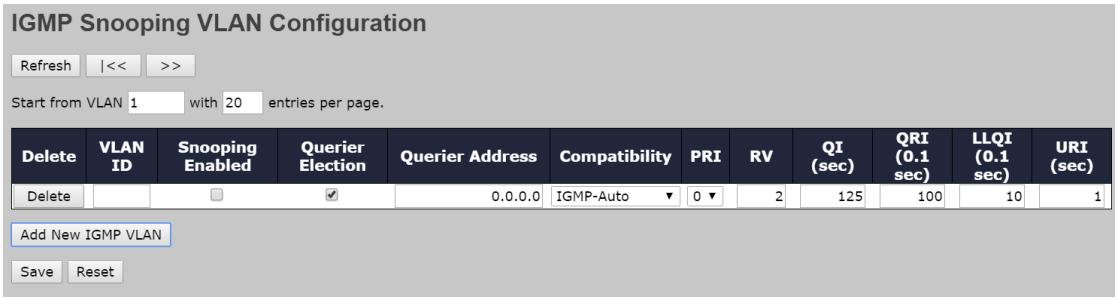
| | |
|---|---|
| **Throttling** | Enable to limit the number of multicast groups to which a switch port can belong. |

## VLAN Configurations of IGMP Snooping

Each page shows up to 99 entries from the VLAN table, with a default value of 20, selected by 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 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.

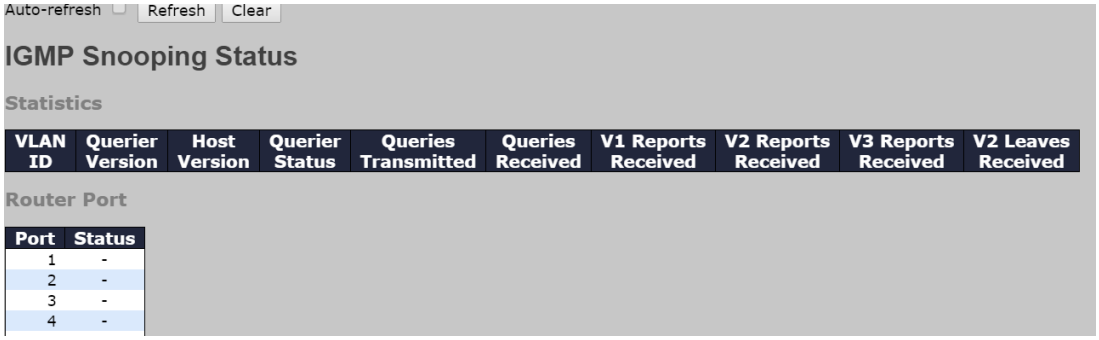



| Label | Description |
|---|---|
| **Delete** | Check to delete the entry. The designated entry will be deleted during the next save. |
| **VLAN ID** | The VLAN ID of the entry |
| **IGMP Snooping Enable** | Check to enable IGMP snooping for individual VLAN. Up to 32 VLANs can be selected. |
| **Querier Election** | Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier. |
| **Querier Address** | Define the IPv4 address as source address used in IP header for IGMP Querier election.<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. |

| | |
|---|---|
| **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.<br>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. |

## IGMP Snooping Status

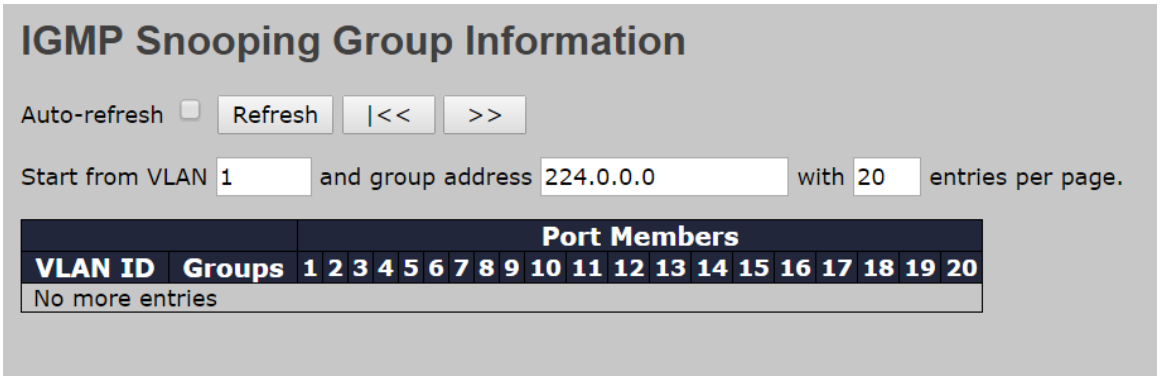
This page provides IGMP snooping status.




| Label | Description |
|---|---|
| **VLAN ID** | The VLAN ID of the entry |
| **Querier Version** | Active Querier version |
| **Host Version** | Active Host version |
| **Querier Status** | Shows the Querier status as **ACTIVE** or **IDLE** |
| **Querier Receive** | The number of transmitted Querier |
| **V1 Reports Receive** | The number of received V1 reports |
| **V2 Reports Receive** | The number of received V2 reports |
| **V3 Reports Receive** | The number of received V3 reports |
| **V2 Leave Receive** | The number of received V2 leave packets |
| **Refresh** | Click to refresh the page immediately |
| **Clear** | Clear all statistics counters |
| **Auto-refresh** | Check to enable an automatic refresh of the page at regular intervals |
| **Port** | Switch port number |
| **Status** | Indicates whether a specific port is a router port or not |

## Groups Information of IGMP Snooping

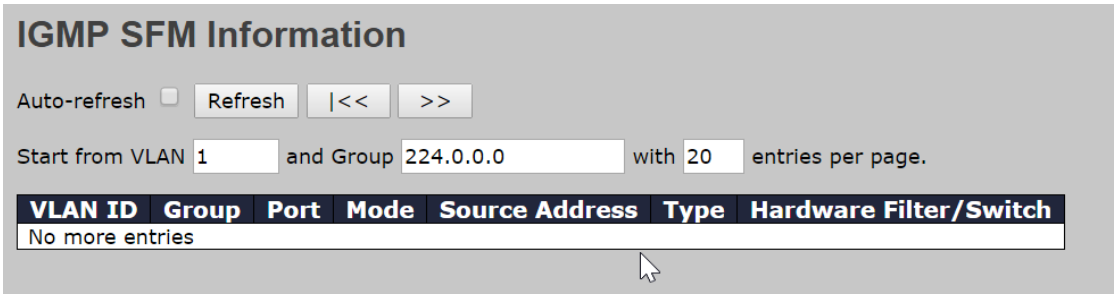
Entries in the **IGMP Group Table** are shown on this page. The **IGMP Group Table** is sorted first by VLAN ID, and then by group.




| Label | Description |
|---|---|
| **VLAN ID** | The VLAN ID of the group |
| **Groups** | The group address of the group displayed |
| **Port Members** | Ports under this group |

## IPv4 SFM Information

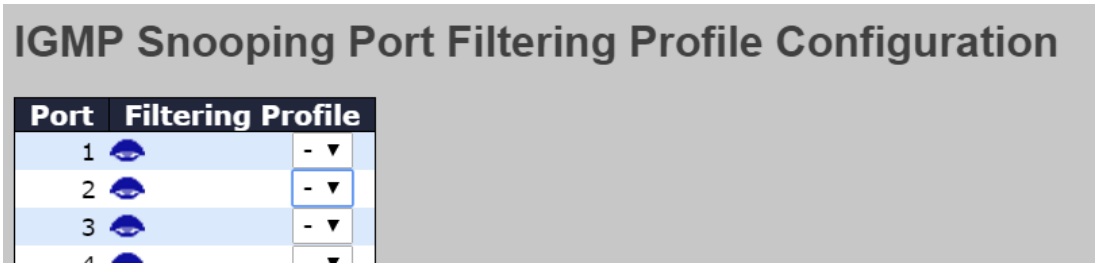
Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.




| Label | Description |
|---|---|
| **VLAN ID** | The VLAN ID of the group |
| **Groups** | The 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. |

### Port Group Filtering



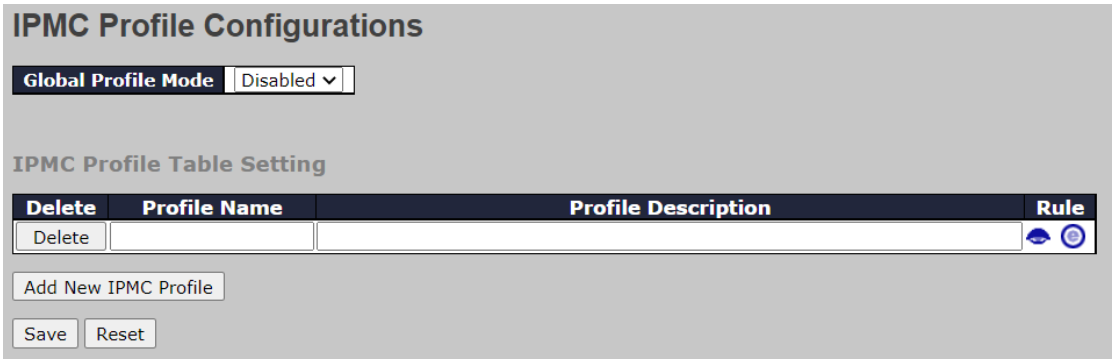

| Label | Description |
|---|---|
| Port | The logical port for the settings. |
| **Filtering Profile** | Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button. |
| **Profile Management Button** | You can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

## 1.8.2 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.

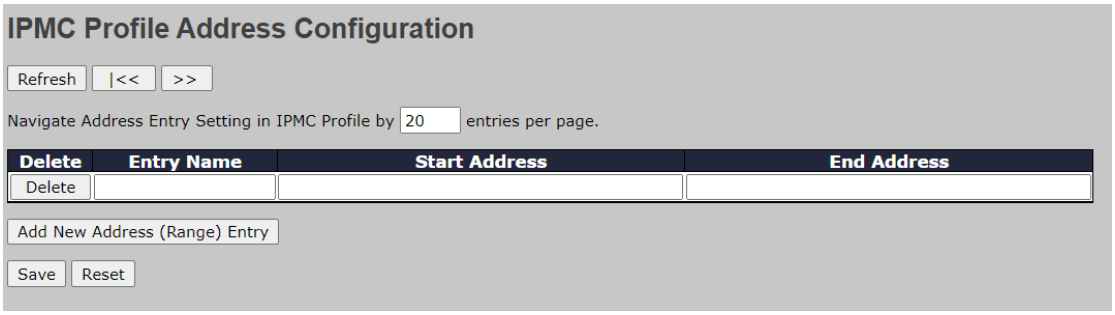


| Label | Description |
|---|---|
| **Global Profile Mode** | Enable/Disable the Global IPMC Profile.<br>System starts to do filtering based on profile settings only when the global profile mode is enabled. |
| **Delete** | Check to delete the entry.<br>The designated entry will be deleted during the 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. |

## 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.

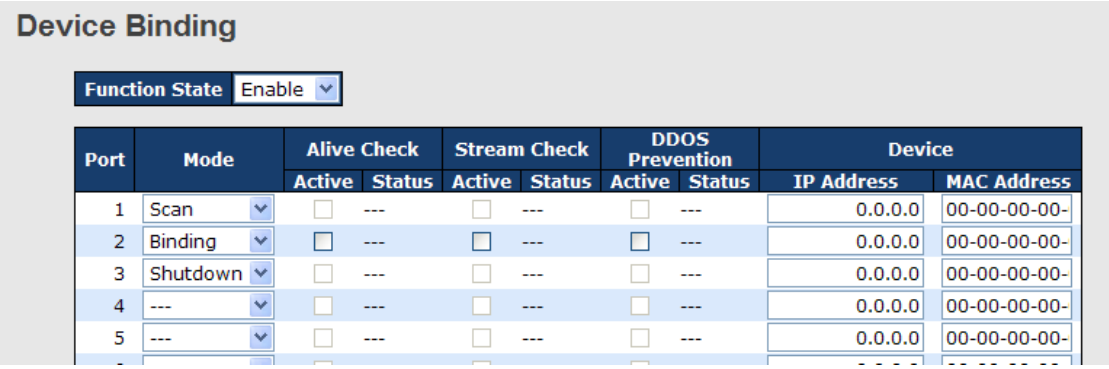


| Label | Description |
|---|---|
| **Delete** | Check to delete the entry.<br>The designated entry will be deleted during the next save. |
| **Entry Name** | The name used for indexing the address entry table.<br>Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric 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. |

# 1.9 Security

## 1.9.1 Device Binding

This page provides device binding configurations. Device binding is a powerful way to monitor devices and network security.



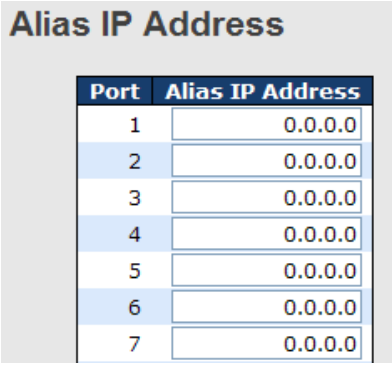

| Label | Description |
|---|---|
| **Mode** | Indicates the device binding operation for each port. Possible modes are:<br>**---**: disable<br>**Scan**: scans IP/MAC automatically, but no binding function<br>**Binding**: enables binding. Under this mode, any IP/MAC that does not match the entry will not be allowed to access the network.<br>**Shutdown**: shuts down the port (No Link) |
| **Alive Check Active** | Check to enable alive check. When enabled, switch will ping the device continually. |

| | |
|---|---|
| **Alive Check Status** | Indicates alive check status. Possible statuses are:<br>**---**: disable<br>**Got Reply**: receive ping reply from device, meaning the device is still alive<br>**Lost Reply**: not receiving ping reply from device, meaning the device might have been dead. |
| **Stream Check Active** | Check to enable stream check. When enabled, the switch will detect the stream change (getting low) from the device. |
| **Stream Check Status** | Indicates stream check status. Possible statuses are:<br>**---**: disable<br>**Normal**: the stream is normal.<br>**Low**: the stream is getting low. |
| **DDoS Prevention Acton** | Check to enable DDOS prevention. When enabled, the switch will monitor the device against DDOS attacks. |
| **DDoS Prevention Status** | Indicates DDOS prevention status. Possible statuses are:<br>**---**: disable<br>**Analyzing**: analyzes packet throughput for initialization<br>**Running**: analysis completes and ready for next move<br>**Attacked**: DDOS attacks occur |
| **Device IP Address** | Specifies IP address of the device |
| **Device MAC Address** | Specifies MAC address of the device |

# Advanced Configurations

## Alias IP Address

This page provides Alias IP Address configuration. Some devices might have more than one IP addresses. You could specify the other IP address here.

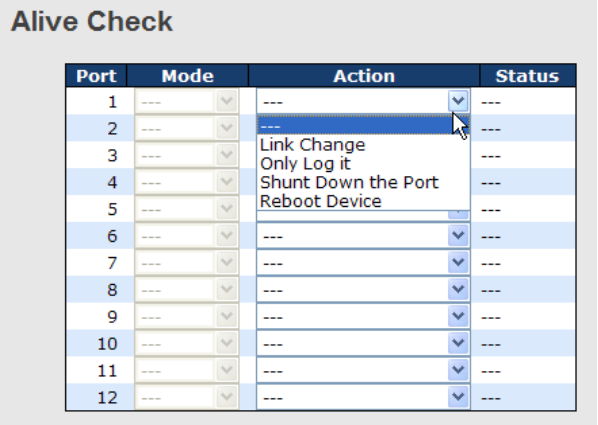



| Label | Description |
|---|---|

| | |
|---|---|
| **Alias IP Address** | Specifies alias IP address. Keep **0.0.0.0** if the device does not have an alias IP address. |

## Alive Check

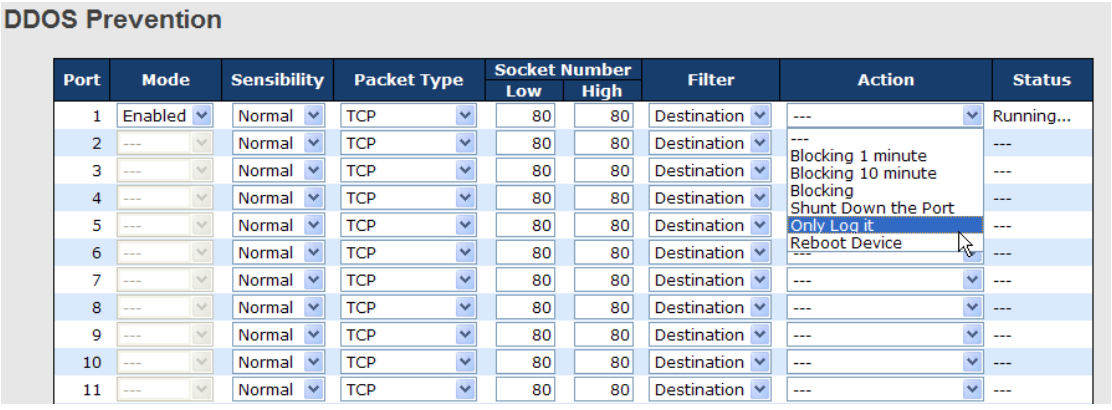
You can use ping commands to check port link status. If port link fails, you can set actions from the drop-down list.




| Label | Description |
|---|---|
| **Link Change** | Disables or enables the port |
| **Only log it** | Simply sends logs to the log server |
| **Shunt Down the Port** | Disables the port |
| **Reboot Device** | Disables or enables PoE power |

## DDoS Prevention

This page provides DDOS Prevention configurations. The switch can monitor ingress packets, and perform actions when DDOS attack occurred on this port. You can configure the setting to achieve maximum protection.

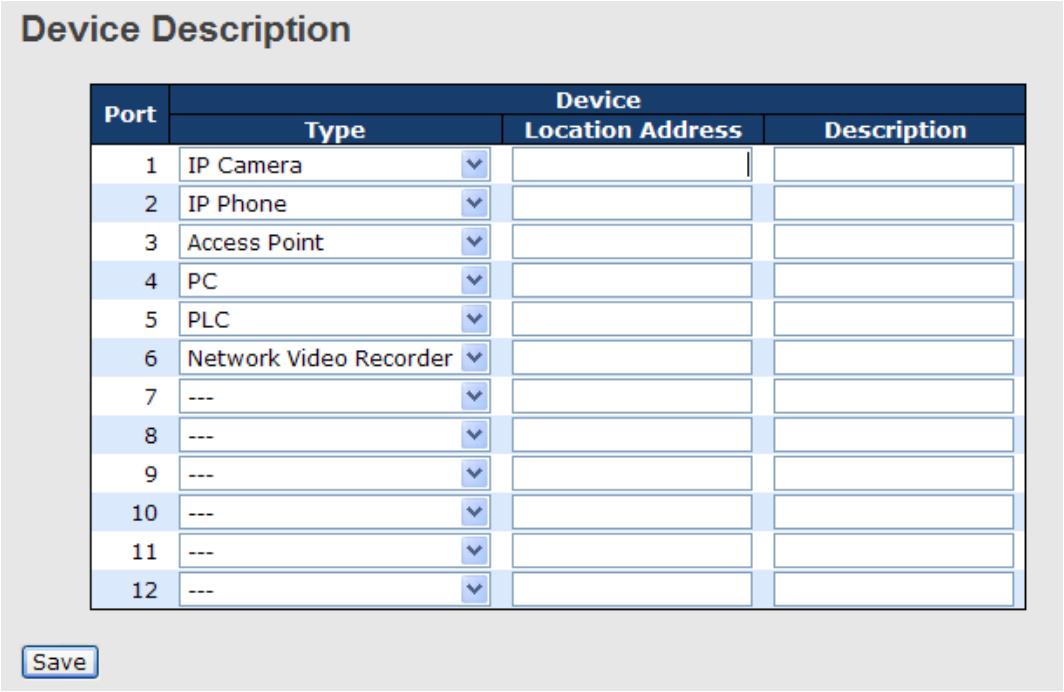


| Label | Description |
|---|---|
| **Mode** | Enables or disables DDOS prevention of the port |
| **Sensibility** | Indicates the level of DDOS detection. Possible levels are:<br>**Low**: low sensibility<br>**Normal**: normal sensibility<br>**Medium**: medium sensibility<br>**High**: high sensibility |
| **Packet Type** | Indicates the types of DDoS attack packets to be monitored. Possible types are:<br>**RX Total**: all ingress packets<br>**RX Unicast**: unicast ingress packets<br>**RX Multicast**: multicast ingress packets<br>**RX Broadcast**: broadcast ingress packets<br>**TCP**: TCP ingress packets<br>**UDP**: UDP ingress packets |
| **Socket Number** | If packet type is UDP (or TCP), please specify the socket number here. The socket number can be a range, from low to high. If the socket number is only one, please fill the same number in the low and high fields. |
| **Filter** | If packet type is UDP (or TCP), please choose the socket direction (**Destination**/**Source**). |
| **Action** | Indicates the action to take when DDOS attacks occur. Possible actions are:<br>**---**: no action<br>**Blocking 1 minute**: blocks the forwarding for 1 minute and log the event<br>**Blocking 10 minute**: blocks the forwarding for 10 minutes and log the event<br>**Blocking**: blocks and logs the event<br>**Shunt Down the Port**: shuts down the port (No Link) and logs the event<br>**Only Log it**: simply logs the event<br>**Reboot Device**: if PoE is supported, the device can be rebooted. The event will be logged. |
| **Status** | Indicates the DDOS prevention status. Possible statuses are:<br>**---**: disables DDOS prevention<br>**Analyzing**: analyzes packet throughput for initialization |

| | |
|---|---|
| | **Running**: analysis completes and ready for next move<br>**Attacked**: DDOS attacks occur |

## Device Description

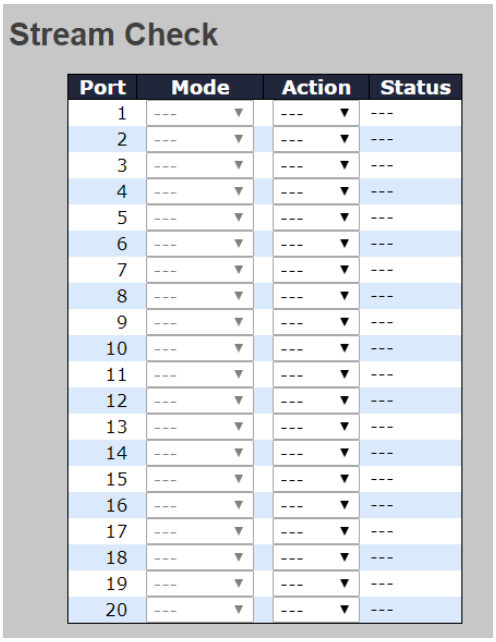
This page allows you to configure device description settings.




| Label | Description |
|---|---|
| **Type** | Indicates device types. Possible types are: **---** (no specification), **IP Camera**, **IP Phone**, **Access Point**, **PC**, **PLC**, and **Network Video Recorder** |
| **Location Address** | Indicates location information of the device. The information can be used for Google Mapping. |
| **Description** | Device descriptions |

## Stream Check

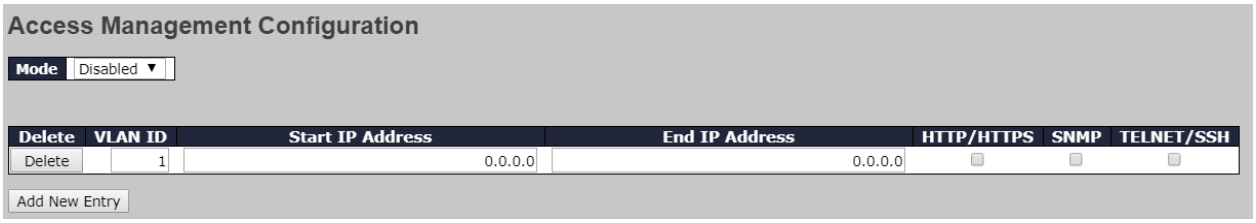
This page allows you to configure stream check settings.




| Label | Description |
|---|---|
| **Mode** | Enables or disables stream monitoring of the port |
| **Action** | Indicates the action to take when the stream gets low. Possible actions are:<br>**---**: no action<br>**Log it**: simply logs the event |

## 1.9.2 Access Management Configuration

You can configure access management table on this page. If the application's type match any one of the access management entries, it will allow access to the switch.

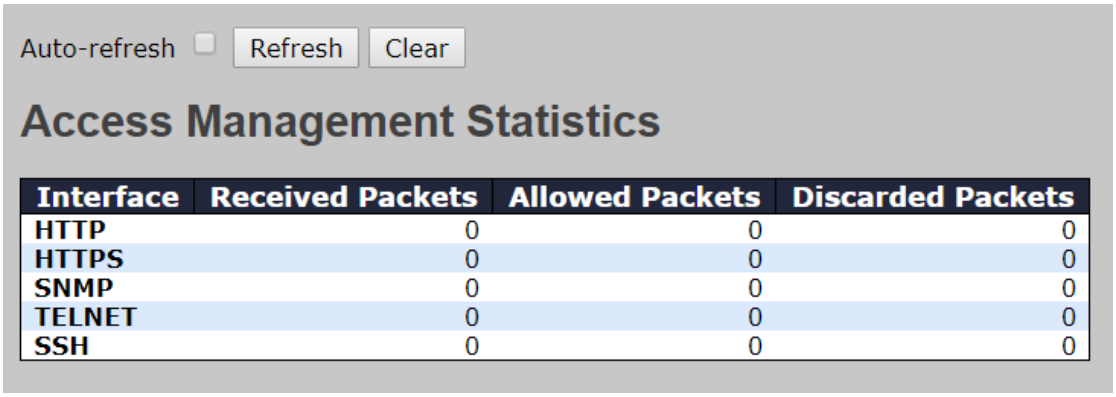



| Label | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **VLAN ID** | The VLAN ID for the access management entry. |
| **Start IP Address** | The start IP address for the access management entry. |
| **End IP Address** | The end IP address for the access management entry. |

| | |
|---|---|
| **HTTP/HTTPS** | 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** | 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** | The host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry. |

## Statistics

This page provides an overview of access management configurations.

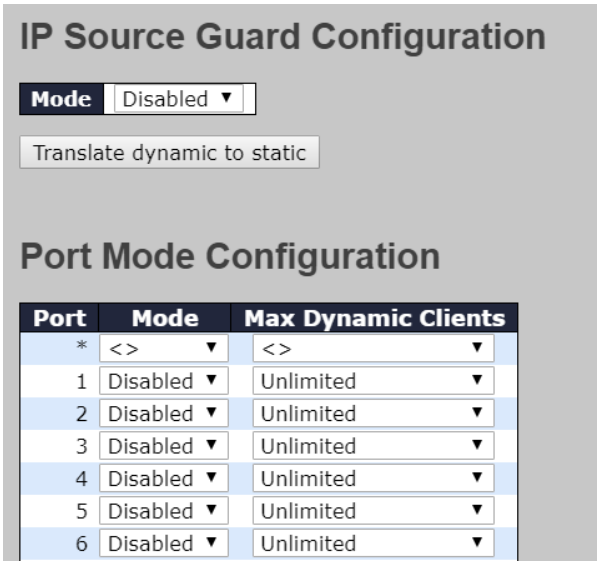



| Interface | Received Packets | Allowed Packets | Discarded Packets |
|---|---|---|---|
| HTTP | 0 | 0 | 0 |
| HTTPS | 0 | 0 | 0 |
| SNMP | 0 | 0 | 0 |
| TELNET | 0 | 0 | 0 |
| SSH | 0 | 0 | 0 |

## 1.9.3 IP Source Guard

IP source guard can prevent traffic attacks if a host tries to use the IP address of its neighbor. You can enable IP source guard when DHCP snooping is enabled on an untrusted interface. With this function enabled, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping.

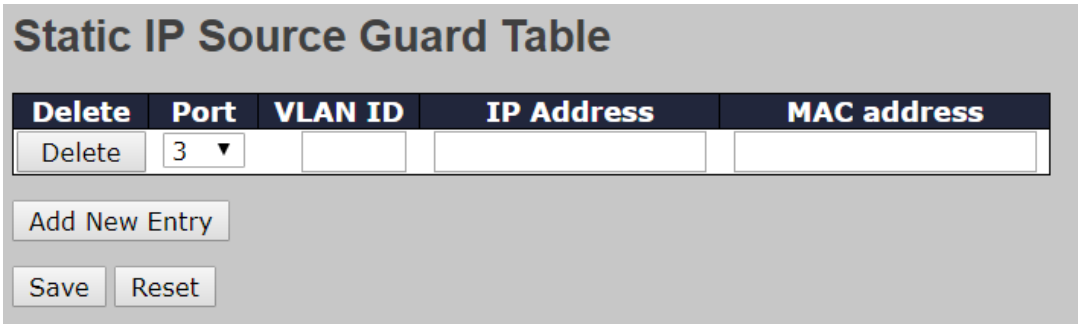
## Configuration




| Port | Mode | Max Dynamic Clients |
|---|---|---|
| * | <> | <> |
| 1 | Disabled | Unlimited |
| 2 | Disabled | Unlimited |
| 3 | Disabled | Unlimited |
| 4 | Disabled | Unlimited |
| 5 | Disabled | Unlimited |
| 6 | Disabled | Unlimited |

| Label | Description |
|---|---|
| **Mode** | Enable or disable this function. |
| **Max Dynamic Clients** | Specify the number of clients supported. |

## Static Table




| Label | 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. |

## Dynamic Table

This page shows entries in the Dynamic IP Source Guard table. The default value is 20. The Start from port address, VLAN, MAC address, and IP address input fields allow you to select the starting point in the table.

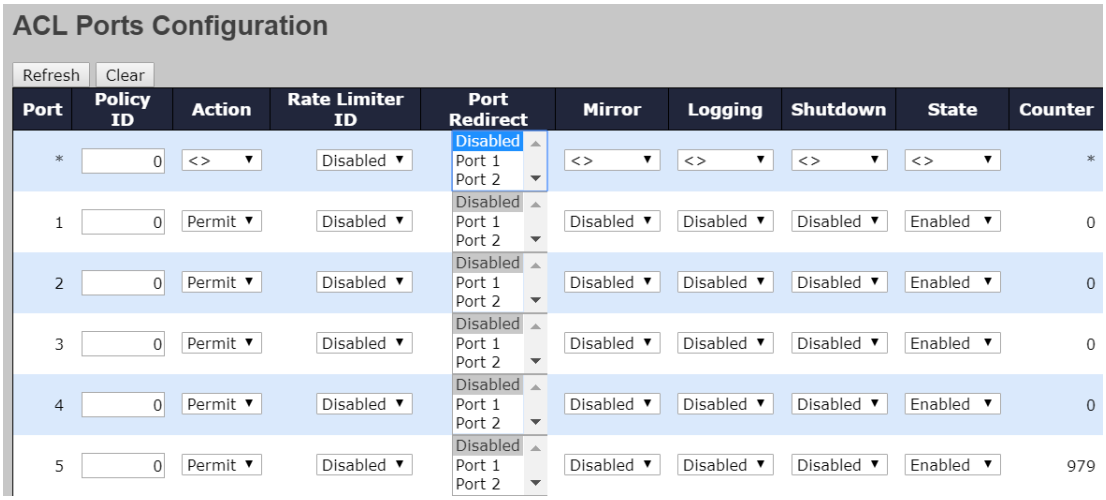

| Label | Description |
|---|---|
| **Port** | The logical port for the settings. |
| **VLAN ID** | The vlan id for the settings. |

| | |
|---|---|
| **IP Address** | Allowed source IP address. |
| **MAC Address** | Allowed source MAC address. |

## 1.9.4 ACL

### Ports

This page allows you to 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.

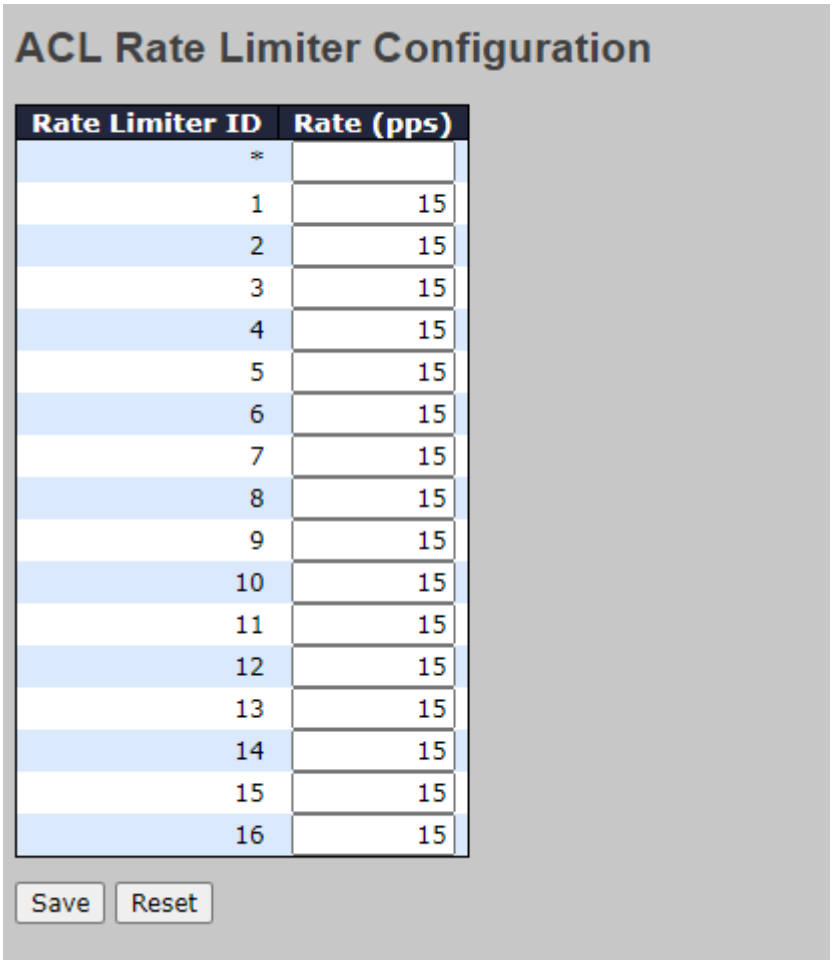



| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied |
| **Policy ID** | Select to apply a policy to the port. The allowed values are 1 to 8. The default value is **1**. |
| **Action** | Select to **Permit** to permit or **Deny** to deny forwarding. The default value is **Permit**. |
| **Rate Limiter ID** | Select a rate limiter for the port. The allowed values are **Disabled** or numbers from 1 to 15. The default value is **Disabled**. |
| **Port Redirect** | Indicates the port redirect operation implemented by the ACE. Frames matching the ACE are redirected to the listed port. |
| **Mirror** | Select which port frames are copied to. The allowed values are **Disabled** or a specific port number. The default value is **Disabled**. |
| **Logging** | Specifies the logging operation of the port. 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**. Please note that system log memory capacity and logging rate is limited. |
| **Shutdown** | Specifies the shutdown 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**. |
| **Counter** | Counts the number of frames that match this ACE. |

## Rate Limiters

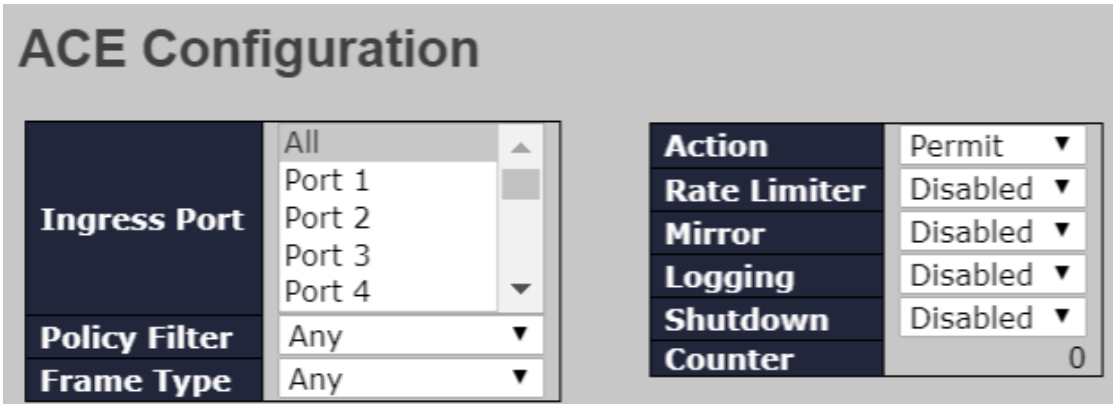
This page allows you to configure the rate limiter for the ACL of the switch.




| Label | Description |
|---|---|
| **Rate Limiter ID** | The rate limiter ID for the settings contained in the same row. |
| **Rate** | The rate unit is packet per second (pps), which can be configured as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K.<br>The 1 kpps is actually 1002.1 pps. |
| **Unit** | Specify the unit for the rate. |

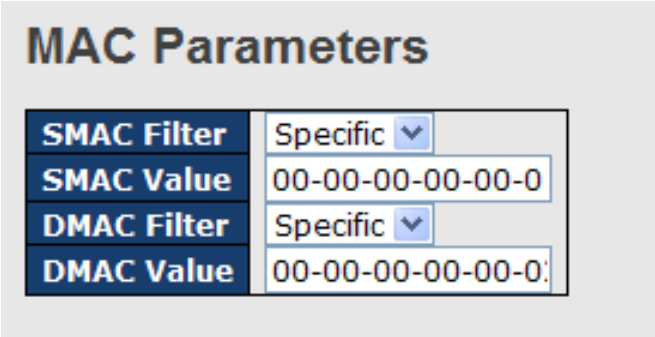
## ACL Control List

This page allows you to configure ACE (Access Control Entry). An ACE consists of several parameters. These parameters vary with the frame type you have selected. First select the ingress port for the ACE, and then the frame type. Different parameter options are displayed according to the frame type you have selected. A frame matching the ACE can be configured here.



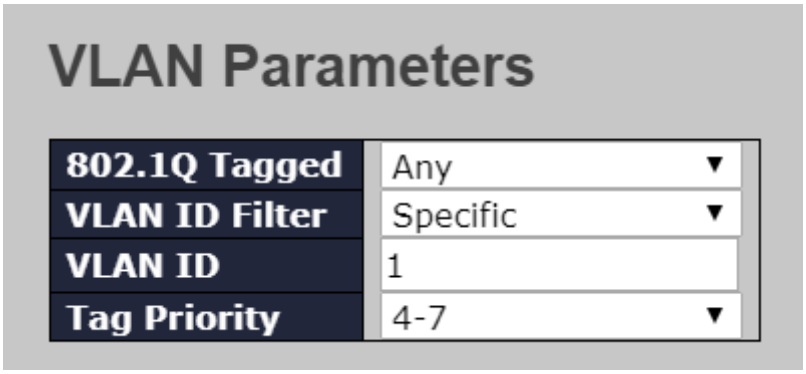

| Label | Description |
|---|---|
| **Ingress Port** | Indicates the ingress port to which the ACE will apply.<br>**Any**: the ACE applies to any port<br>**Port n**: the ACE applies to this port number, where n is the number of the switch port.<br>**Policy n**: the ACE applies to this policy number, where n can range from 1 to 8. |
| **Frame Type** | Indicates the frame type of the ACE. These frame types are mutually exclusive.<br>**Any**: any frame can match the ACE.<br>**Ethernet Type**: only Ethernet type frames can match the ACE. The IEEE 802.3 descripts the value of length/types should be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).<br>**ARP**: only ARP frames can match the ACE. Notice the ARP frames will not match the ACE with Ethernet type.<br>**IPv4**: only IPv4 frames can match the ACE. Notice the IPv4 frames will not match the ACE with Ethernet type. |
| **Action** | Specifies the action to take when a frame matches the ACE.<br>Permit: takes action when the frame matches the ACE.<br>Deny: drops the frame matching the ACE. |
| **Rate Limiter** | Specifies the rate limiter in number of base units. The allowed range |

| | |
|---|---|
| | is 1 to 15. **Disabled** means the rate limiter operation is disabled. |
| **Port Copy** | Frames matching the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled means the port copy operation is disabled. |
| **Logging** | Specifies the logging operation of the ACE. 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>Please note that system log memory capacity and logging rate is limited. |
| **Shutdown** | Specifies the shutdown 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 shutdown is disabled for the ACE. |
| **Counter** | Indicates the number of times the ACE matched by a frame. |

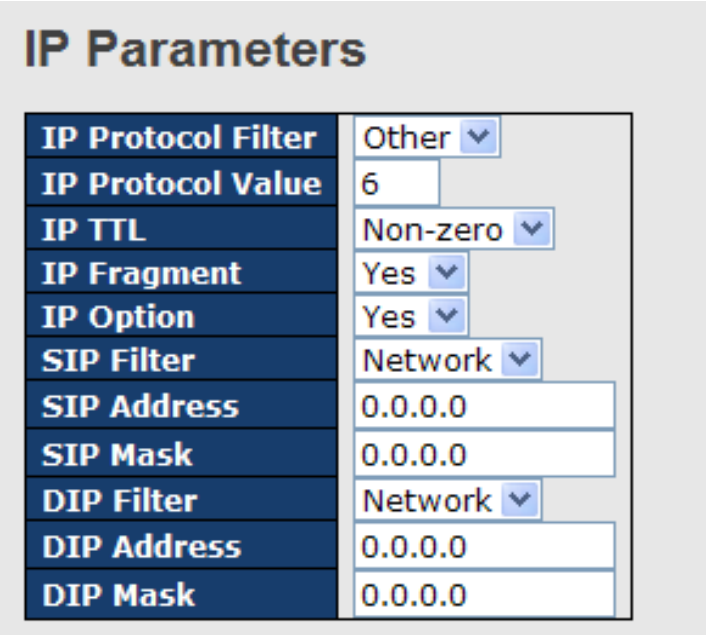



| Label | Description |
|---|---|
| **SMAC Filter** | (Only displayed when the frame type is Ethernet Type or ARP.)<br>Specifies the source MAC filter for the ACE.<br>**Any**: no SMAC filter is specified (SMAC filter status is "**don't-care**").<br>**Specific**: if you want to filter a specific source MAC address with the 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". Frames matching the ACE will use this SMAC value. |
| **DMAC Filter** | Specifies 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. |

| | |
|---|---|
| | **BC**: frame must be broadcast.<br>**UC**: frame must be unicast.<br>**Specific**: If you want to filter a specific destination MAC address with the 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". Frames matching the ACE will use this DMAC value. |

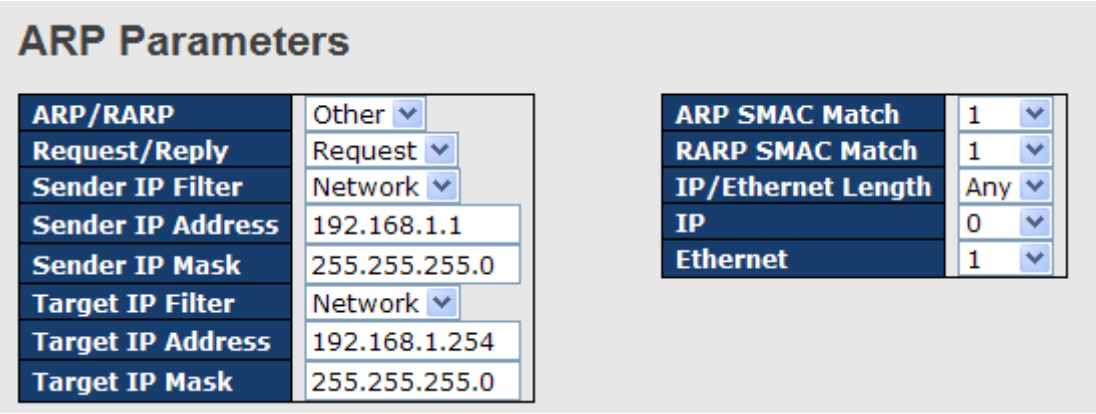



| Label | Description |
|---|---|
| **VLAN ID Filter** | Specifies the VLAN ID filter for the ACE<br>**Any**: no VLAN ID filter is specified (VLAN ID filter status is "**don't-care**").<br>**Specific**: if you want to filter a specific VLAN ID with the ACE, choose this value. A field for entering a VLAN 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. Frames matching the ACE will use this VLAN ID value. |
| **Tag Priority** | Specifies the tag priority for the ACE. A frame matching the ACE will use this tag priority. The allowed number range is 0 to 7. **Any** means that no tag priority is specified (tag priority is "**don't-care**"). |




| Label | Description |
|---|---|
| **IP Protocol Filter** | Specifies the IP protocol filter for the 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 the ACE, choose this value. A field for entering an IP protocol filter appears.<br>ICMP: selects ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. For more details of these fields, please refer to the help file.<br>**UDP**: selects UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. For more details of these fields, please refer to the help file.<br>**TCP**: selects TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. For more details of these fields, please refer to the help file. |
| **IP Protocol Value** | **Specific** allows you to enter a specific value. The allowed range is 0 to 255. Frames matching the ACE will use this IP protocol value. |
| **IP TTL** | Specifies the time-to-live settings for the ACE<br>**Zero**: IPv4 frames with a time-to-live value 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**"). |

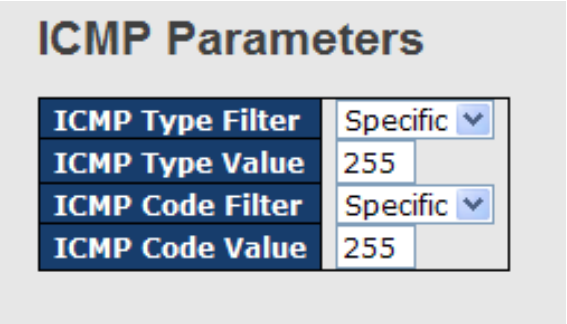
| | |
|---|---|
| **IP Fragment** | Specifies the fragment offset settings for the ACE. This includes settings of More Fragments (MF) bit and Fragment Offset (FRAG OFFSET) for an IPv4 frame.<br>**No**: IPv4 frames whose MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.<br>**Yes**: IPv4 frames whose 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** | Specifies the options flag settings for the ACE<br>**No**: IPv4 frames whose options flag is set must not be able to match this entry.<br>**Yes**: IPv4 frames whose options flag is set must be able to match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |
| **SIP Filter** | Specifies 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** | Specifies the destination IP filter for the 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. |



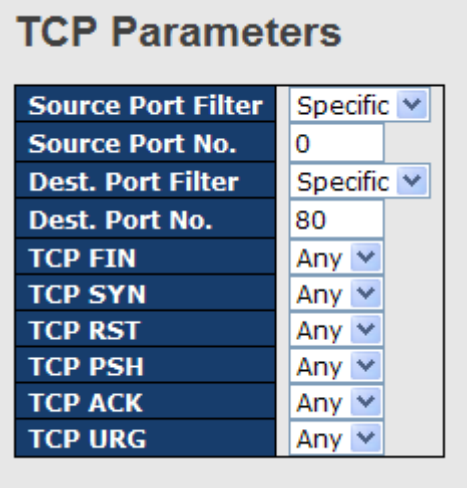

| Label | Description |
|---|---|
| **ARP/RARP** | Specifies the available ARP/RARP opcode (OP) flag for the ACE<br>**Any**: no ARP/RARP OP flag is specified (OP is "**don't-care**").<br>**ARP**: frame must have ARP/RARP opcode set to ARP<br>**RARP**: frame must have ARP/RARP opcode set to RARP.<br>**Other**: frame has unknown ARP/RARP Opcode flag. |
| **Request/Reply** | Specifies the available ARP/RARP opcode (OP) flag for the ACE<br>**Any**: no ARP/RARP 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** | Specifies the sender IP filter for the 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** | Specifies the target IP filter for the specific ACE |

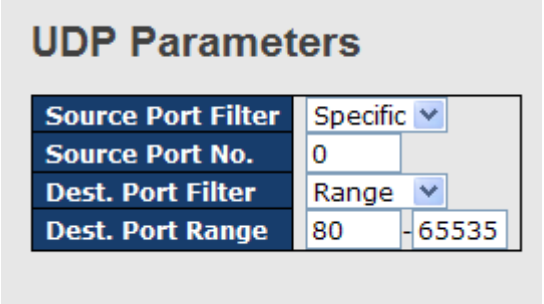
| | |
|---|---|
| | **Any**: no target IP filter is specified (target IP filter is "**don't-care**").<br>**Host**: target IP filter is set to **Host**. Specify the target IP address in the **Target IP Address** field that appears.<br>**Network**: target IP filter is set to **Network**. Specify the target 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 SMAC Match** | Specifies whether frames will meet 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 SMAC Match** | Specifies whether frames will meet the action according to their target hardware address field (THA) settings.<br>**0**: RARP frames where THA is not equal to the SMAC address<br>**1**: RARP frames where THA is equal to the SMAC address<br>**Any**: any value is allowed ("**don't-care**") |
| **IP/Ethernet Length** | Specifies whether frames will meet 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 equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must not match this entry.<br>**1**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |
| **IP** | Specifies whether frames will meet the action according to their ARP/RARP hardware address space (HRD) settings.<br>**0**: ARP/RARP frames where the HLD is equal to Ethernet (1) must not match this entry.<br>**1**: ARP/RARP frames where the HLD is equal to Ethernet (1) |

| | |
|---|---|
| | must match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |
| **Ethernet** | Specifies whether frames will meet the action according to their ARP/RARP protocol address space (PRO) settings.<br>**0**: ARP/RARP frames where the PRO is equal to IP (0x800) must not match this entry.<br>**1**: ARP/RARP frames where the PRO is equal to IP (0x800) must match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |




| Label | Description |
|---|---|
| **ICMP Type Filter** | Specifies the ICMP filter for the 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 the 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 matching the ACE will use this ICMP value. |
| **ICMP Code Filter** | Specifies the ICMP code filter for the 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 the 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 matching the ACE will use this ICMP code value. |



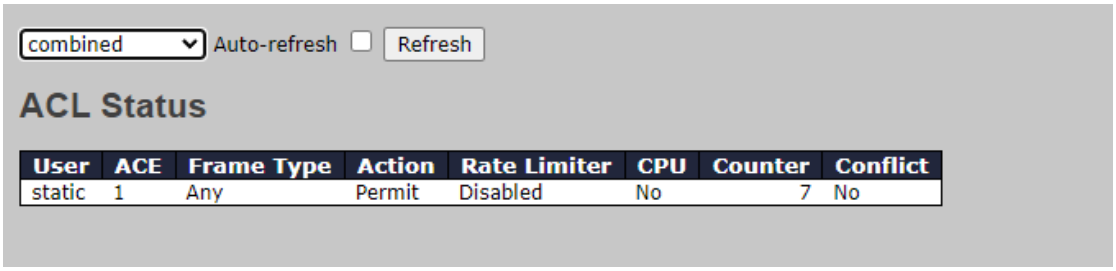

| Label | Description |
|---|---|
| **TCP/UDP Source Filter** | Specifies the TCP/UDP source filter for the ACE<br>**Any**: no TCP/UDP source filter is specified (TCP/UDP source filter status is "**don't-care**").<br>**Specific**: if you want to filter a specific TCP/UDP source filter with the ACE, you 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 the ACE, you can enter a specific TCP/UDP source range. 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 matching the ACE will use 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 matching the ACE will use this TCP/UDP source value. |
| **TCP/UDP Destination Filter** | Specifies the TCP/UDP destination filter for the 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 the 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 the ACE, you can enter a specific TCP/UDP destination range. 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 matching the ACE will use 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 matching the ACE will use this TCP/UDP destination value. |
| **TCP FIN** | Specifies the TCP FIN ("no more data from sender") value for the 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** | Specifies the TCP SYN ("synchronize sequence numbers") value for the 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 PSH** | Specifies the TCP PSH ("push function") value for the 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** | Specifies the TCP ACK ("acknowledgment field significant") value for the 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** | Specifies the TCP URG ("urgent pointer field significant") value for the 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**"). |

## 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.



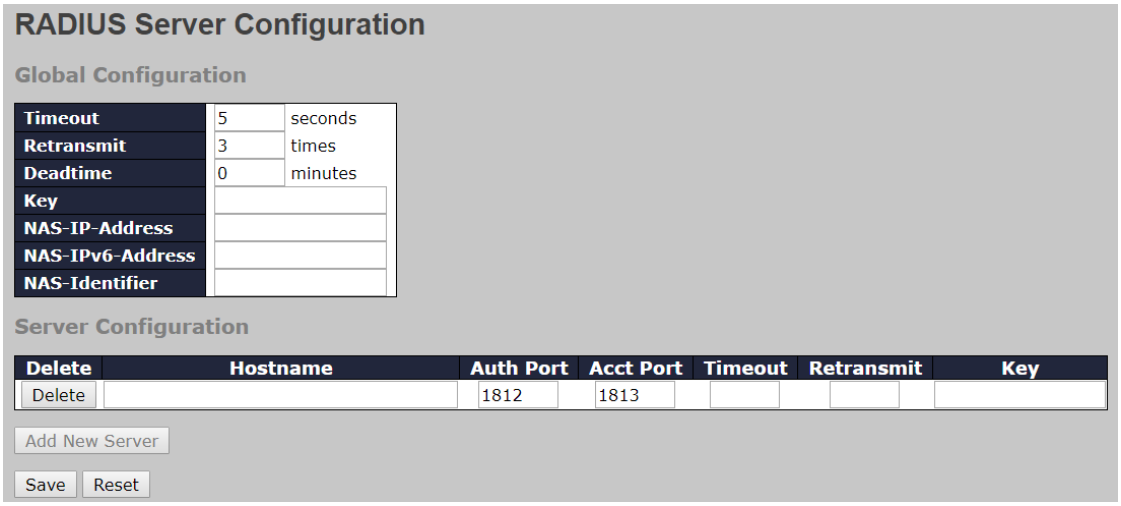

| Label | Description |
|---|---|
| **User** | Indicates the ACL user. |
| **ACE** | Indicates the ACE ID on local switch. |
| **Frame Type** | Indicates the frame type of the ACE. Possible values are:<br>**Any:** The ACE will match any frame type.<br>**EType:** The ACE will match Ethernet Type frames. 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. |

| | |
|---|---|
| | **Deny:** Frames matching the ACE are dropped. |
| **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. |

## 1.9.5 AAA

### Common Server Configurations

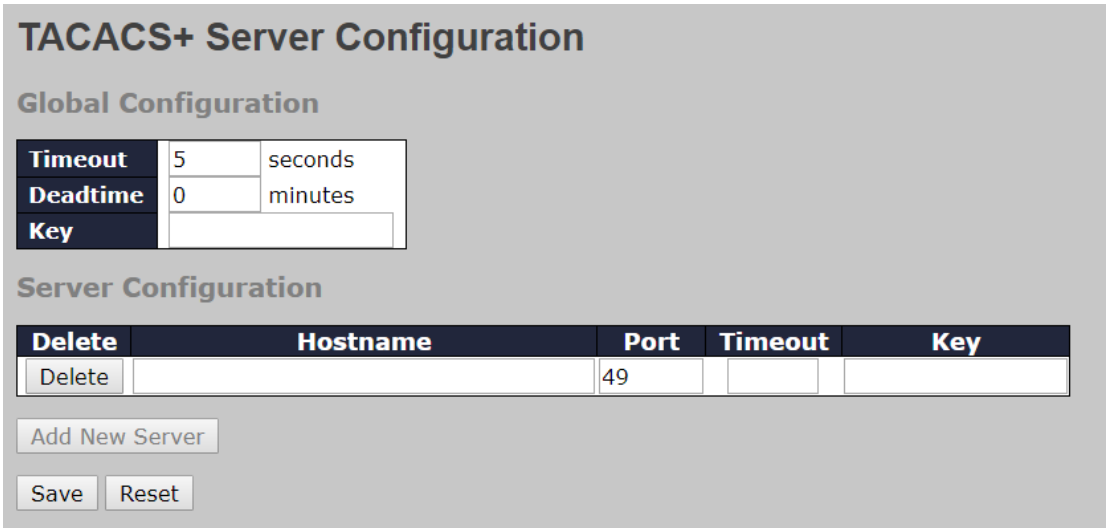
This page allows you to configure authentication servers.




| Label | Description |
|---|---|
| **Timeout** | The timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server.<br>If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled server (if any).<br>RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead. |

| | |
|---|---|
| **Retransmit** | The number of times the switch tries to connect to a RADIUS server. |
| **Dead Time** | The dead time, which can be set to a number between 0 and 3600 seconds, 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 dead time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. |
| **NAS-IP-Address** | Indicates the identifying IP Address of the NAS which is requesting authentication of the user, and SHOULD be unique to the NAS within the scope of the RADIUS server. |
| **NAS-ID** | Network Access Server identifier (NAS-ID) for the interface. The NAS-ID is sent to the RADIUS server by the controller (as a RADIUS client) using the authentication request, which is used to classify users to different groups. You can enter up to 32 alphanumeric characters. |
| **Delete** | Click to delete an entry from the table. |
| **Hostname** | Specifies the host name of the RADIUS server. The maximum supported length for the AAA RADIUS hostname is 40 characters. |
| **Auth Port** | The authentication port which specifies the UDP port used to connect the RADIUS server for authentication. The default is 1812. |
| **Acct Port** | The UDP port to use on the RADIUS accounting server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS accounting server. |
| **Key** | The shared secret between the switch and the RADIUS server. |
| **Timeout** | The time to wait for the RADIUS server to respond. |
| **Retransmit** | The number of times the switch tries to connect to a RADIUS server. |

### 1.9.6 TACACS+




| Label | Description |
|---|---|
| **Timeout** | The timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server.<br>If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled server (if any).<br>TACACS+ servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead. |
| **Dead Time** | The dead time, which can be set to a number between 0 and 3600 seconds, 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 dead time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. |
| **Key** | The shared secret between the switch and the TACACS+ server. |
| **Hostname** | Specifies the host name of the TACACS+ server. The maximum supported length for the AAA RADIUS hostname is 40 characters. |

| | |
|---|---|
| **Timeout** | The time to wait for the TACACS+ server to respond. |
| **Key** | The shared secret between the switch and the TACACS+ server. |

## 1.9.7 RADIUS

### Authentication and Accounting Server Configurations

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

**RADIUS Server Status Overview**

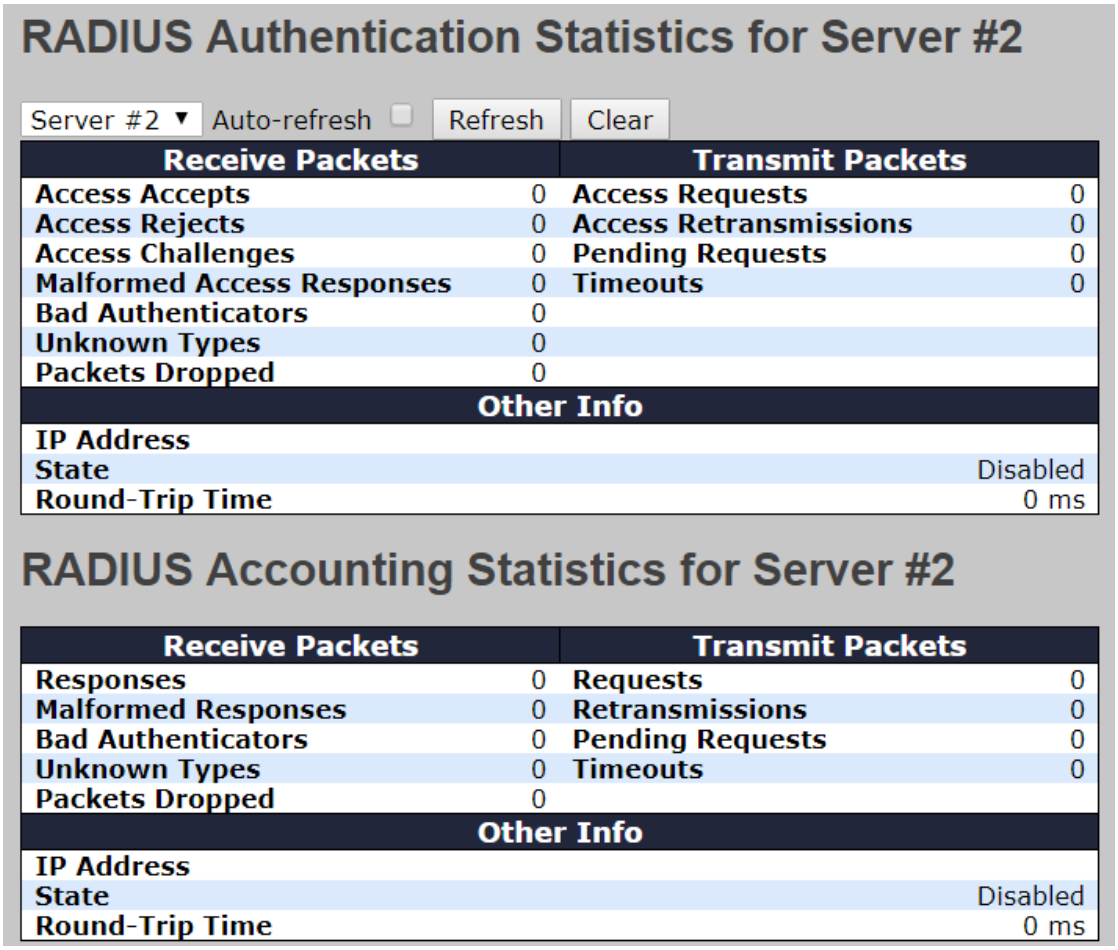
Auto-refresh Refresh

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

| Label | Description |
|---|---|
| # | The RADIUS server number. Click to navigate to detailed statistics of the server |
| **IP Address** | The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of the server |
| **Status** | The current status of the server. This field has 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 communications are built, and the RADIUS module is ready to accept access attempts.<br>**Dead** (X seconds left): access attempts are made to this server, but it does not reply within the configured timeout. The server has temporarily been disabled, but will be 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. |

## RADIUS Details

This page shows the access statistics of the authentication and accounting servers. Use the server drop-down list to switch between the backend servers to show related details.



RADIUS Authentication Statistics for Server #2

Server #2 ▼ Auto-refresh Refresh Clear

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

RADIUS Accounting Statistics for Server #2

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

### 1.9.8 ARP Inspection (only for Layer 3 Model)

This page provides ARP Inspection related configuration.

## Configuration

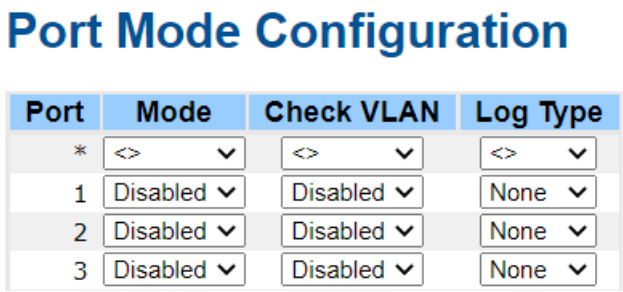
Mode Disabled Rate Limit (pps) 15

Translate dynamic to static

| Label | Description |
|---|---|
| **Mode** | Enable the Global ARP Inspection or disable the Global ARP Inspection. |
| **Rate Limit (PPS** | The Rate Limit for ARP Inspection. The valid rate is 0-131071 in pps. |

## Port Mode Configuration

Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:




| Label | Description |
|---|---|
| **Port Mode Configuration** | **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. 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.<br>Buttons |

### 1.9.9 NAS (802.1x)

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 authentication configuration page.

MAC-based authentication allows for authentication of more than one user on the same port, and does not require the users to have special 802.1X software installed on their system. The switch uses the users' MAC addresses to authenticate against the backend server. As intruders can create counterfeit MAC addresses, MAC-based authentication is less secure than 802.1X authentication.

#### Overview of 802.1X (Port-Based) Authentication

In an 802.1X network environment, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch 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 which 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 as it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) does not need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding the result to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: in an environment where two backend servers are enabled, the server timeout is configured to X seconds (using the authentication configuration page), and the first server in the list is currently down (but not considered dead), if the supplicant retransmits EAPOL Start

frames at a rate faster than X seconds, it will never be authenticated because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. Since the server has not failed (because the X seconds have not expired), the same server will be contacted when 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.

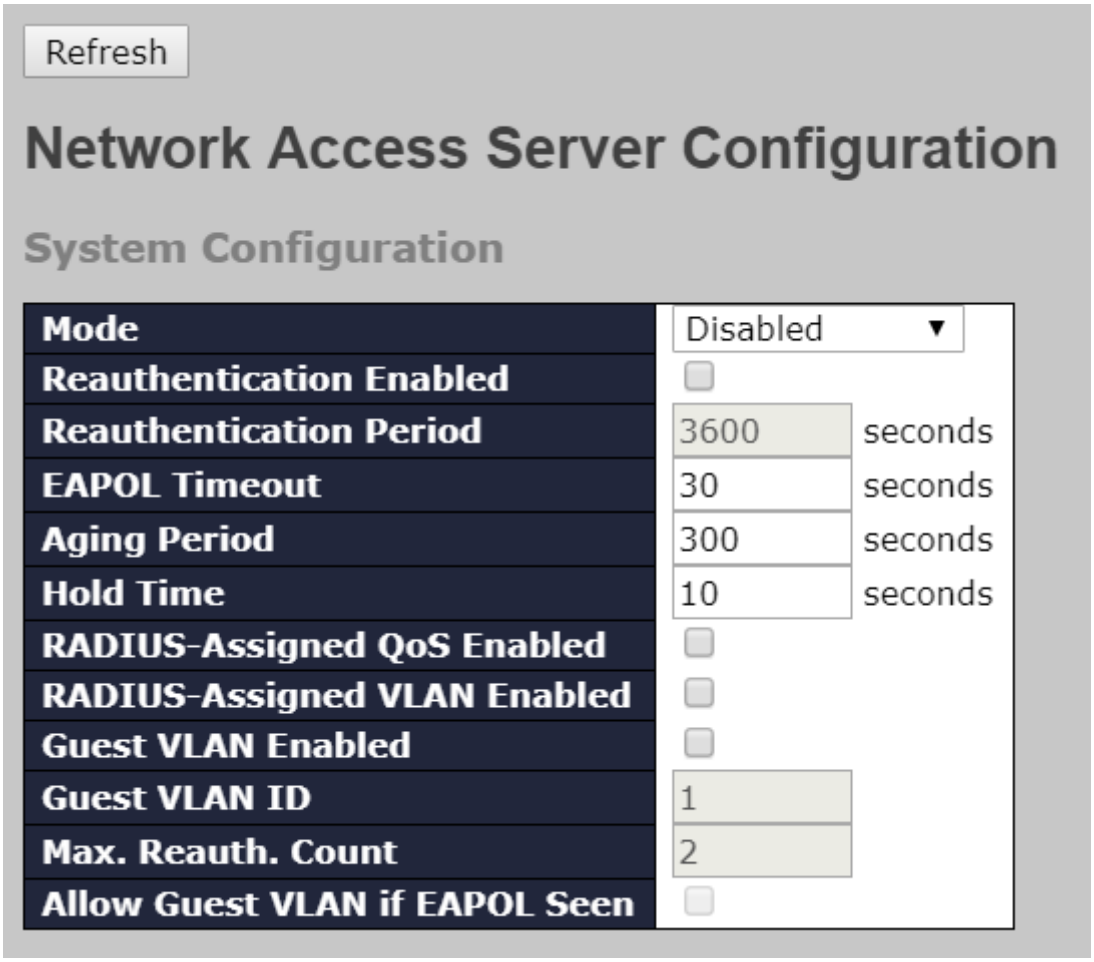
## Overview of MAC-Based Authentication

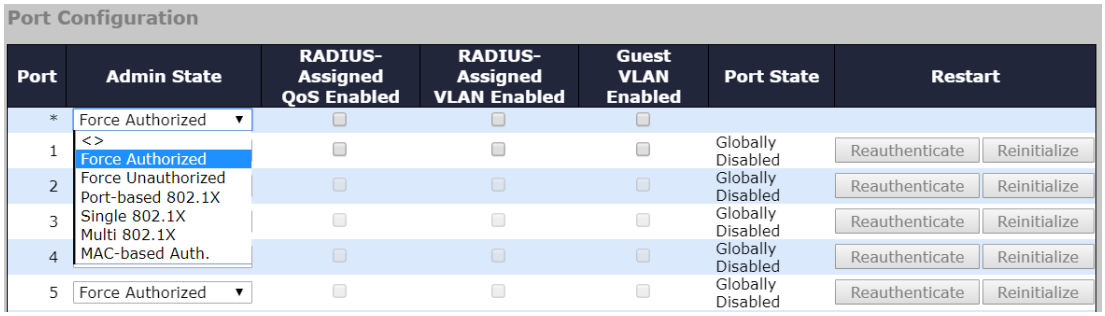
Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by 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 in the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

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

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients do npt 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, and only the MD5-Challenge method is supported.

802.1X and MAC-Based authentication configurations consist of two sections: system- and port-wide.




| Label | Description |
|---|---|
| **Mode** | Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch. If globally disabled, all ports are allowed to forward frames. |
| **Reauthentication Enabled** | If checked, 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.<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 does not imply that a client is still present on a port (see Age Period below). |
| **Reauthentication Period** | Determines the period, in seconds, after which a connected client must be re-authenticated. This is only active if the **Reauthentication Enabled** checkbox is checked. Valid range of the value is 1 to 3600 seconds. |
| **EAPOL Timeout** | Determines the time for retransmission of Request Identity EAPOL frames.<br>Valid range of the value is 1 to 65535 seconds. This has no effect for MAC-based ports. |
| **Age Period** | This setting applies to the following modes, i.e. modes using the **Port Security** functionality to secure MAC addresses:<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>For ports in **MAC-based Auth.** mode, reauthentication does not cause direct communications 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>**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 Unauthorized state. The hold timer does not count during an on-going authentication.<br>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. |
| **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 is up, and any client on the port will be allowed network access without authentication.<br>**Force Unauthorized**<br>In this mode, the switch will send one EAPOL Failure frame when the port link is up, and any client on the port will be disallowed network access.<br>**Port-based 802.1X**<br>In an 802.1X network environment, 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 which encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server is 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 as it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) does not 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 the result to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant. |

| | |
|---|---|
| | Note: in an environment where two backend servers are enabled, the server timeout is configured to X seconds (using the authentication configuration page), and the first server in the list is currently down (but not considered dead), if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, it will never be authenticated because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. Since the server has not failed (because the X seconds have not expired), the same server will be contacted when 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>**a. 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 are not authenticated individually. To overcome this security breach, use the Single 802.1X variant.<br>Single 802.1X is not yet an IEEE standard, but features many of the same characteristics as 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 communications between the supplicant and the switch. If more than one supplicant are connected to a port, the one that comes first when the port's link is connected will be the first one considered. If that supplicant does not provide valid credentials within a certain amount of time, the chance will be given to another supplicant. 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>**b. Multi 802.1X**<br>In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for |

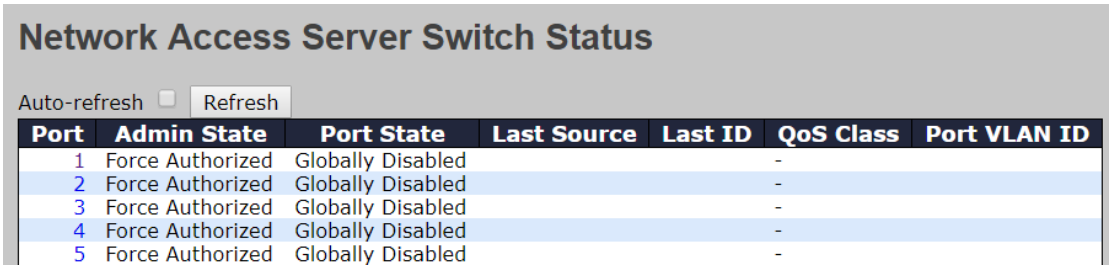
| | |
|---|---|
| | network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they are not authenticated individually. To overcome this security breach, use the Multi 802.1X variant.<br>Multi 802.1X is not yet an IEEE standard, but features many of the same characteristics as port-based 802.1X. In Multi 802.1X, one or more supplicants can be 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 the destination MAC address for EAPOL frames sent from the switch to 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>**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 in the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. |

| | |
|---|---|
| | When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based authentication has nothing to do with the 802.1X standard.<br>The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients do not 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. |
| **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. |

| | |
|---|---|
| | **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 on successfully authenticated clients on the port and will not cause the clients to be temporarily unauthorized.<br>**Reinitialize**: forces a reinitialization of the clients on the port and hence a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress. |

## Switch

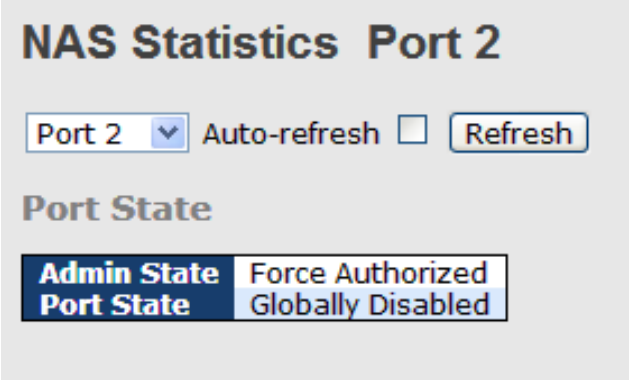
This page provides an overview of the current NAS port states.




| Port | Admin State | Port State | Last Source | Last ID | QoS Class | Port VLAN ID |
|---|---|---|---|---|---|---|
| 1 | Force Authorized | Globally Disabled | | | - | |
| 2 | Force Authorized | Globally Disabled | | | - | |
| 3 | Force Authorized | Globally Disabled | | | - | |
| 4 | Force Authorized | Globally Disabled | | | - | |
| 5 | Force Authorized | Globally Disabled | | | - | |

| Label | Description |
|---|---|
| **Port** | The switch port number. Click to navigate to detailed 802.1X statistics of each port. |
| **Admin State** | The port's current administrative state. Refer to **NAS Admin State** for more details regarding each value. |
| **Port State** | The current state of the port. Refer to **NAS Port State** for more details regarding each value. |
| **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** | Shows the level of QoS. |

This page provides detailed IEEE 802.1X statistics for a specific switch port using port-based authentication. For MAC-based ports, only selected backend server (RADIUS Authentication Server) statistics is showed. Use the port drop-down list to select which port details to be displayed.




| Label | Description |
|---|---|
| **Admin State** | The port's current administrative state. Refer to **NAS Admin State** for more details regarding each value. |
| **Port State** | The current state of the port. Refer to **NAS Port State** for more details regarding each value. |
| **EAPOL Counters** | These supplicant frame counters are available for the following administrative states:<br>• **Force Authorized**<br>• **Force Unauthorized**<br>• 802.1X<br><br>EAPOL Counters<br>Direction / Name / IEEE Name / Description<br>Rx / **Total** / dot1xAuthEapolFramesRx / The number of valid EAPOL frames of any type that have been received by the switch.<br>Rx / **Response ID** / dot1xAuthEapolRespIdFramesRx / The number of valid EAP Resp/ID frames that have been received by the switch.<br>Rx / **Responses** / dot1xAuthEapolRespFramesRx / The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.<br>Rx / **Start** / dot1xAuthEapolStartFramesRx / The number of EAPOL Start frames that have been received by the switch.<br>Rx / **Logoff** / dot1xAuthEapolLogoffFramesRx / The number of valid EAPOL logoff frames that have been received by the switch.<br>Rx / **Invalid Type** / dot1xAuthInvalidEapolFramesRx / The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.<br>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.<br>Tx / **Total** / dot1xAuthEapolFramesTx / The number of EAPOL frames of any type that have been transmitted by the switch.<br>Tx / **Request ID** / dot1xAuthEapolReqIdFramesTx / The number of EAP initial request frames that have been transmitted by the switch.<br>Tx / **Requests** / dot1xAuthEapolReqFramesTx / The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch. |
| **Backend Server Counters** | These backend (RADIUS) frame counters are available for the following administrative states:<br>• **802.1X** |

<table>
<tr><td></td><td>

• **MAC-based Auth.**

<table>
<tr><th colspan="4">Backend Server Counters</th></tr>
<tr><th>Direction</th><th>Name</th><th>IEEE Name</th><th>Description</th></tr>
<tr><td>Rx</td><td>Access Challenges</td><td>dot1xAuthBackendAccessChallenges</td><td>Port-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).</td></tr>
<tr><td>Rx</td><td>Other Requests</td><td>dot1xAuthBackendOtherRequestsToSupplicant</td><td>Port-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.</td></tr>
<tr><td>Rx</td><td>Auth. Successes</td><td>dot1xAuthBackendAuthSuccesses</td><td>Port- 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.</td></tr>
<tr><td>Rx</td><td>Auth. Failures</td><td>dot1xAuthBackendAuthFails</td><td>Port- 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.</td></tr>
<tr><td>Tx</td><td>Responses</td><td>dot1xAuthBackendResponses</td><td>Port-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.</td></tr>
</table>

</td></tr>
<tr><td>

**Last Supplicant/Client Info**

</td><td>

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

• **802.1X**

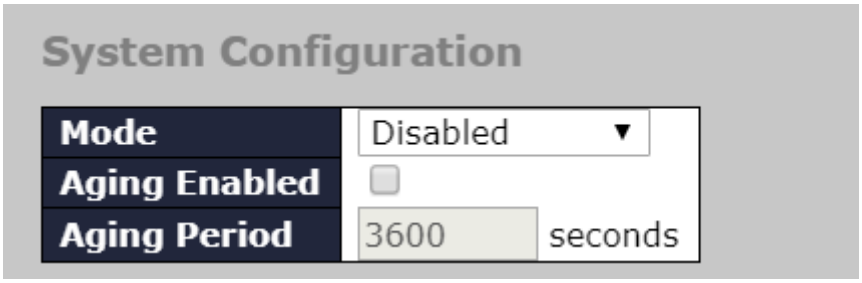
• **MAC-based Auth.**

<table>
<tr><th colspan="3">Last Supplicant/Client Info</th></tr>
<tr><th>Name</th><th>IEEE Name</th><th>Description</th></tr>
<tr><td>MAC Address</td><td>dot1xAuthLastEapolFrameSource</td><td>The MAC address of the last supplicant/client.</td></tr>
<tr><td>VLAN ID</td><td>-</td><td>The VLAN ID on which the last frame from the last supplicant/client was received.</td></tr>
<tr><td>Version</td><td>dot1xAuthLastEapolFrameVersion</td><td>802.1X-based:<br>The protocol version number carried in the most recently received EAPOL frame.<br>MAC-based:<br>Not applicable.</td></tr>
<tr><td>Identity</td><td>-</td><td>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.</td></tr>
</table>

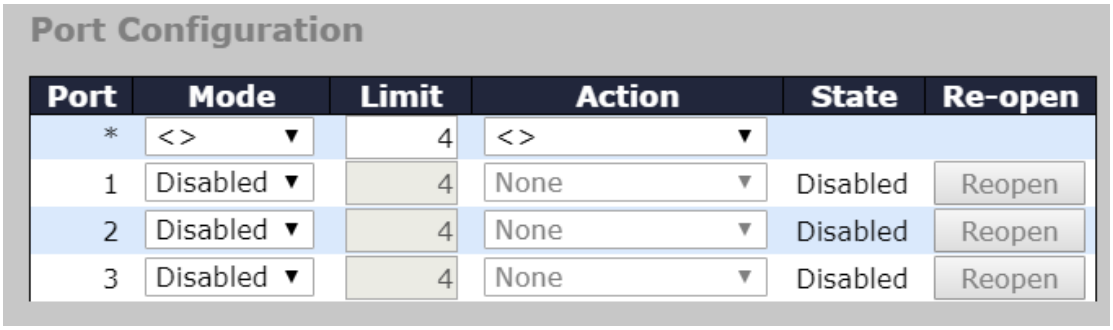
</td></tr>
</table>

## 1.9.10 Port Security Limit Control

This page allows you to configure limit control for port security system- or port-wise. It will limit the number of users on a given port. If the specified number is exceeded, an action is taken..




| Label | Description |
|---|---|
| **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** | You can specify the aging period in seconds. The Aging Period can be set to a number between 10 and 10,000,000 seconds. |

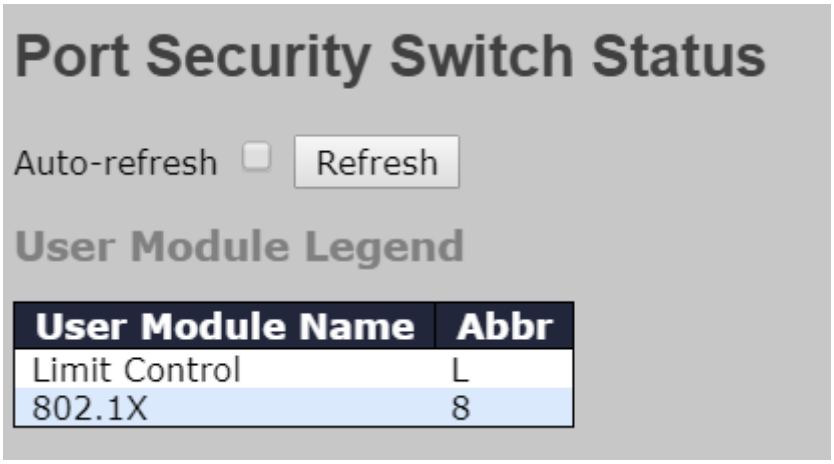



| Label | Description |
|---|---|
| **Mode** | Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port. |
| **Limit** | The maximum number of MAC addresses that can be secured on this port. The maximum allowed value is 1024. If the limit is exceeded, the corresponding action is taken. |
| **Action** | If the limit number is reached, the switch will take one of the following actions:<br>**None**: Do not allow more than Limit MAC addresses on the port, |

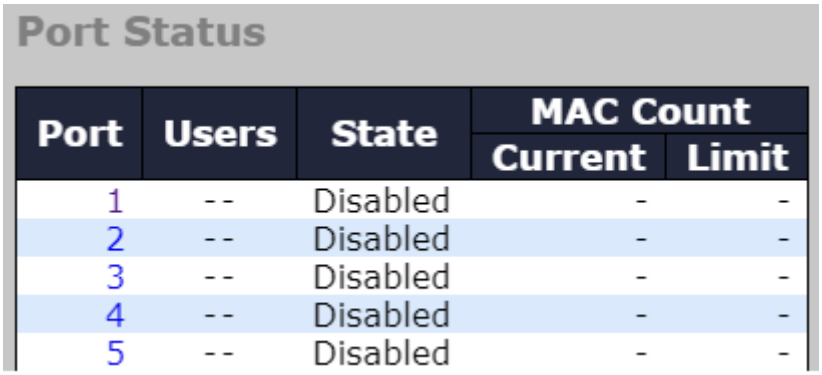
| | |
|---|---|
| | but take no further action.<br>**Trap**: If Limit + 1 MAC addresses is seen on the port, send an *SNMP (Simple Network Management Protocol)* trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.<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.<br>**Trap & Shutdown**: If Limit + 1 MAC addresses is seen on the port, both the “Trap” and the “Shutdown” actions described above will be taken. |
| **State** | This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:<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** | If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case.<br>Note that clicking the **Re-open** button causes the page to be refreshed, so non-committed changes will be lost. |

## Switch

This page allows you to review the port security status.




| Label | Description |
|---|---|
| **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. |

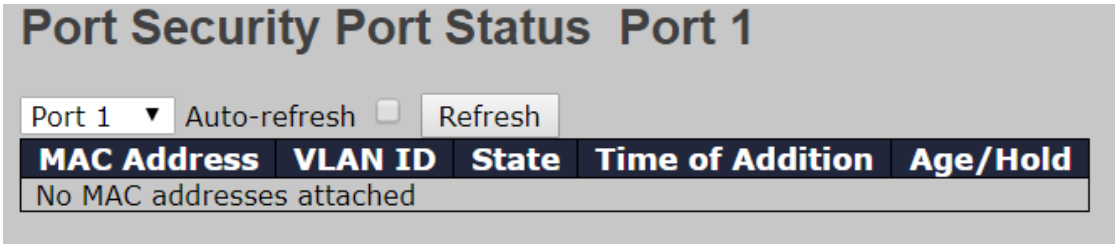



| Label | Description |
|---|---|
| **Users** | Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security. |
| **State** | Shows the current state of the port which includes the following 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** | The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-). |

## Port

This page allows you to review the MAC addresses secured by the Port Security module.



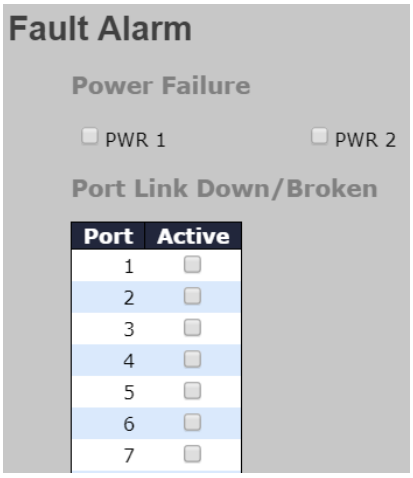

| Label | Description |
|---|---|
| **MAC Address** | The MAC address that is seen on this port. If no MAC addresses are learned, a single row stating No MAC addresses attached is displayed. |
| **VLAN ID** | The VLAN ID that is seen on this port. |
| **State** | Indicates whether the corresponding MAC address is blocked or forwarding. If blocked, it will not be allowed to transmit or receive traffic. |
| **Time of Addition** | Shows the date and time when this MAC address was first seen on the port. |

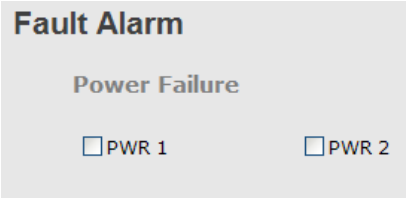
| | |
|---|---|
| **Age/Hold** | If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module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

# 1.10 Warning

## 1.10.1 Fault Alarm

When any selected fault event happens, the Fault LED on the switch panel will light up and the electric relay will signal at the same time.

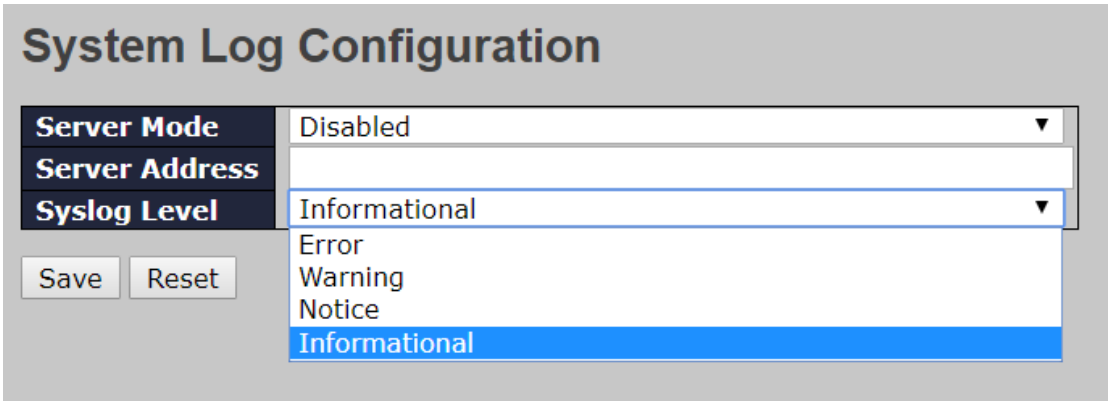



## 1.10.2 System Warning

### SYSLOG Setting

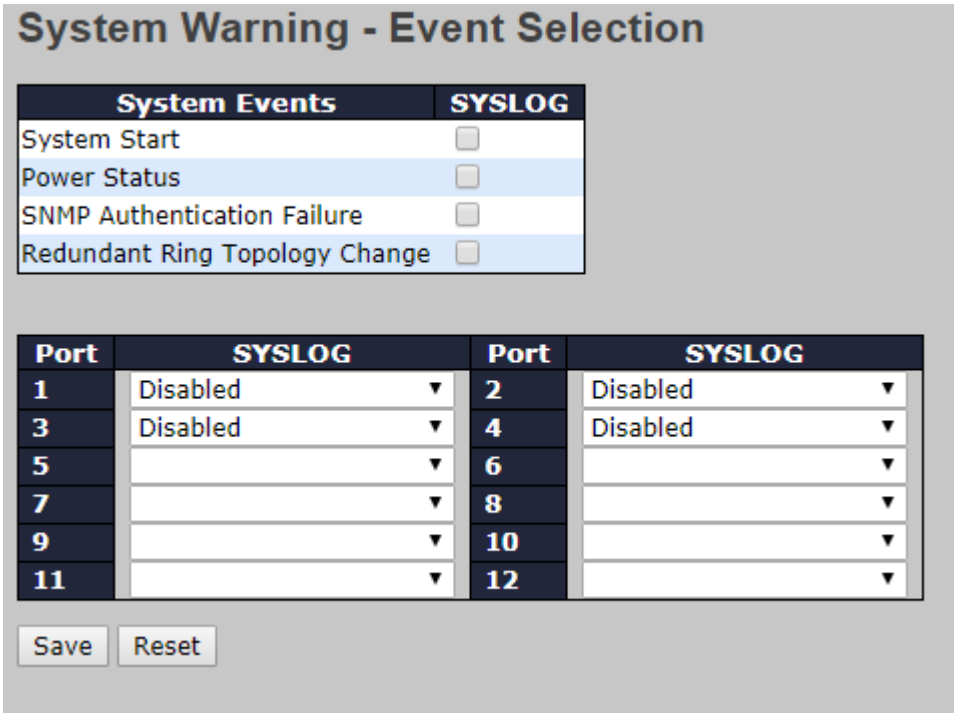
The SYSLOG is a protocol that transmits event notifications across networks.




| Label | Description |
|---|---|
| **Server Mode** | Indicates existing server mode. When the mode operation is enabled, the syslog message will be sent to syslog server. The syslog protocol is based on UDP communications and received on UDP port 514 and the syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always be sent even if the syslog server does not exist. Possible modes are:<br>**Enabled**: enable server mode<br>**Disabled**: disable server mode |
| **Server Address** | Indicates the IPv4 host address of syslog server. If the switch provides DNS functions, it also can be a host name. |
| **Syslog Level** | Select the severity level for the syslog messages to be logged. The list contains:<br>**Error**: Log error messages.<br>**Warning**: Log warning messages.<br>**Notice**: Log messages that represent significant condition but not errors.<br>**Informational**: Log informational messages. |

## Event Selection

SYSLOG and SMTP are two warning methods supported by the system. Check the corresponding box to enable the system event warning method you want. Please note that the checkbox cannot be checked when SYSLOG or SMTP is disabled.

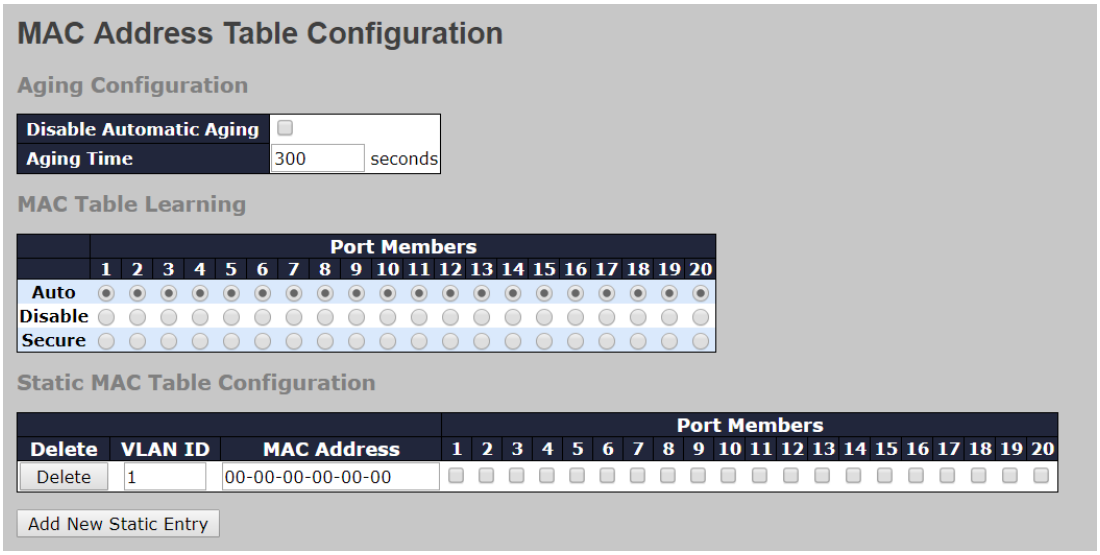



| Label | Description |
|---|---|
| **System Cold Start** | Sends out alerts when the system is restarted |
| **Power Status** | Sends out alerts when power is up or down |
| **SNMP Authentication Failure** | Sends out alert when SNMP authentication fails |
| **Redundant-Ring Topology Change** | Sends out alerts when Redundant-Ring topology changes |
| **Port Event SYSLOG** | ■ **Disable**<br>■ **Link Up**<br>■ **Link Down**<br>■ **Link Up & Link Down** |
| **Apply** | Click to activate the configurations |
| **Help** | Shows help file |

# 1.11 Monitor and Diag

## 1.11.1 MAC Table

The MAC address table can be configured on this page. You can set timeouts for entries in the dynamic MAC table and configure the static MAC table here.




## Aging Configuration

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

You can configure aging time by entering a value in the box below in seconds; for example, **Age Time** seconds.

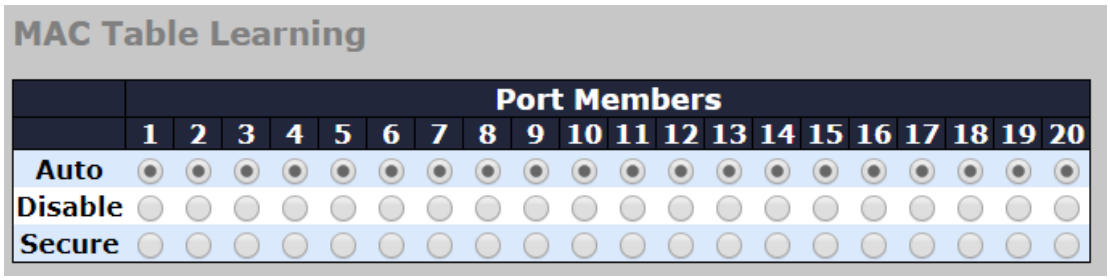
The allowed range is 10 to 1000000 seconds.

You can disable the automatic aging of dynamic entries by checking **Disable Automatic Aging**.

## MAC Table Learning

If the learning mode for a given port is grayed out, it means another module is in control of the mode, and thus the user cannot change the configurations. An example of such a module is MAC-Based authentication under 802.1X.

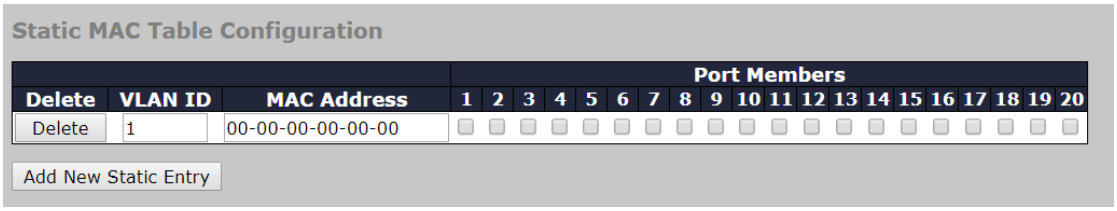
You can configure the port to dynamically learn the MAC address based upon the following settings:



| Label | Description |
|---|---|
| **Auto** | Learning is done automatically as soon as a frame with unknown SMAC is received. |
| **Disable** | No learning is done. |
| **Secure** | Only static MAC entries are learned, all other frames are dropped. Note: make sure the link used for managing the switch is added to the static Mac table before changing to secure learning mode, otherwise the management link will be 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 Configurations

The static entries in the MAC table are shown in this table. The static MAC table can contain up to 64 entries. The entries are for the whole stack, not for individual switches. The MAC table is sorted first by VLAN ID and then by MAC address.




| Label | Description |
|---|---|
| **Delete** | Check to delete an entry. It will be deleted during the next save. |
| **VLAN ID** | The VLAN ID for the entry |
| **MAC Address** | The MAC address for the entry |
| **Port Members** | Checkmarks indicate which ports are members of the entry. Check or uncheck to modify the entry. |
| **Adding New Static Entry** | Click to add a new entry to the static MAC table. You can specify the VLAN ID, MAC address, and port members for the new entry. Click **Save** to save the changes. |

## MAC Table

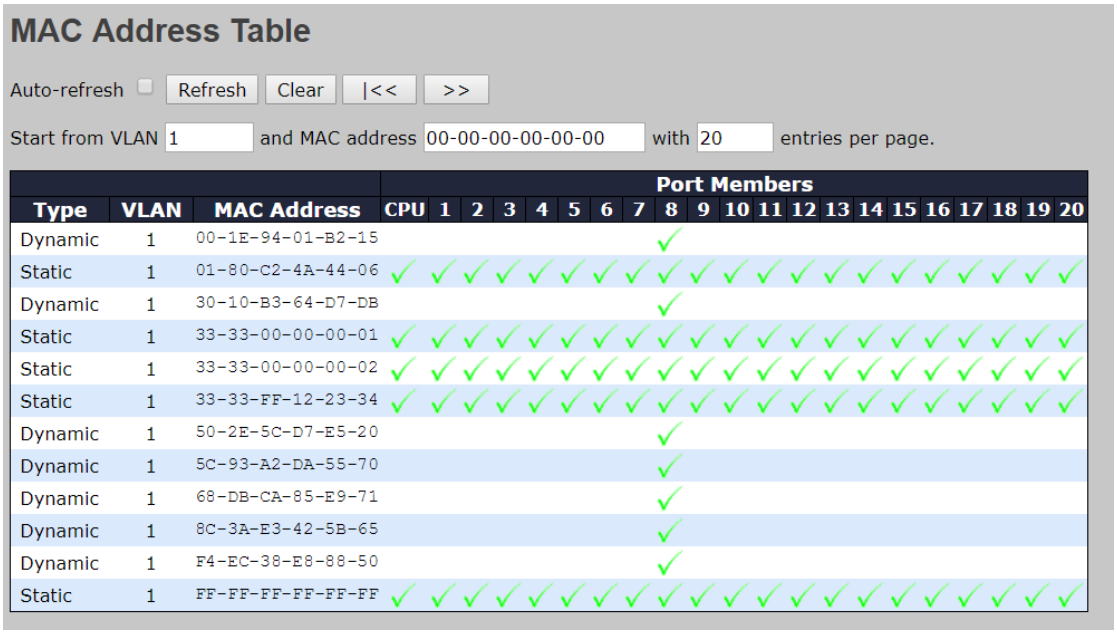
Each page shows up to 999 entries from the MAC table, with a default value of 20, selected by the **Entries Per Page** input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

Each page shows up to 999 entries from the MAC table, with a default value of 20, selected by

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** 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 clicking **Refresh** - assume the value of the first displayed entry, allows 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 it reaches the end, the text "**no more entries**" is shown in the displayed table. Use the **|<<** button to start over.




| Label | Description |
|---|---|
| **Type** | Indicates whether the entry is a static or 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. |

## 1.11.2 Port Statistics

### Traffic Overview

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

**Port Statistics Overview**

Auto-refresh Refresh Clear

| Port | Description | Packets | | Bytes | | Errors | | Drops | | Filtered |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received |
| 1 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | | 42716 | 18891 | 5721301 | 3208070 | 0 | 0 | 0 | 0 | 1967 |
| 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 |

| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied. |
| **Packets** | The number of received and transmitted packets per port |
| **Bytes** | The number of received and transmitted bytes per port |
| **Errors** | The number of frames received in error and the number of incomplete transmissions per port |
| **Drops** | The number of frames discarded due to ingress or egress congestion |
| **Filtered** | The number of received frames filtered by the forwarding process |
| **Auto-refresh** | Check to enable an automatic refresh of the page at regular intervals. |
| **Refresh** | Updates the counter entries, starting from the current entry ID. |
| **Clear** | Flushes all counters entries |

### Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port drop-down list to decide the details of which switch port to be displayed.

The displayed counters include the total number for receive and transmit, the size for receive and transmit, and the errors for receive and transmit.

### Detailed Statistics – Total Receive & Transmit

**Detailed Port Statistics Port 1**

Port 1 ▾ Auto-refresh ☐ Refresh Clear

| Receive Total | | Transmit Total | |
|---|---|---|---|
| Rx Packets | 0 | Tx Packets | 0 |
| Rx Octets | 0 | Tx Octets | 0 |
| Rx Unicast | 0 | Tx Unicast | 0 |
| Rx Multicast | 0 | Tx Multicast | 0 |
| Rx Broadcast | 0 | Tx Broadcast | 0 |
| Rx Pause | 0 | Tx Pause | 0 |
| **Receive Size Counters** | | **Transmit Size Counters** | |
| Rx 64 Bytes | 0 | Tx 64 Bytes | 0 |
| Rx 65-127 Bytes | 0 | Tx 65-127 Bytes | 0 |
| Rx 128-255 Bytes | 0 | Tx 128-255 Bytes | 0 |
| Rx 256-511 Bytes | 0 | Tx 256-511 Bytes | 0 |
| Rx 512-1023 Bytes | 0 | Tx 512-1023 Bytes | 0 |
| Rx 1024-1526 Bytes | 0 | Tx 1024-1526 Bytes | 0 |
| Rx 1527- Bytes | 0 | Tx 1527- Bytes | 0 |
| **Receive Queue Counters** | | **Transmit Queue Counters** | |
| Rx Q0 | 0 | Tx Q0 | 0 |
| Rx Q1 | 0 | Tx Q1 | 0 |
| Rx Q2 | 0 | Tx Q2 | 0 |
| Rx Q3 | 0 | Tx Q3 | 0 |
| Rx Q4 | 0 | Tx Q4 | 0 |
| Rx Q5 | 0 | Tx Q5 | 0 |
| Rx Q6 | 0 | Tx Q6 | 0 |
| Rx Q7 | 0 | Tx Q7 | 0 |

| Label | Description |
|---|---|
| **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, including FCS, except 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** | The number of MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation |
| **Rx Drops** | The number of frames dropped due to insufficient receive buffer 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 a valid CRC |
| **Rx Oversize** | The number of long[2] frames received with a valid CRC |
| **Rx Fragments** | The number of short[1] frames received with an invalid CRC |
| **Rx Jabber** | The number of long[2] frames received with an invalid CRC |
| **Rx Filtered** | The number of received frames filtered by the forwarding process |
| **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 |

1. Short frames are frames smaller than 64 bytes.
2. Long frames are frames longer than the maximum frame length configured for this port.

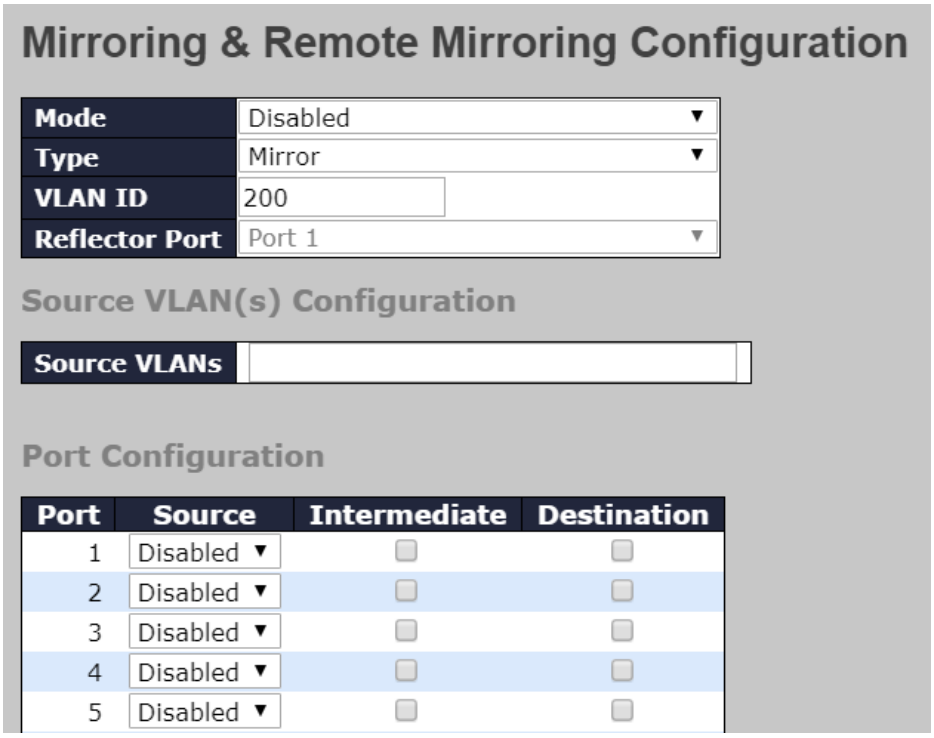
### 1.11.3 Port Monitoring

You can configure port mirroring on this page. To solve network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow. The traffic to be copied to the mirror port is selected as follows:

All frames received on a given port (also known as ingress or source mirroring).

All frames transmitted on a given port (also known as egress or destination mirroring).

Port to mirror is also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port. Disabled option disables mirroring.

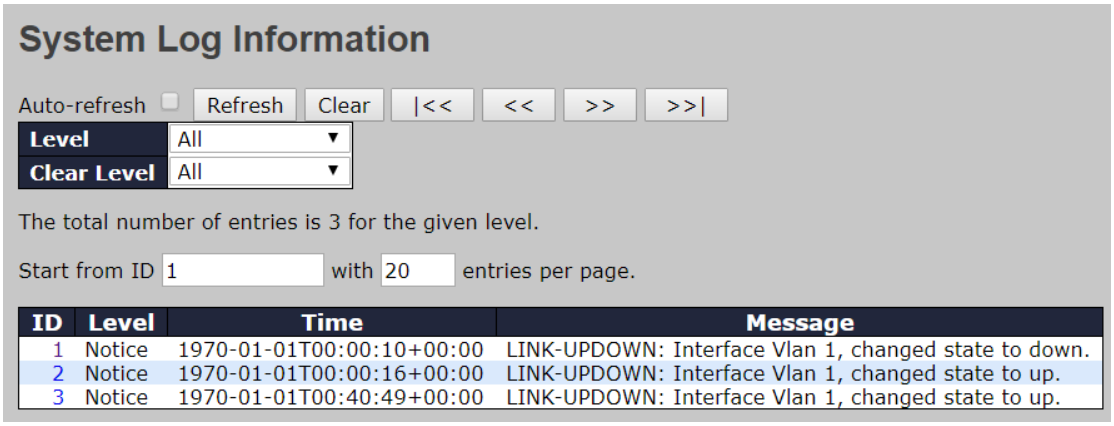



| Label | Description |
|---|---|
| **Mode** | Enable or disable this function. |
| **Type** | Mirror: the switch is running on mirror mode. The source port(s) and destination port are located on this switch.<br>Source: the switch is a source node for monitor flow. The source port(s) and intermediate port(s) are located on this switch.<br>Intermediate: the switch is a forwarding node for monitor flow and the switch is an option node. The object is to forward traffic from source |

| | |
|---|---|
| | switch to destination switch. The intermediate ports are located on this switch.<br>Destination: the switch is an end node for monitor flow. The destination port(s) and intermediate port(s) are 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** | Select a reflector port. This port carries all the mirrored traffic at source switch. |
| **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** | The logical port for the settings contained in the same row. The CPU also can be selected. |
| **Source** | Selects mirror mode.<br>**Disabled**: Neither frames transmitted nor frames received are mirrored.<br>**Both**: Frames received and frames transmitted are mirrored on the Intermediate/Destination port.<br>**Rx only**: Frames received on this port are mirrored on the Intermediate/Destination port. Frames transmitted are not mirrored.<br>**Tx only**: Frames transmitted on this port are mirrored on the Intermediate/Destination port. Frames received are not mirrored. |
| **Intermediate** | Select intermediate port. This checkbox is designed for Remote Mirroring. The intermediate port is a switched port to connect to other switch. All packets that are going through intermediate port will be tagged when the mirror function is enabled. |
| **Destination** | Select destination port. This checkbox is designed for mirror or Remote Mirroring. The destination port is a switched port that you receive a copy of traffic from the source port. |

### 1.11.4 System Log Information

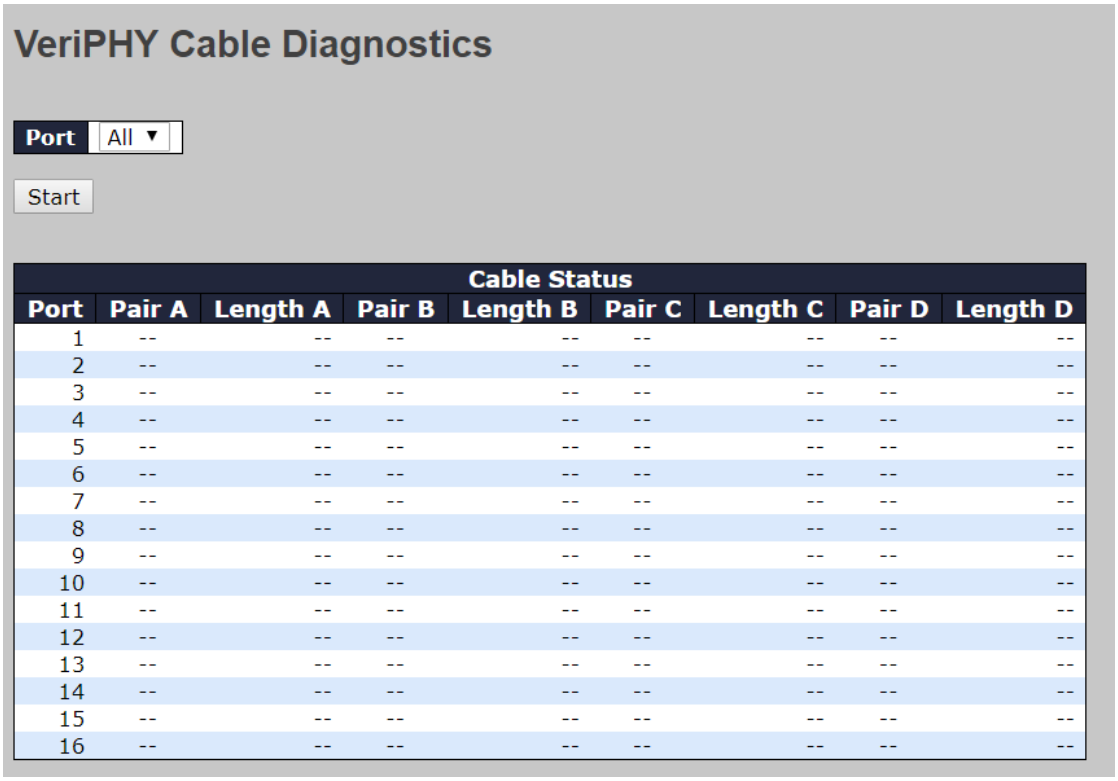
This page provides switch system log information.




| Label | Description |
|---|---|
| **ID** | The ID (>= 1) of the system log entry |
| **Level** | The level of the system log entry. The following level types are supported:<br>**Notice:** Log messages that represent significant condition but not errors.<br>**Informational**: Log informational messages.<br>**Warning**: Log warning messages.<br>**Error**: Log error messages.<br>**All**: Log all messages. |
| **Time** | The time of the system log entry |
| **Message** | The MAC address of the switch |
| **Auto-refresh** | Check this box to enable an automatic refresh of the page at regular intervals. |
| **Refresh** | Updates system log entries, starting from the current entry ID |
| **Clear** | Flushes all system log entries |
| **\|<<** | Updates system log entries, starting from the first available entry ID |
| **<<** | Updates system log entries, ending at the last entry currently displayed |
| **>>** | Updates system log entries, starting from the last entry currently displayed. |
| **>>\|** | Updates system log entries, ending at the last available entry ID. |

## 1.11.5 VeriPHY Cable Diagnostics

This page allows you to perform VeriPHY cable diagnostics.




| Port | Pair A | Length A | Pair B | Length B | Pair C | Length C | Pair D | Length D |
|---|---|---|---|---|---|---|---|---|
| 1 | -- | -- | -- | -- | -- | -- | -- | -- |
| 2 | -- | -- | -- | -- | -- | -- | -- | -- |
| 3 | -- | -- | -- | -- | -- | -- | -- | -- |
| 4 | -- | -- | -- | -- | -- | -- | -- | -- |
| 5 | -- | -- | -- | -- | -- | -- | -- | -- |
| 6 | -- | -- | -- | -- | -- | -- | -- | -- |
| 7 | -- | -- | -- | -- | -- | -- | -- | -- |
| 8 | -- | -- | -- | -- | -- | -- | -- | -- |
| 9 | -- | -- | -- | -- | -- | -- | -- | -- |
| 10 | -- | -- | -- | -- | -- | -- | -- | -- |
| 11 | -- | -- | -- | -- | -- | -- | -- | -- |
| 12 | -- | -- | -- | -- | -- | -- | -- | -- |
| 13 | -- | -- | -- | -- | -- | -- | -- | -- |
| 14 | -- | -- | -- | -- | -- | -- | -- | -- |
| 15 | -- | -- | -- | -- | -- | -- | -- | -- |
| 16 | -- | -- | -- | -- | -- | -- | -- | -- |

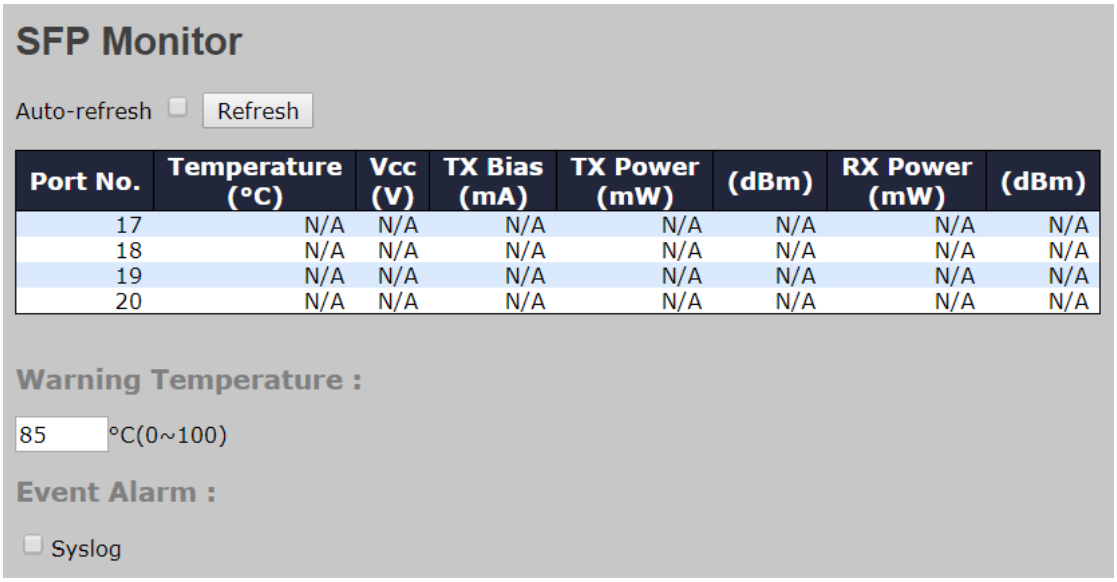
Press **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY diagnostics is only accurate for cables 7 - 140 meters long.

10 and 100 Mbps ports will be disconnected while running VeriPHY diagnostics. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

| Label | Description |
|---|---|
| **Port** | The port for which VeriPHY Cable Diagnostics is requested |
| **Cable Status** | Port: port number<br>Pair: the status of the cable pair<br>Length: the length (in meters) of the cable pair |

### 1.11.6 SFP Monitor

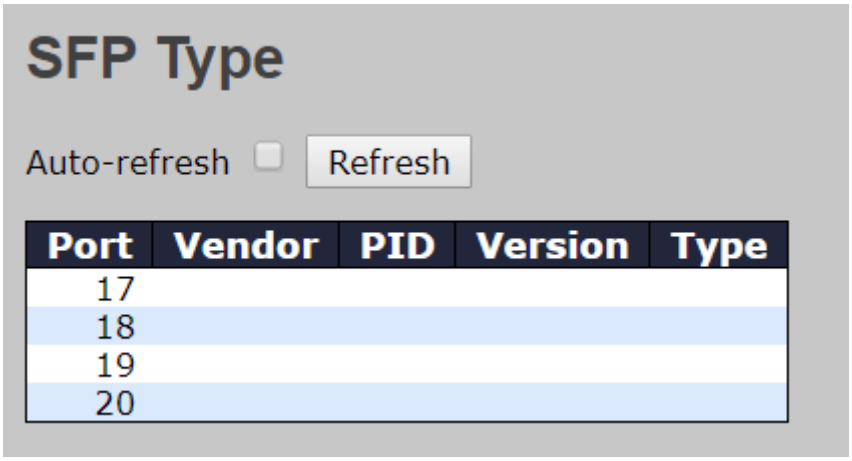
SFP modules with DDM (Digital Diagnostic Monitoring) function can measure the temperature of the apparatus, helping you monitor the status of connection and detect errors immediately. You can manage and set up event alarms through DDM Web interface.




| Port No. | Temperature (°C) | Vcc (V) | TX Bias (mA) | TX Power (mW) | (dBm) | RX Power (mW) | (dBm) |
|---|---|---|---|---|---|---|---|
| 17 | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| 18 | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| 19 | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| 20 | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

### 1.11.7 SFP Type

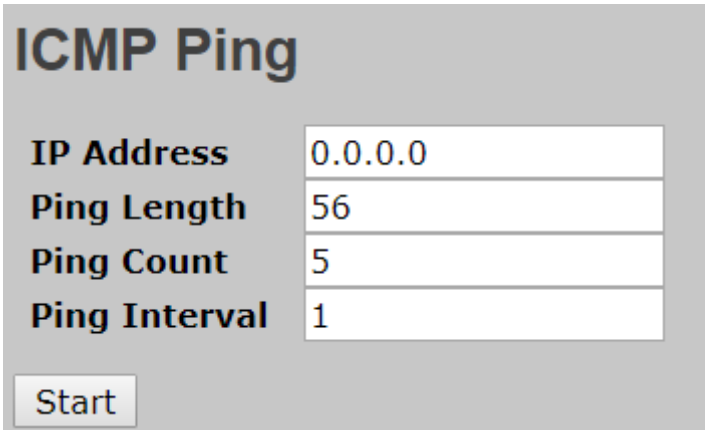
This page shows the details of the SFP port. For each port, the summary displays the SFP type, the vendor name and serial number.




| Port | Vendor | PID | Version | Type |
|---|---|---|---|---|
| 17 | | | | |
| 18 | | | | |
| 19 | | | | |
| 20 | | | | |

### 1.11.8 Ping / Ping6

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.



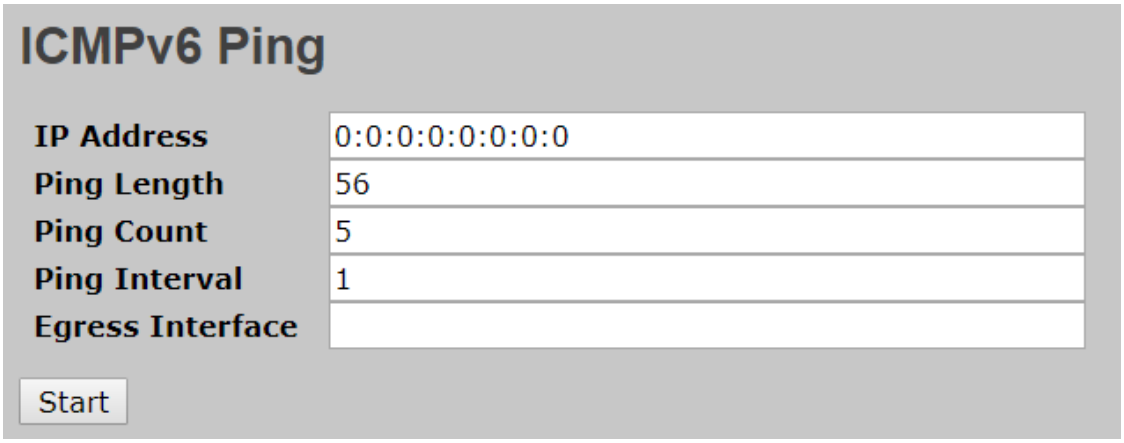

After you press **Start**, five ICMP packets will be transmitted, and the sequence number and roundtrip time will be displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING6 server ::10.10.132.20
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

| Label | Description |
|---|---|
| **IP Address** | The destination IP Address |
| **Ping Size** | The payload size of the ICMP packet. Values range from 8 to 1400 bytes. |

## IPv6 Ping



PING6 server ::192.168.10.1

sendto

sendto

sendto

sendto

sendto

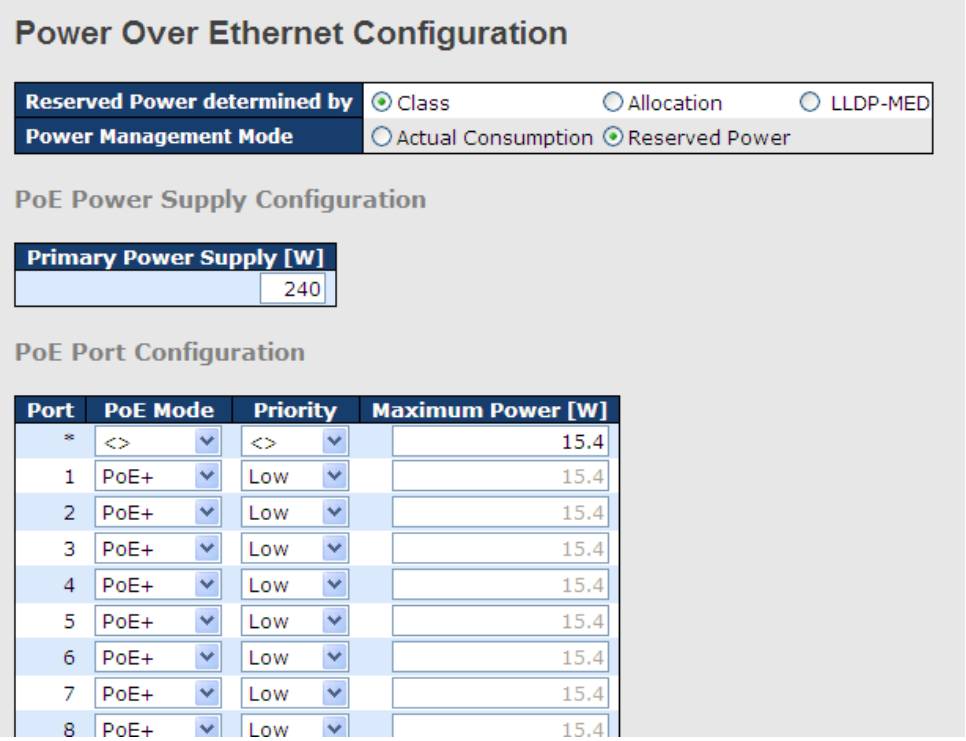
Sent 5 packets, received 0 OK, 0 bad

# 1.12 POE (only for POE Model)

## 1.12.1 Configuration

PoE is an acronym for Power Over Ethernet.

Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.



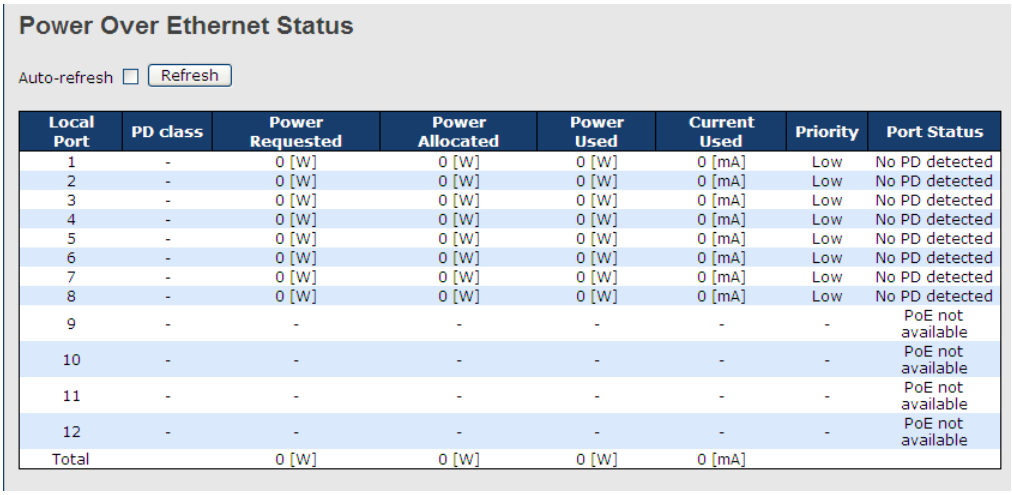

| Label | Description |
|---|---|
| **Reserved Power determined by** | There are three modes for configuring how the ports/PDs may reserve power. |

| | |
|---|---|
| | 1. Allocated mode: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.<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. |
| **Primary and Backup Power Source** | Some switches support having two PoE power supplies. One is used as primary power source, and one as backup power source. If the switch doesn't support backup power supply only the primary power supply settings will be shown. In case that the primary power source fails the backup power source will take over. For being able to determine the amount of power the PD may use, it must be defined what amount of power the primary and backup power sources can deliver. |

| | |
|---|---|
| | Valid values are in the range 0 to 2000 Watts. |
| **Port** | This is the logical port number for this row.<br>Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for. |
| **PoE Mode** | The PoE Mode represents the PoE operating mode for the port.<br><br>Disabled: PoE disabled for the port.<br><br>PoE : Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W)<br><br>PoE+ : Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W) |
| **Priority** | The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.<br><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.(The maximum allowed value is 30 W.) |

## 1.12.2 Status

This page allows the user to inspect the current status for all PoE ports.



Power Over Ethernet Status

Auto-refresh ☐ Refresh

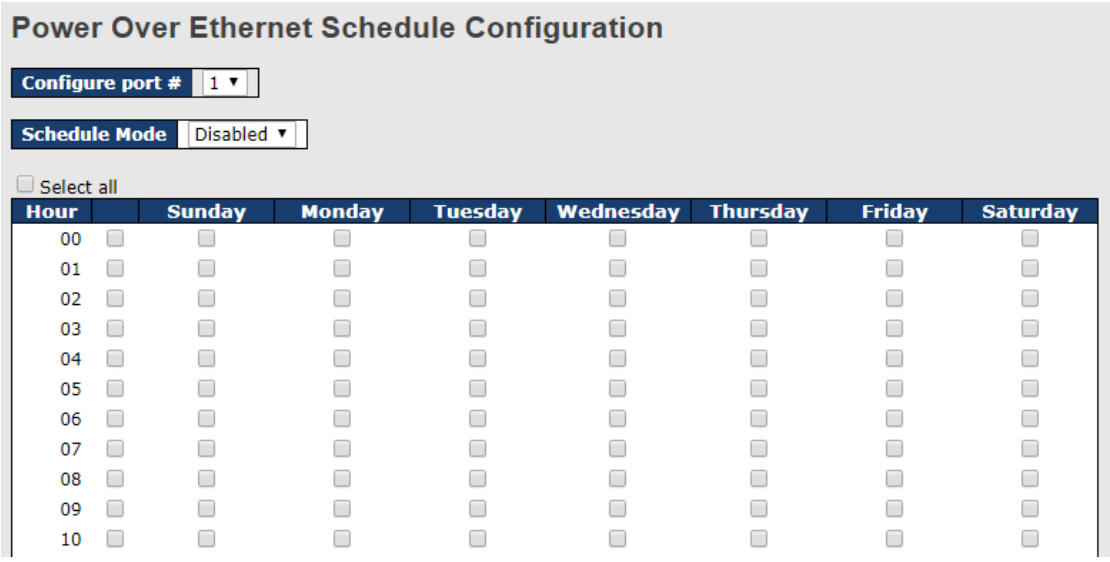
| Local Port | PD class | Power Requested | Power Allocated | Power Used | Current Used | Priority | Port Status |
|---|---|---|---|---|---|---|---|
| 1 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 2 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 3 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 4 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 5 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 6 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 7 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 8 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 9 | - | - | - | - | - | - | PoE not available |
| 10 | - | - | - | - | - | - | PoE not available |
| 11 | - | - | - | - | - | - | PoE not available |
| 12 | - | - | - | - | - | - | PoE not available |
| Total | | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | | |

| Label | 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>Five 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 |
| **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** | 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><br>PoE turned OFF - PoE disabled : PoE is disabled by user.<br><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><br>No PD detected - No PD detected for the port.<br><br>PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down. |

| | |
|---|---|
| | PoE turned OFF - PD is off.<br><br>Invalid PD - PD detected, but is not working correctly. |

## 1.12.3 PoE Schedule

Configure port number of the switch supplying power around the clock on this page. The users can set the desired power policy accordingly.



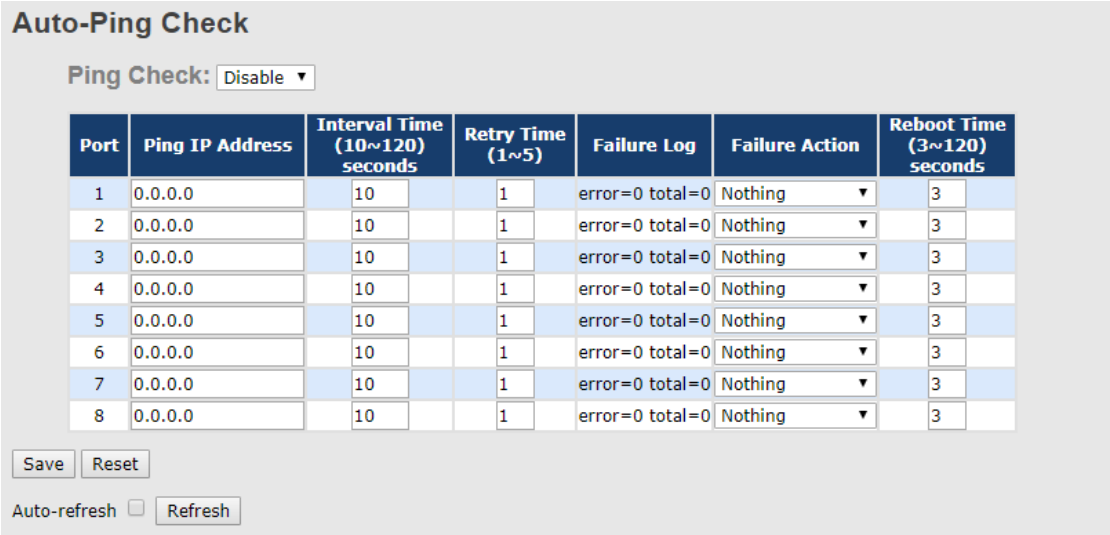

| Label | Description |
|---|---|
| **Configure Port** | Choose port of the switch port number to configure |
| **Mode** | Indicates the PoE Schedule mode operation. Possible modes are:<br>Enabled: Enable PoE Schedule configure.<br>Disabled: Disable PoE Schedule configure. |
| **Daily Schedule Form** | Check Hours and Week checkbox to set port working times. |

## 1.12.4 PoE Auto-Ping

This page can monitor the real-time status of connected power devices.

Switch could send alive-checking packets to assure the connected devices are in working state.

If the connected devices fail to response,switch could reactivate the connected devives to assure the reliability of the network.



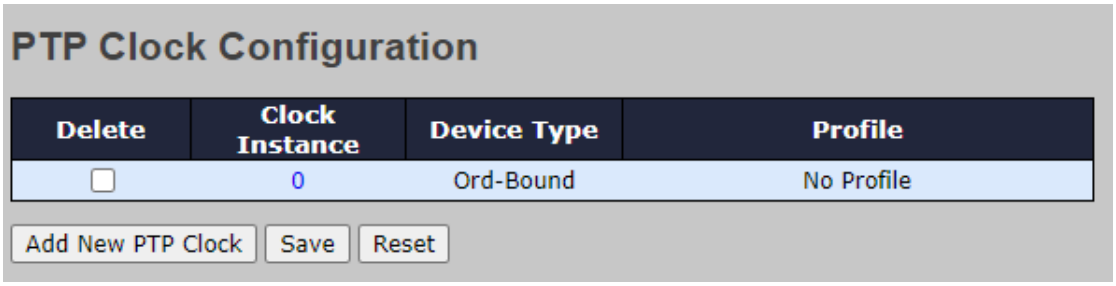

| Label | Description |
|---|---|
| **Ping Check** | Indicates the Ping Check mode operation. Possible modes are:<br>Enabled: Enable Auto-Ping configure.<br>Disabled: Disable Auto-Ping configure |
| **Port** | Port of the switch port number. |
| **Ping IP Address** | Send alive-checking packets to ip adress. |
| **Interval Time** | Set (10~120)seconds to control switch sending alive-checking packets each Interval Time. |
| **Retry Time** | If the connected devices fail to response, retry until numbers of set frequency . |
| **Failure Log** | Monitor connection status.<br>If the connected devices succeed to response,total plus one;<br>if the connected devices fail to response,error plus one. |
| **Failure Action** | If the connected devices fail to response,the users can choose five Features;<br>Nothing: Nothing to do.<br>Restart Forever: Try to supply power and cut power until connected devices success.<br>Restart Once:Try to cut power and supply power once.<br>Power On:Supply power to device.<br>Power Off:Stop supplying power to device. |
| **Reboot Time** | Configure the switch delay (3-120)seconds sending alive-checking packet when the users choose<br>Restart Forever / Restart Once Fratures. |

# 1.13 Synchronization(only for P-Series Model)

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

## PTP-Configuration

This page allows the user to configure and inspect the current PTP clock settings.

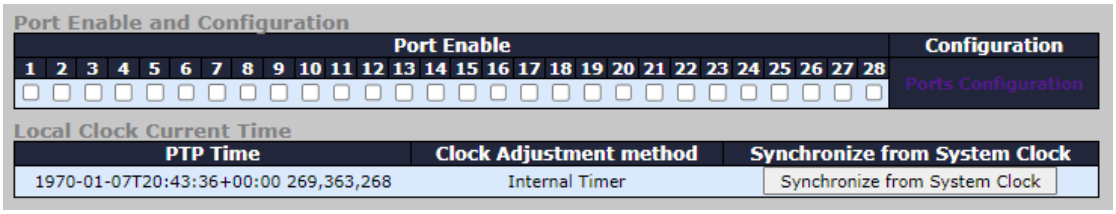



| Label | Description |
|---|---|
| **Delete** | Check this box and click on 'Save' to delete the clock instance. |
| **Clock Instance** | Indicates the Instance of a particular Clock Instance [0..3].<br>Click on the Clock Instance number to edit the Clock details. |
| **Devcie Type** | Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3]. More instances may use the same clock domain, e.g. a Boundary clock and a Transparent clock. Only one Slave or Boundary clock is allowed within the same Clock domain. |
| **Profile** | Indicates the Type of the Clock Instance. There are five Device Types.<br>**1. Ord-Bound -** clock's Device Type is Ordinary-Boundary Clock.<br>**2. P2p Transp -** clock's Device Type is Peer to Peer Transparent Clock.<br>**3. E2e Transp -** clock's Device Type is End to End Transparent Clock.<br>**4. Master Only -** clock's Device Type is Master Only.<br>**5. Slave Only -** clock's Device Type is Slave Only. |

## PTP Clock Instance

This page allows the user to inspect and configure the current PTP clock settings

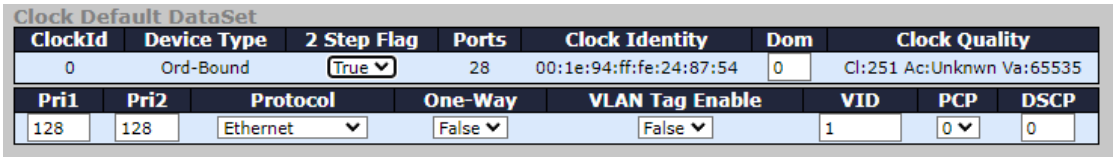
## Lock Current Time




| Label | Description |
|---|---|
| **PTP Time** | Shows the actual PTP time with nanosecond resolution. |
| **Clock Adjustment Method** | Shows the actual clock adjustment method. The method depends on the available hardware. |
| **Synchronize from System Clock** | Activate this button to synchronize the System Clock to PTP Time. |
| **Ports Configuration** | Click to edit the port data set for the ports assigned to this clock instance. |

## Clock Default Dataset

The clock default data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members defined at clock creation time, the Dynamic members defined by the system, and the configurable members which can be set here.




| Label | Description |
|---|---|
| **Clock ID** | An internal instance id (0..3) |
| **Device Type** | Indicates the Type of the Clock Instance. There are five Device Types.<br>**1. Ord-Bound -** Clock's Device Type is Ordinary-Boundary Clock.<br>**2. P2p Transp -** Clock's Device Type is Peer to Peer Transparent Clock.<br>**3. E2e Transp -** Clock's Device Type is End to End Transparent Clock.<br>**4. Master Only -** Clock's Device Type is Master Only. |

| | |
|---|---|
| | **5. Slave Only -** Clock's Device Type is Slave Only. |
| **2 Step Flag** | True if two-step Sync events and Pdelay_Resp events are used |
| **Ports** | The total number of physical ports in the node |
| **Clock Identity** | It shows unique clock identifier |
| **Dom** | Clock domain [0..127]. |
| **Clock Quality** | The clock quality is determined by the system, and holds 3 parts: Clock Class, Clock Accuracy and OffsetScaledLog Variance as defined in IEEE1588.<br>The Clock Accuracy values are defined in IEEE1588 table 6 (Currently the clock Accuracy is set to 'Unknown' as default). |
| **Pri 1** | Clock priority 1 [0..255] used by the BMC master select algorithm. |
| **Pri 2** | Clock priority 2 [0..255] used by the BMC master select algorithm. |
| **Protocol** | Transport protocol used by the PTP protocol engine<br>Ethernet PTP over Ethernet multicast<br>EthernetMixed PTP using a combination of Ethernet multicast and unicast<br>IPv4Multi PTP over IPv4 multicast<br>IPv4Mixed PTP using a combination of IPv4 multicast and unicast<br>IPv4Uni PTP over IPv4 unicast |
| **One-Way** | If true, one way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests. |
| **VLAN Tag Enable** | The VLAN Tag Enable parameter is ignored, because the tagging is controlled by the VLAN configuration. |
| **VID** | VLAN Identifier used for tagging the VLAN packets. |
| **PCP** | Priority Code Point value used for PTP frames. |

## Clock Current Data Set

The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic

Clock Current DataSet

| stpRm | Offset From Master | Mean Path Delay |
|---|---|---|
| 0 | 0.000,000,000 | 0.000,000,000 |

| Label | Description |
|---|---|
| **stpRm** | Steps Removed : It is the number of PTP clocks traversed from the grandmaster to the local slave clock. |

| | |
|---|---|
| **Offset form master** | Time difference between the master clock and the local slave clock, measured in ns. |
| **Mean Path Delay** | The mean propagation time for the link between the master and the local slave |

## Clock Parent Data Set

The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

Clock Parent DataSet

| Parent Port ID | Port | PStat | Var | Rate | GrandMaster ID | GrandMaster Clock Quality | Pri1 | Pri2 |
|---|---|---|---|---|---|---|---|---|
| 00:1e:94:ff:fe:24:87:54 | 0 | False | 0 | 0 | 00:1e:94:ff:fe:24:87:54 | Cl:251 Ac:Unknwn Va:65535 | 128 | 128 |

| Label | Description |
|---|---|
| **Parent Port Identity** | Clock identity for the parent clock, if the local clock is not a slave, the value is the clocks own id. |
| **Port** | Port Id for the parent master port |
| **P Stat** | Parents Stats (always false). |
| **Var** | It is observed parent offset scaled log variance |
| **Change Rate** | Observed Parent Clock Phase Change Rate. i.e. the slave clocks rate offset compared to the master. (unit = ns per s). |
| **Grand Master Identity** | Clock identity for the grand master clock, if the local clock is not a slave, the value is the clocks own id. |
| **Grand Master Clock Quality** | The clock quality announced by the grand master (See description of Clock Default DataSet:Clock Quality) |
| **Pri 1** | Clock priority 1 announced by the grand master |
| **Pri 2** | Clock priority 2 announced by the grand master. |

## Clock Time Properties Data Set

The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, i.e. the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation.

The valid values for the Time Source parameter are:

Clock Time Properties DataSet

| UtcOffset | Valid | leap59 | leap61 | Time Trac | Freq Trac | ptp Time Scale | Time Source |
|---|---|---|---|---|---|---|---|
| 0 | False | False | False | False | False | True | 160 |

| Address | Description |
|---|---|
| 16 (0x10) | ATOMIC_CLOCK |

| | |
|---|---|
| 32 (0x20) | GPS |
| 48 (0x30) | TERRESTRIAL_RADIO |
| 64 (0x40) | PTP |
| 80 (0x50) | NTP |
| 96 (0x60) | HAND_SET |
| 144 (0x90) | OTHER |
| 160 (0xA0) | INTERNAL_OSCILLATOR |

## Servo Parameters

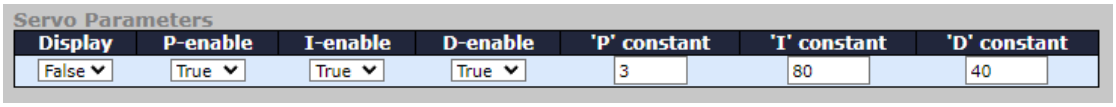
The default clock servo uses a PID regulator to calculate the current clock rate. i.e.

clockAdjustment =

OffsetFromMaster/ P constant +

Integral(OffsetFromMaster)/ I constant +

Differential OffsetFromMaster)/ D constant




| Label | Description |
|---|---|
| **Display** | If true then Offset From Master, MeanPathDelay and clockAdjustment are logged on the debug terminal |
| **P-enable** | If true the P part of the algorithm is included |
| **I-enable** | If true the I part of the algorithm is included |
| **D-enable** | If true the D part of the algorithm is included |
| **'P' constant** | [1..1000] see above |
| **'I' constant** | [1..10000] see above |
| **'D' constant** | [1..10000] see above |

## Filter Parameters

The default delay filter is a low pass filter, with a time constant of

2**DelayFilter*DelayRequestRate.

If the DelayFilter parameter is set to 0, the delay filter uses the same algorithm as the offset filter.

The default offset filter uses a minimum offset or a mean filter method

i.e. The minimum measured offset during Period samples is used in the calculation.

The distance between two calculations is Dist periods.

Note: In configurations with Timestamp enabled PHYs, the period is automatically increased, if (period*dist < SyncPackets pr sec/4), i.e. max 4 adjustments are made pr sec.

If Dist is 1 the offset is averaged over the Period,

If Dist is >1 the offset is calculated using 'min' offset.

Filter Parameters

| Filter Type | Delay Filter | Period | Dist |
|---|---|---|---|
| Basic | 6 | 1 | 2 |

| Label | Description |
|---|---|
| **Delay Filter** | See above |
| **Filter Type** | Shows the filter type used which can be either the basic filter or an advanced filter that can be configured to use only a fraction of the packets received (i.e. the packets that have experienced the least latency). |
| **Period** | See above |
| **Dist** | See above |
| **Height** | The height of the sample window measured in microseconds (only applicable to advanced offset filter). |
| **Percentage** | The percentage of sync packets (with smallest delay) used by the offset filter (only applicable to advanced offset filter). |
| **Reset Threshold** | The threshold in micro seconds at which the offset filter will be reset and the slave clock synchronized to the master. |

## Unicast Slave Configuration

When operating in IPv4 Unicast mode, the slave is configured up to 5 master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then request Sync messages from the selected master.

Unicast Slave Configuration

| Index | Duration | ip_address | grant | CommState |
|---|---|---|---|---|
| 0 | 100 | 0.0.0.0 | 0 | IDLE |
| 1 | 100 | 0.0.0.0 | 0 | IDLE |
| 2 | 100 | 0.0.0.0 | 0 | IDLE |
| 3 | 100 | 0.0.0.0 | 0 | IDLE |
| 4 | 100 | 0.0.0.0 | 0 | IDLE |

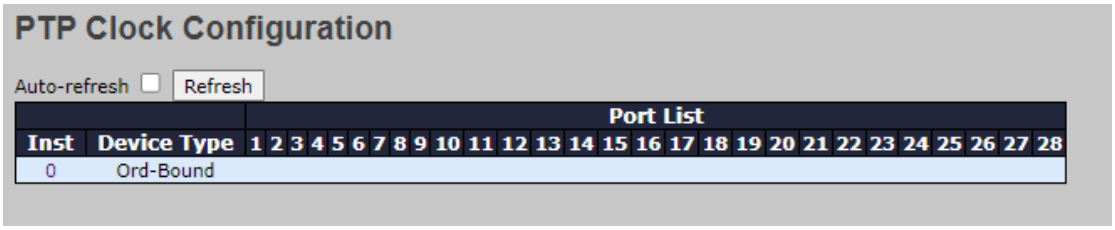
Save Reset

| Label | Description |
|---|---|
| **Duration** | The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds. |
| **IP_address** | IPv4 Address of the Master clock |
| **Grant** | The granted repetition period for the sync message |
| **Comm State** | The state of the communication with the master, possible values |

| | |
|---|---|
| | are:<br>**IDLE :** The entry is not in use.<br>**INIT :** Announce is sent to the master (Waiting for a response).<br>**CONN :** The master has responded.<br>**SELL :** The assigned master is selected as current master.<br>**SYNC :** The master is sending Sync messages. |

## PTP Status

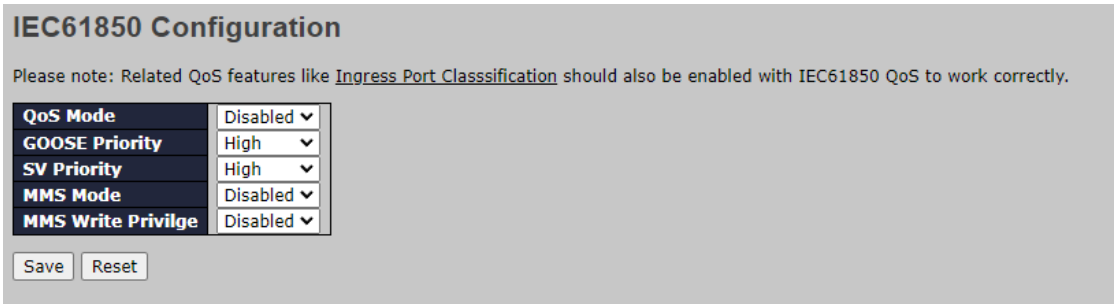
This page allows the user to inspect the current PTP clock settings.




| Label | Description |
|---|---|
| **Inst** | Indicates the Instance of a particular Clock Instance [0..3].<br>Click on the Clock Instance number to monitor the Clock details. |
| **Device Type** | Indicates the Type of the Clock Instance. There are five Device Types.<br>**1. Ord-Bound -** Clock's Device Type is Ordinary-Boundary Clock.<br>**2. P2p Transp -** Clock's Device Type is Peer to Peer Transparent Clock.<br>**3. E2e Transp -** Clock's Device Type is End to End Transparent Clock.<br>**4. Master Only -** Clock's Device Type is Master Only.<br>**5. Slave Only -** Clock's Device Type is Slave Only. |
| **Port List** | Shows the ports configured for that Clock Instance. |

# 1.14 IEC61850 (only for P-Series Model)

The page allow use setting IEC-61850 Packet forwarding priority .

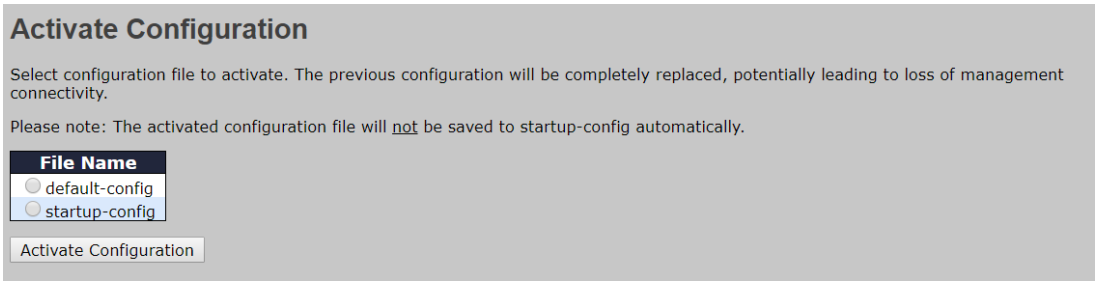



| Label | Description |
|---|---|
| **QoS Mode** | Enable or Disable the QOS Mode. |
| **GOOSE Priority** | Setting Goose packet forwarding priority. (high / medium / low ) |
| **SV Priority** | Setting Sampled Values protocol forwarding priority. (high / medium / low ) |
| **MMS Mode** | Enable or Disable the MMS Mode. |
| **MMS Write Privilge** | Enable or Disable the MMS Write Privilge. Warning: Enabling this causes possible security risk, as MMS communication is not authenticated! |

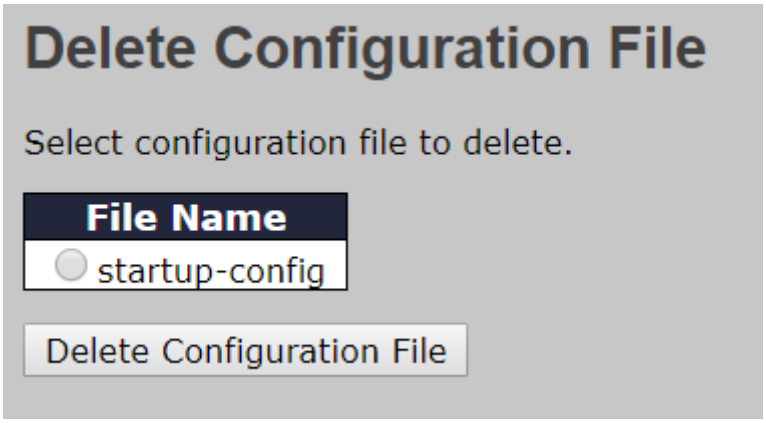
# 1.15 Configuration

This setting allows you to activate or delete configuration files. Simply select the files to be activated or deleted and press the button.

## 1.15.1 Activate




## 1.15.2 Delete




# 1.16 Save

You can save current configurations as a startup configuration file.


# 1.17 Troubleshooting

## 1.17.1 Factory Defaults

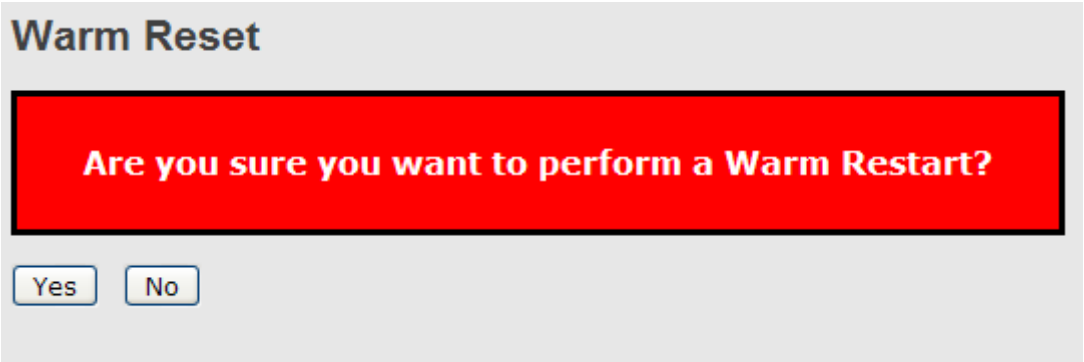
You can reset the configuration of the stack switch on this page. Only the IP configuration is retained.


| Label | Description |
|---|---|
| **Yes** | Click to reset the configuration to factory defaults |
| **No** | Click to return to the Port State page without resetting |

## 1.17.2 System Reboot

You can reset the stack switch on this page. After reset, the system will boot normally as if you

have powered on the devices.




| Label | Description |
|---|---|
| **Yes** | Click to reboot device |
| **No** | Click to return to the **Port State** page without rebooting |

# 9000 Series

# CLI User manual

# INTRODUCTION TO CLI

## 1.1 General Introduction

The **9000** Series of industrial Ethernet core switches provide a number of configuration/management methods. The first and very basic is serial console access. This method is also called out-of-band management and is only available when a terminal or administrator PC can be physically connected to the local 9000 Series switch at the CONSOLE port using RJ45 to RS-232 console cable. Accessing the switch via CONSOLE port allows the user to use Command Line Interface (CLI) to manage and configure the device. The out-of-band management is relatively useful when you lose the network connection to the device.

The out-of-band management via console access, using a command line (CLI), is familiar to most network engineers. For engineers that are not comfortable using CLI, this device can also be managed using any standard Web Browser in a more user friendly 'point-and-click' method. Therefore, in most configuration scenarios, the console will only be used to initially configure the 9000 IP address, so that the device may be accessed via the other methods which require working TCP/IP.

After the device has been properly configured for the application and placed into service, a third method of configuration/management can be employed using Simple Network Management Protocol (SNMP). The operator will use SNMP management software to manage and monitor the 9000 Series switches on a network. This requires some configuration of the device to allow SNMP management. In addition, the network management platform will need to import and compile the proprietary MIB (management information base) file so that the manager knows "how" to manage the 9000 devices.

## 1.2 CONSOLE Operation

Using the provided accessory cable, connect the 9000 "CONSOLE" port (RJ-45) to the PC terminal communications port (DB9). Run any terminal emulation program (HyperTerminal, PuTTY, TeraTerm Pro, etc.) and configure the communication parameters as follows:

Speed: 115,200
Data: 8 bits
Parity: none
Stop bits: 1
Flow Control: None
From a cold start, the following screen will be displayed. At the "Username" prompt, **enter 'admin' with no password**.

```
Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from the
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.
Platform: VCore-III (MIPS32 24KEc) JAGUAR
RAM: 0x80000000-0x88000000 [0x80021798-0x87fe0000 available]
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
== Executing boot script in 2.000 seconds - enter ^C to abort
RedBoot> fi lo -a -f managed
RedBoot> go
Press ENTER to get started
Username: admin
Password:
```

## 1.3 CLI Modes

The Command Line Interface (CLI) of 9000 series is mainly divided into four basic modes; these are User mode, EXEC mode, Config mode and Config Interface mode. After entering the username and password, you start from the EXEC mode (prompted with "#"). The commands available in User mode and EXEC mode are limited. For more advanced configurations, you must enter Config mode or Config Interface mode. In each mode, a question mark (?) at the system prompt can be issued to obtain a list of commands available for each command mode. The following table provides a brief overview of modes available in this device.

| Mode | Prompt | Enter Method | Exit Method |
|---|---|---|---|
| User mode | > | enable | disable |
| EXEC mode | # | Enter authorized username and password | Exit, logout |
| Global Config Mode | (config)# | Enter "configure terminal" after "#" | End, exit, do logout |
| Config Interface Mode | (config-if)# | Specify interface, interface type and number after (config)# | End, exit, do logout |

## 1.4 Quick Keys

There are several useful quick keys you can use when editing command lines.

| Keyboard | Action |
|---|---|
| ? | Issue "?" to get a list of commands available in the current mode. |
| Up arrow key | To view the previous entered commands. |
| Down arrow key | To view the previous entered commands. |
| Tab key | To complete an unfinished command. |

## 1.5 Command Syntax

Commands introduced in this user manual are written using the coherent symbols and easy-to-understand syntax and style. Although users can issue Help command to complete a desired command in CLI, it is useful to understand frequently-used symbols and syntax conventions. The following table lists the syntax conventions used in this user manual together with an example.

**Example: (config-if-vlan)# ip address { { <address> <netmask> } | { dhcp [ fallback <fallback_address> <fallback_netmask> [ timeout <fallback_timeout> ] ] } }**

| Symbol | Function | Example | Explanation |
|---|---|---|---|
| < > (Angle bracket) | Enter a value, alphanumeric strings or keywords. | <address> <netmask> | Enter IP address and subnet mask. |
| [ ] (Square bracket) | This is an optional parameter. | [ fallback <fallback_address> <fallback_netmask> [ timeout <fallback_timeout> ] ] | Fallback parameter is an optional item. |
| { } (Curly bracket) | A curly bracket has the following two functions:<br>1. If there are more than two options available, a curly bracket can be used to | { { <address> <netmask> } \| { dhcp [ fallback <fallback_address> <fallback_netmask> [ timeout <fallback_timeout> ] ] } } | At least specify one option to complete the command. |

| | | | |
|---|---|---|---|
| | separate them.<br>2. The uter curly bracket means that this is a must parameter. At least one value should be specified. | | |
| **\|** (Vertical bar) | Use a vertical bar to separate options. | { { <address> <netmask> } **\|** { dhcp [ fallback <fallback_address> <fallback_netmask> [ timeout <fallback_timeout> ] ] } } | Enter IP address or use DHCP to assign IP address automatically. |

## 1.6 Basic Configurations

This section introduces users how to change the default IP address to the desired one and save the current running configurations to startup configurations. For detailed introductions to commands, please see section 1.7,1.8, 1.9.

### *1.1.1 Configuring IPv4 Address*

IP address: 192.168.0. 101
Subnet mask: 255.255.255.0

```
# config terminal
(config)# interface vlan 1
(config-if-vlan)# ip address 192.168.0.101 255.255.255.0
(config-if-vlan)# exit
(config)# exit
# show ip interface brief
Vlan Address          Method  Status
---- -------------------- -------- ------
   1 192.168.0.101/24    Manual  DOWN
```

### *1.1.2 Enter Config Interface Mode*

• Enter Port 3's Config Interface mode. #

```
config terminal
(config)# interface GigabitEthernet 1/3
(config-if)#
```

*Note: 1/3 means Ethernet Interface 1, Port 3.*

• Enter Port 1~3's Config Interface mode. #

```
config terminal
(config)# interface GigabitEthernet 1/1-3
(config-if)#
```

*Note: 1/1-3 means Ethernet Interface 1, Port 1 to Port 3.*

• Enter Port 1~3 & Port 5's Config Interface mode. #

```
config terminal
(config)# interface GigabitEthernet 1/1-3,5
(config-if)#
```

*Note: 1/1-3,5 means Ethernet Interface 1, Port 1 to Port 3 and Port 5.*

### 1.1.3 Save Configurations

```
# copy running-config startup-config
Building configuration...
%Saving 1469 bytes to flash:startup-config
#
```

### 1.1.4 Restart the Device

```
# reload cold
%Cold reload in progress, please stand by.
#

Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from the
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.

RedBoot> fi lo -d managed
Image loaded from 0x80040000-0x80ae54cc
RedBoot> go

Press ENTER to get started
```

### 1.1.5 Load Factory Defaults

Load factory default settings

```
# reload defaults
% Reloading defaults. Please stand by.
```

Load factory defaults but keep IP settings

```
# reload defaults keep-ip
% Reloading defaults, attempting to keep VLAN 1 IP address. Please stand by.
```

### 1.1.6 Show System and Software Information

```
# show version

MEMORY          : Total=77679 KBytes, Free=51457 KBytes, Max=51417 KBytes
MAC Address     : xx-xx-xx-00-00-01
Previous Restart : Cold

System Contact  :
System Name     :
System Location :
System Time     : 2019-01-01T00:28:35+00:00
System Uptime   : 00:28:39

Active Image
------------------
Image           managed
```

```
Version          :
Date             : 2015-01-01T00:03:06+00:00

Alternative Image
------------------
Image            : managed.bk
Version
Date             : 2015-08-03T16:21:44+08:00
------------------
SID : 1
------------------
Software Version : V1.038
Build Date       : 2015-08-03T16:33:15+08:00
```

### *1.1.7 Show Running Configurations*

```
# show running-config
Building configuration...
username admin privilege 15 password none
!
vlan 1
!
!
!
no smtp server
spanning-tree mst name 00-02-ab-00-00-01 revision 0
!
interface GigabitEthernet 1/1
 no spanning-tree
!
interface GigabitEthernet 1/2
 no spanning-tree
!
interface GigabitEthernet 1/3
 no spanning-tree
!
interface GigabitEthernet 1/4
 no spanning-tree
!
-- more --, next page: Space, continue: g, quit: ^C
```

### *1.1.8 Show History Commands*

```
# show history
  config t
  exit
  config t
  ip arp ex
  exit
```

```
> show history
 config t
  interface GigabitEthernet 1/3
  exit
  interface GigabitEthernet 1/1-5
  exit
```

```
interface GigabitEthernet 1/1-3,5,7
flowcontrol on
exit
show interface * status
disable
show clock detail
show dot1x
show history
```

### *1.1.9 Help*

Help command can be issued in User, Exec, and Global Config mode to get a hint message describing how to use "show" command to get help from CLI.

```
# help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

### *1.1.10 Logout*

To close an active terminal session, issue the "logout" command in User or EXEC mode.

```
(config)# exit
# logout

Press ENTER to get started
```

```
# disable
> logout

Press ENTER to get started
```

## 1.7 Commands in User Mode

When you successfully login in Command Line Interface, you are in EXEC Mode (prompted with "#"). To enter User mode, issue "disable" command after # prompt. Then you will be directed to User mode with ">" prompt.

```
Username: admin
Password:
#
# disable
>
```

In User mode, only limited commands are available. These commands are used for clearing statistics, entering Exec mode and pinging the specified destination. To configure a function, you should enter Config mode or Config Interface mode.

### *1.7.1 > clear ip arp*

**Syntax:** > clear ip arp

**Explanation:** Clear ARP cache.

### *1.7.2 > clear lldp statistics*

**Syntax:** > clear lldp statistics

**Explanation:** Clear LLDP statistics.

### *1.7.3 > clear statistics*

**Syntax:** > clear statistics {[ interface ] ( <port_type> [ <v_port_type_list> ] )}

<port_type>: Specify the interface type.

[ <v_port_type_list>: Specify the ports that you want to clear.

**Explanation:** Clear statistics of the specified interfaces.

### *1.7.4 > enable*

**Syntax:** > enable [ <new_priv> ]

[ <new_priv: 0-15> ]: Choose a privilege level.

**Explanation:** Enter the EXEC mode.

### *1.7.5 > exit*

**Syntax:** > exit

**Explanation:** Return to the previous mode. Issuing this command in User mode will logout the Command Line Interface.

### *1.7.6 > help*

**Syntax:** > help

**Explanation:** Provide help messages.

### *1.7.7 > logout*

**Syntax:** > logout
**Explanation:** Logout the Command Line Interface.

### *1.7.8 > ping ip*

**Syntax:** > ping ip <v_ip_addr> [ repeat <count> ] [ size <size> ] [ interval <seconds> ]

<v_ip_addr>: Specify IPv4 address that you want to ping.

[ repeat <count> ]: The number of packets that are sent to the destination IP or host.

[ size <size> ]: The size of the packet.

[ interval <seconds> ]: Timeout interval. The ping test is successful only when it receives echo reply from the destination IP or host within the time specified here.

**Explanation:** To carry out ping tests on the specified destination IPv4 address or host.

### *1.7.9 > ping ipv6*

**Syntax:** > ping ipv6 <v_ipv6_addr> [ repeat <count> ] [ size <size> ] [ interval <seconds> ] [ interface vlan <v_vlan_id> ]

<v_ipv6_addr>: Specify IPv6 address that you want to ping.

[ repeat <count> ]: The number of packets that are sent to the destination IP or host.

[ size <size> ]: The size of the ping packet.

[ interval <seconds> ]: Timeout interval. The ping test is successful only when it receives echo reply from the destination IP or host within the time specified here.

[ interface vlan <v_vlan_id> ]:

**Explanation:** To carry out ping tests on the specified destination IPv6 address or host.

### *1.7.10 show commands*

In User mode, “show” commands can be issued to display current status or settings of a certain command. They will be introduced in Section 3.9 “Commands in Config Mode”.

## 1.8 Commands in EXEC Mode

### *1.8.1 # clear access management statistics*

**Syntax:** # clear access management statistics

**Explanation:** Clear access (HTTP, HTTPs, SNMP, Telnet, SSH) management statistics.

### *1.8.2 # clear access-list ace statistics*

**Syntax:** # clear access-list ace statistics

**Explanation:** Clear access list entry statistics.

### *1.8.3 # clear dot1x statistics*

**Syntax:** # clear dot1x statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]

**Parameter:**

[ interface ( <port_type> [ <v_port_type_list> ] ) ]: Specify the interface that you want to clear.

**Explanation:** Clear (the specified interfaces') dot1x statistics.

### *1.8.4 # clear ip arp*

**Syntax:** # clear ip arp

**Explanation:** Clear ARP cache.

### *1.8.5 # clear ip dhcp detailed statistics*

**Syntax:** # clear ip dhcp detailed statistics { server | client | snooping | relay | helper | all } [ interface ( <port_type> [ <in_port_list> ] ) ]

**Explanation:** Clear IP DHCP statistics.

**Parameter:**

{server | client | snooping | relay | helper | all}: Specify the type of information that you want to clear.

[ interface ( <port_type> [ <in_port_list> ] ) ]: Specify the interface type and port number.

### *1.8.6 # clear ip dhcp server binding <ip>*

**Syntax:** # clear ip dhcp server binding <ip>

**Parameter:**

<ip>: Specify the IP address for this server binding setup.

**Explanation:** Clear DHCP server binding cache in reletion to the specified IP address.

### *1.8.7 # clear ip dhcp server binding { automatic | manual | expired }*

**Syntax:** # clear ip dhcp server binding { automatic | manual | expired }

**Parameter:**

{automatic | manual | expired}: Specify the server binding mode.

**Explanation:** Clear automatic, manual or expired server binding caches.

### *1.8.8 # clear ip dhcp server statistics*

**Syntax:** # clear ip dhcp server statistics

**Explanation:** Clear DHCP server statistics.

### *1.8.9 # clear ip dhcp relay statistics*

**Syntax:** # clear ip dhcp relay statistics

**Explanation:** Clear IP DHCP Relay statistics.

### *1.8.10 # clear ip dhcp snooping statistics*

**Syntax:** # clear ip dhcp snooping statistics [ interface ( <port_type> [ <in_port_list> ] ) ]

**Explanation:** Clear IP DHCP Snooping statistics.

### *1.8.11 # clear ip igmp snooping*

**Syntax:** # clear ip igmp snooping [ vlan <v_vlan_list> ] statistics

**Explanation:** Clear IP IGMP Snooping statistics.

### *1.8.12 # clear ip statistics*

**Syntax:** # clear ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]

**Explanation:** Clear IPv4 statistics for system, interface and ICMP.

### *1.8.13 # clear ipv6 mld snooping*

**Syntax:** # clear ipv6 mld snooping [ vlan <v_vlan_list> ] statistics

**Explanation:** Clear statistics for IPv6 MLD Snooping.

### *1.8.14 # clear ipv6 neighbors*

**Syntax:** # clear ipv6 neighbors

**Explanation:** Clear the table for IPv6 neighbors.

### *1.8.15 # clear ipv6 statistics*

**Syntax:** # clear ipv6 statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]

**Explanation:** Clear IPv6 statistics for system, interface and ICMP.

### *1.8.16 # clear lacp statistics*

**Syntax:** # clear lacp statistics

**Explanation:** Clear LACP statistics.

### *1.8.17 # clear lldp statistics*

**Syntax:** # clear lldp statistics

**Explanation:** Clear LLDP statistics.

### *1.8.18 # clear logging*

**Syntax:** # clear logging [ info ] [ warning ] [ error ] [ switch <switch_list> ]

**Explanation:** Clear specific syslog events.

### *1.8.19 # clear mac address-table*

**Syntax:** # clear mac address-table

**Explanation:** Clear MAC address table.

### *1.8.20 # clear spanning-tree*

**Syntax:** # clear spanning-tree {{statistics [interface (<port_type> [<v_port_type_list>])]}|{detected-protocols [ interface ( <port_type> [ <v_port_type_list_1> ] ) ] } }

**Explanation:** Clear specific interfaces' Spanning Tree statistics.

### *1.8.21 # clear statistics*

**Syntax:** # clear statistics [ interface ] ( <port_type> [ <v_port_type_list> ] )

**Explanation:** Clear Fast Ethernet and/or Gigabit Ethernet interfaces' statistics.

### *1.8.22 # config terminal*

**Syntax:** # config terminal

**Explanation:** Enter the Global Config mode.

**Example:**

```
# config t
(config)#
```

### *1.8.23 # copy*

**Syntax:** # copy { startup-config **|** running-config **|** <source_path> } { startup-config **|** running-config **|** <destination_path> } [ syntax-check ]

{startup-config **|** running-config **|** <source_path>}: Specify the file type that you want to copy from. This can be "startup-config", "running-config" or a specific source file in flash or TFTP server.

{startup-config **|** running-config **|** <destination_path>}: Specify the file type that you want to copy to. This can be "startup-config", "running-config" or a specific destination file in flash or TFTP server.

**Explanation:** Save running configurations to startup configurations.

```
# copy running-config startup-config
Building configuration...
% Saving 1596 bytes to flash:startup-config
#
```

**Explanation:** Save startup configurations to running configurations.

```
# copy startup-config running-config
Building configuration...
% Saving 1596 bytes to flash:startup-config
#
```

**Explanation:** Save running configurations to Flash 201

```
# copy running-config Flash:201
Building configuration...
% Saving 1487 bytes to flash:201
# dir
Directory of flash:
     r-   1970-01-01   00:00:00          284  default-config
     rw   2015-01-01   01:56:32         1487  startup-config
     rw   2015-01-01   01:56:49         1487  201
3 files, 3258 bytes total.
```

### *1.8.24 # delete*

**Syntax:** # delete <path>

**Explanation:** Delete a file saved in Flash.

**Parameters:**

<Path : word>: Name of the file in Flash to be deleted.

**Example:** Delete a file named 201 in Flash.

```
# dir
Directory of flash:
    r- 1970-01-01 00:00:00      284 default-config
    rw 2015-01-01 01:56:32     1487 startup-config
    rw 2015-01-01 01:56:49     1487 201
3 files, 3258 bytes total.
# delete flash:201
# dir
Directory of flash:
    r- 1970-01-01 00:00:00      284 default-config
    rw 2015-01-01 01:56:32     1487 startup-config
2 files, 1771 bytes total.
```

### *1.8.25 # dir*

**Explanation:** Display files in flash.

**Example:**

```
# dir
Directory of flash:
    r-    1970-01-01  00:00:00        284  default-config
    rw    2015-01-01  01:56:32       1487  startup-config
    rw    2015-01-01  01:56:49       1487  201
3 files, 3258 bytes total.
```

### *1.8.26 #disable&#enable*

**Explanation:** Return to user mode or enter exec mode.

```
# disable
>
>
> enable
#
#
# enable 0
>
```

### *1.8.27 # dot1x*

**Syntax:** # dot1x initialize [ interface ( <port_type> [ <plist> ] )

[ interface ( <port_type> [ <plist> ] ) ]: Specify the type of interface that you intend to use. “*” means all interfaces.

<plist>: Specify the ports that apply to this command.

**Explanation:** To initialize dot1x function in an interface immediately.

### *1.8.28 # firmware swap*

**Syntax:** # firmware swap

**Explanation:** Use the other standby firmware image file uploaded to flash.

### *1.8.29 # firmware upgrade*

**Syntax:** # firmware upgrade <TFTPServer_path_file : word>

<TFTPServer_path_file : word>: Specify the TFTP server IP address and firmware filename.

**Explanation:** Upgrade the firmware image.

### *1.8.30 # ip dhcp retry interface vlan*

**Syntax:** # ip dhcp retry interface vlan <vlan_id>

<vlan_id>: Specify the valid VLAN ID for DHCP query.

**Explanation:** Restart the DHCP query process.

### *1.8.31 # more*

**Syntax:** # more <path>

<path>: Specify the filename.

**Explanation:** Display file in Flash or in TFTP server.

### *1.8.32 # ping ip*

**Syntax:** # ping ip <v_ip_addr> [ repeat <count> ] [ size <size> ] [ interval <seconds> ]

**Explanation:** Ping the specified IP.

**Parameters:**

<addr>: Specify the IPv4 address or IPv6 address for ping test.

### *1.8.33 # ping ipv6*

**Syntax:** #ping ipv6 <v_ipv6_addr> [ repeat <count> ] [ size <size> ] [ interval <seconds> ] [ interface vlan <v_vlan_id> ]

< v_ipv6_addr >: Specify the IPv4 address or IPv6 address for ping test.

**Explanation:** Ping the specified IPv6 address.

**Parameters:**

[repeat <count>]: The number of echo packets will be sent.

[ size <size> ]: The size or length of echo packets.

[ interval <seconds> ]: The time interval between each ping request.

[ interface vlan <v_vlan_id> ]: Specify the VLAN ID.

### *1.8.34 # reload cold*

**Syntax:** # reload cold

**Explanation:** Perform a cold reload on the system.

### *1.8.35 # reload defaults*

**Syntax:** # reload defaults [keep-ip]

**Explanation:** Restore the device to factory default settings.

**Parameters:**

[keep-ip]: Keep VLAN 1 IP setting.

### *1.8.36 # send*

**Syntax:** # send { * **|** <session_list> **|** console 0 **|** vty <vty_list> } <message>

**Explanation:** Send messages to other tty lines.

**Parameters:**

{ * **|** <session_list> **|** console 0 **|** vty <vty_list> }: Choose one of the options.

* : Specify "*" to denote all tty users.

<session_list>: Specify a session number between 0 and 16.

console 0: This means primary terminal line.

<vty_list>: Send a message to a virtual terminal.

<message>: Enter a message in 128 characters that you want to send.

### *1.8.37 # terminal editing*

**Syntax:** # terminal editing

**Explanation:** Enable command line editing.

**Show: >** show terminal
# show terminal

**Negation:** # no terminal editing

### *1.8.38 # terminal exec-timeout*

**Syntax:** # terminal exec-timeout <0-1440> [<0-3600>]

**Parameters:**

<0-1440>: Specify the timeout value in minutes.

[<0-3600>]: Specify the timeout value in seconds.

**Explanation:** Set up terminal timeout value.

**Show: >** show terminal
# show terminal

**Negation:** # no terminal exec-timeout

### *1.8.39 # terminal history size*

**Syntax:** # terminal history size <0-32>

**Parameters:**

<0-32>: Specify the current history size. “0” means to disable.

**Explanation:** Set up terminal history size.

**Show:** **>** show terminal
# show terminal

**Negation:** # no terminal history size

### *1.8.40 # terminal length*

**Syntax:** # terminal length <0 or 3-512>

**Parameters:**

<0 or 3-512>: Specify the lines displayed on the screen. “0” means no pausing.

**Explanation:** Set up terminal length.

**Show:** **>** show terminal
# show terminal

**Negation:** # no terminal length

### *1.8.41 # terminal width*

**Syntax:** # terminal width <0 or 40-512>

**Parameters:**

<0 or 40-512>: Specify the width displayed on the screen. “0” means unlimited width.

**Explanation:** Set up terminal display width.

**Show:** **>** show terminal
# show terminal

**Negation:** # no terminal width

### *1.8.42 # no port-security shutdown*

**Syntax:** # no port-security shutdown [interface (<port_type>[<v_port_type_list>])]

**Explanation:** Reopen ports that are shutdown or disabled by Port Security function.

**Parameters:**

[interface (<port_type>[<v_port_type_list>])]: Specify the port type and port numbers that you want to reopen.

### *1.8.43 show commands*

In Exec mode, “show” commands can be issued to display current status or settings of a certain command. They will be introduced in Section 3.9 “Commands in Config Mode”.

## 1.9 Commands in Config Mode

### *1.9.1 (config)# aaa authentication login*

**Syntax:** (config)# aaa authentication login {console | telnet | ssh | http}{{local | radius | tacacs}[{local | radius | tacacs } [ { local **|** radius **|** tacacs } ] ] }

**Explanation:** Configure the authentication method for the client.

**Parameters:**

{ console **|** telnet **|** ssh **|** http }: Specify one of the authentication clients.

{{local **|** radius **|** tacacs}[{local **|** radius **|** tacacs}[{local **|** radius **|** tacacs}]]}: Specify one of the authentication methods for the specified client. At least one method needs to be specified. Users can specify three methods at most.

**local:** Use the local user database on the switch for authentication.

**radius:** Use remote RADIUS server(s) for authentication.

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

***NOTE:*** *Methods that involve remote servers will time out if the remote servers are offline. In this case the next method is tried. Each method is tried 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.*

**Example:** Set the Console client to use remote RADIUS server(s) for authentication.

```
# config t
(config)# aaa authentication login console radius
```

**Negation:** (config)# no aaa authentication login { console **|** telnet **|** ssh **|** http }

**Show:** # show aaa

### *1.9.2 (config)# access management*

**Syntax:** (config)# access management <access_id> <access_vid> <start_addr> [ to <end_addr> ] { [ web ] [ snmp ] [ telnet ] | all }

**Explanation:** Create an access management rule.

**Parameters:**

<access_id: 1-16>: Specify an ID for this access management entry.

<access_vid>: Indicates the VLAN ID for the access management entry.

<start_addr> [ to <end_addr> ]: Indicate the starting and ending IP address for the access management entry.

{ [ web ] [ snmp ] [ telnet ] | all }: Specify matched hosts can access the switch from which interface.

**Example:** Allow IP 192.168.0.1 to 192.168.0.10 to access the device via Web, SNMP and Telnet.

```
# config t
(config)# access management 1 1 192.168.0.1 to 192.168.0.10 all
```

**Negation:** (config)# no access management
(config)# no access management <access_id>

**Show:** # show access management [ statistics | <access_id_list> ]

**Clear:** # clear access management statistics

## *1.9.3 (config)# access-list*

### *1.9.3.1 (config)# access-list ace*

**Syntax:** (config)# access-list ace <AceId : 1-256> [ action {deny | filter | permit}] [ dmac-type {any| broadcast | multicast | unicast } ] [frame-type {any| arp|etype|ipv4|ipv4-icmp|ipv4-tcp|ipv4-udp|ipv6|ipv6-icmp|ipv6-tcp|ipv6-udp} ] [ingress {any | interface <PORT_TYPE> }] [logging] [next { <AceId : 1-256>|last}] [policy <PolicyId : 0-255>] [rate-limiter {<RateLimiterId : 1-16>|disable}] [redirect {disable| interface <PORT_TYPE>}] [shutdown] [tag {any|tagged|untagged}] [tag-priority {0-1| 0-3| 2-3| 4-5| 4-7| 6-7| <TagPriority : 0-7>|any}] [vid { <Vid : 1-4095>|any}]
**Explanation:** Configure an access control list.

**Parameters:**

<AceId : 1-256>: Specify access control list ID that applies to this rule.

[ action {deny | filter | permit}]: Specify the action that applies to this rule.

[ dmac-type {any| broadcast | multicast | unicast } ]: Specify destination MAC type that applies to this rule.

[frame-type {any| arp|etype|ipv4|ipv4-icmp|ipv4-tcp|ipv4-udp|ipv6|ipv6-icmp|ipv6-tcp|ipv6-udp} ]: Specify the frame type that applies to this rule.

[ingress {any | interface <PORT_TYPE> }]: Specify the ingress port.

[logging]: Enable logging function.

[mirror]: Enable the function of mirroring frames to destination mirror port.

[next{<AceId : 1-256>|last}]: Insert the current ACE ID before the next ACE ID or put the ACE ID to the last one.

[policy <PolicyId : 0-255>]: Specify the policy ID.

[rate-limiter {<RateLimiterId : 1-16>|disable}]: Specify the rate limit ID or disable this function.

[redirect {disable | interface <PORT_TYPE>}]: Redirect frames to a specific port or disable this function.

[shutdown]: Enable shutdown function.

[tag {any|tagged|untagged}]: Specify whether frames should be tagged or untagged.

[tag-priority {0-1 | 0-3 | 2-3 | 4-5 | 4-7 | 6-7 | <TagPriority : 0-7> | any}]: Specify the priority value.

[vid { <Vid : 1-4095>|any}]: Specify the VLAN ID.

**Show:** # show access-list [interface [(<port_type> [<v_port_type_list>])]] [rate-limiter [<rate_limiter_list>]] [ace statistics [ <ace_list> ] ]

**Negation:** (config)# no access-list ace <ace_list>

**Clear:** # clear access-list ace statistics

### *1.9.3.2 (config)# access-list ace update*

**Syntax:** (config)# access-list ace update <AceId : 1-256> [action {deny | filter | permit}] [dmac-type {any| broadcast | multicast | unicast } ] [frame-type {any | arp|etype | ipv4 | ipv4-icmp | ipv4-tcp | ipv4-udp | ipv6|ipv6-icmp | ipv6-tcp | ipv6-udp} ] [ingress {any | interface <PORT_TYPE> }] [logging] [next { <AceId : 1-256>|last}] [policy <PolicyId : 0-255>] [rate-limiter {<RateLimiterId : 1-16>|disable}] [redirect {disable | interface <PORT_TYPE>}] [shutdown] [tag {any|tagged|untagged}] [tag-priority {0-1 | 0-3 | 2-3 | 4-5 | 4-7 | 6-7 | <TagPriority : 0-7> | any}] [vid { <Vid : 1-4095>|any}]

**Explanation:** Update an access control list.

**Parameters:**

<AceId : 1-256>: Specify access control list ID that applies to this rule.

[ action {deny | filter | permit}]: Specify the action that applies to this rule.

[ dmac-type {any| broadcast | multicast | unicast } ]: Specify destination MAC type that applies to this rule.

[frame-type {any | arp|etype | ipv4|ipv4-icmp | ipv4-tcp | ipv4-udp | ipv6|ipv6-icmp | ipv6-tcp | ipv6-udp} ]: Specify the frame type that applies to this rule.

[ingress {any | interface <PORT_TYPE> }]: Specify the ingress port.

[logging]: Enable logging function.

[mirror]: Enable the function of mirroring frames to destination mirror port.

[next{<AceId : 1-256>|last}]: Insert the current ACE ID before the next ACE ID or put the ACE ID to the last one.

[policy <PolicyId : 0-255>]: Specify the policy ID.

[rate-limiter {<RateLimiterId : 1-16>|disable}]: Specify the rate limit ID or disable this function.

[redirect {disable | interface <PORT_TYPE>}]: Redirect frames to a specific port or disable this function.

[shutdown]: Enable shutdown function.

[tag {any|tagged|untagged}]: Specify whether frames should be tagged or untagged.

[tag-priority {0-1 | 0-3 | 2-3 | 4-5 | 4-7 | 6-7 | <TagPriority : 0-7> | any}]: Specify the priority value.

[vid { <Vid : 1-4095>|any}]: Specify the VLAN ID.

**Show:** # show access-list [ interface [ ( <port_type> [ <v_port_type_list> ] ) ] ] [ rate-limiter [ <rate_limiter_list> ] ] [ ace statistics [ <ace_list> ] ]

**Negation:** (config)# no access-list ace <ace_list>

### *1.9.3.3 (config)# access-list rate-limiter*

**Syntax:** (config)# access-list rate-limiter [ <rate_limiter_list> ] { pps <pps_rate> | 100pps <pps100_rate> | kpps <kpps_rate> | 100kbps <kpbs100_rate> }

**Explanation:** Configure rate limiter that applies to each rate limit ID.

**Parameters:**

[ <rate_limiter_list> ]: Specify the “rate limit ID”, “100kbps” or “pps” . The allowed rate limit ID range is from1~16.

{ pps <pps_rate> | 100pps <pps100_rate> | kpps <kpps_rate> | 100kbps <kpbs100_rate> }: Specify the rate limit rate.

**Show:** # show access-list rate-limiter [<RateLimiterList : 1~16>]

### *1.9.3.4 (config-if)# access-list action*

**Syntax:** (config-if)# access-list action { permit|deny}

**Explanation:** Configure a specific port’s action option.

**Parameters:**

{ permit|deny}: Permit or deny frames on a specific port.

**Show:** # show access-list [ interface [ ( <port_type> [ <v_port_type_list> ] ) ] ]

### *1.9.3.5 (config-if)# access-list logging*

**Syntax:** (config-if)# access-list logging

**Explanation:** Enable a specific port’s logging function.

**Show:** # show access-list [ interface [ ( <port_type> [ <v_port_type_list> ] ) ] ]

**Negation:** (config-if)# no access-list logging

### *1.9.3.6 (config-if)# access-list policy*

**Syntax:** (config-if)# access-list policy <policy_id>

**Parameters:**

<policy_id:0-255>: Specify a policy ID that applies to this specific port.

**Explanation:** Apply a policy ID to a specific port.

**Show:** # show access-list [ interface [ ( <port_type> [ <v_port_type_list> ] ) ] ]

**Negation:** (config-if)# no access-list policy

### *1.9.3.7 (config-if)# access-list port-state*

**Syntax:** (config-if)# access-list port-state

**Explanation:** Enable a specific port's port state.

**Negation:** (config-if)# no access-list port-state

### *1.9.3.8 (config-if)# access-list rate-limiter*

**Syntax:** (config-if)# access-list rate-limiter <rate_limiter_id>

**Parameters:**

<rate_limiter_id:1-16>: Specify a rate limiter ID to a specific port.

**Explanation:** Apply a rate limiter ID to a specific port.

**Negation:** (config-if)# no access-list rate-limiter

### *1.9.3.9 (config-if)# access-list shutdown*

**Syntax:** (config-if)# access-list shutdown

**Explanation:** Shutdown this port when specified rules are matched.

**Negation:** (config-if)# no access-list shutdown

### *1.9.3.10 (config-if)# access-list {redirect| port-copy }*

**Syntax:** (config-if)# access-list { redirect | port-copy } interface { <port_type> <port_type_id> | ( <port_type> [ <port_type_list> ] ) }

**Parameters:**

{ redirect **|** port-copy }: Redirect or copy this port's frames to the specified port.

interface{<port_type><port_type_id>**|**(<port_type>[<port_type_list>])}: Specify the redirect or copy port type and port list.

**Explanation:** Redirect or copy this port's frames to the specified port.

**Negation:** (config-if)# no access-list { redirect **|** port-copy }

## *1.9.4 (config)# aggregation*

### *1.9.4.1 (config)# aggregation mode*

**Syntax:** (config)# aggregation mode { [ smac ] [ dmac ] [ ip ] [ port ] }

**Explanation:** Configure aggregation mode.

**Parameters:**

[smac]: All traffic from the same Source MAC address is output on the same link in a trunk.

[dmac]: All traffic with the same Destination MAC address is output on the same link in a trunk.

[ip]: All traffic with the same source and destination IP address is output on the same link in a trunk.

[port]: All traffic with the same source and destination TCP/UDP port number is output on the same link in a trunk.

**Negation:** (config)# no aggregation mode

**Show:** # show aggregation [mode]

## *1.9.5 (config)# banner*

### *1.9.5.1 (config)# banner [ motd ] <banner>*

**Syntax:** (config)# banner [ motd ] <banner>

**Parameters:**

[ motd ]: Type in the message of the day.

**Explanation:** Configure the message of the day.

**Negation:** (config)# no banner [motd]

### *1.9.5.2 (config)# banner exec <banner>*

**Syntax:** (config)# banner exec <banner>

**Explanation:** Display the configured message when successfully entering Exec mode.

**Negation:** (config)# no banner exec

### *1.9.5.3 (config)# banner login <banner>*

**Syntax:** (config)# banner login <banner>

**Explanation:** Display the configured message when prompted for login ID and password.

**Negation:** (config)# no banner login

## *1.9.6 (config)# clock*

### *1.9.6.1 (config)# clock summer-time <word16> date*

**Syntax:** clock summer-time <word16> date [ <start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [ <offset_var> ] ]

**Explanation:** Configure daylight saving time. This is used to set the clock forward or backward according to the configurations set for a defined Daylight Saving Time duration. "Recurring" command is used to repeat the configuration every year.

**Parameters:**

summer-time <word16>: Specify a description for this day-light setting.

date [ <start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [ <offset_var> ] ]

<start_month_var:1-12>: Specify the starting month.

<start_date_var: 1-31>: Specify the starting day.

<start_year_var:2000-2097>: Specify the starting year.

<start_hour_var: hh:mm>: Specify the time to start.

<end_month_var:1-12>: Specify the ending month.

<end_date_var: 1-31>: Specify the ending day.

<end_year_var:2000-2097>: Specify the ending year.

<end_hour_var: hh:mm>: Specify the time to start.

[ <offset_var: 1-1440> ]: Specify the number of minutes to add during Daylight Saving Time. The allowed range is 1 to 1440.

**Negation:** (config)# no clock summer-time

**Show:** > show clock
> show clock detail
# show clock
# show clock detail

### *1.9.6.2 (config)# clock summer-time <word16> recurring*

**Syntax:** (config)# clock summer-time <word16> recurring [ <start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [ <offset_var> ] ]

**Explanation:** Configure daylight saving time. This is used to set the clock forward or backward according to the configurations set for a defined Daylight Saving Time duration. "Recurring" command is used to repeat the configuration every year.

**Parameters:**

summer-time <word16>: Specify a description for this day-light setting.

recurring [ <start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [ <offset_var> ] ]

<start_week_var:1-5>: Specify the starting week.

<start_day_var: 1-31>: Specify the starting day.

<start_month_var:1-12>: Specify the starting month.

<start_hour_var: hh:mm>: Specify the time to start.

<end_week_var:1-5>: Specify the ending week.

<end_day_var: 1-31>: Specify the ending day.

<end_month_var: 1-12>: Specify the ending month.

<end_hour_var: hh:mm>: Specify the time to end.

[ <offset_var: 1-1440> ]: Specify the number of minutes to add during Daylight Saving Time. The allowed range is 1 to 1440.

**Negation:** (config)# no clock summer-time

**Show:** # show clock
# show clock detail

#### *1.9.6.3 (config)# clock timezone*

**Syntax:** (config)# clock timezone <word> <-23-23> [<0-59>]

**Explanation:** Configure a timezone used in the switch.

**Parameters:**

<word16>: Specify the name of the timezone.

<-23-23>: Hours offset from UTC.

[<0-59>]: Minutes offset from UTC.

**Negation:** (config)# no clock timezone

**Show:** # show clock
# show clock detail

### *1.9.7 (config)# defaultaccess-list rate-limiter*

**Syntax:** (config)# default access-list rate-limiter [ <rate_limiter_list> ]

**Explanation:** To default the specified rate-limiter ID.

**Parameters:**

[ <rate_limiter_list: 1-16> ]: Specify a rate limiter ID.

**Example:** To default rate-limiter 1.

```
# config t
(config)# default access-list rate-limiter 1
```

### *1.9.8 (config)# dot1x*

#### *1.9.8.1 (config)# dot1x system-auth-control*

**Syntax:** (config)# dot1x system-auth-control

**Explanation:** To enable 802.1x service.

**Parameters:** None.

**Example:** Enable 802.1x service.

```
# config t
(config)# dot1x system-auth-control
```

**Negation:** (config)# no dot1x system-auth-control

**Show:** >show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]
#show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]

### *1.9.8.2 (config)# dot1x re-authentication*

**Syntax:** (config)# dot1x re-authentication

**Explanation:** Set clients to be re-authenticated after an interval set in "Re-authenticate" field. Re-autentication can be used to detect if a new device is attached to a switch port.

**Example:** Enable re-authentication function.

```
# config t
(config)# dot1x re-authentication
```

**Negation:** (config)# no dot1x re-authentication

**Show:** >show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]
#show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]

### *1.9.8.3 (config)# dot1x authentication timer re-authenticate*

**Syntax:** (config)# dot1x authentication timer re-authenticate <1-3600>

**Explanation:** Specify the time interval for a connected device to be re-authenticated. By default, the re-authenticated period is set to 3600 seconds. The allowed range is 1 - 3600 seconds.

**Parameters:**

<1-3600>: Specify a re-authentication value between 1 and 3600.

**Example:** Set re-authentication timer to 100.

```
# config t
(config)# dot1x authentication timer re-authenticate 100
```

**Negation:** (config)# no dot1x authentication timer re-authenticate

### *1.9.8.4 (config)# dot1x timeout tx-period*

**Syntax:** (config)# dot1x timeout tx-period <v_1_to_65535>

**Explanation:** Specify the time that the switch waits for a supplicant response during an authentication session before transmitting a Request Identify EAPOL packet. By default, it is set to 30 seconds.

**Parameters:**

<v_1_to_65535>: Specify a timeout value between 1 and 65535 (seconds).

**Example:** Set EAPOL timeout to 30 seconds.

```
# config t
(config)# dot1x timeout tx-period 30
```

**Negation:** (config)# no dot1x timeout tx-period

### *1.9.8.5 (config)#dot1x authentication timer inactivity*

**Syntax:** (config)# dot1x authentication timer inactivity <10-1000000>

**Explanation:** Specify the period that is used to age out a client's allowed access to the switch via 802.1X and MAC-based authentication. The default period is 300 seconds. The allowed range is 10 - 1000000 seconds.

**Parameters:**

<10-1000000>: Specify a value between 10 and 1000000 (seconds).

**Example:** Set the aging time to 300 seconds.

```
# config t
(config)# dot1x authentication timer inactivity 300
```

**Negation:** (config)# no dot1x authentication timer inactivity

### *1.9.8.6 (config)# dot1xtimeout quiet-period*

**Syntax:** (config)# dot1x timeout quiet-period <v_10_to_1000000>

**Explanation:** The time after an EAP Failure indication or RADIUS timeout that a client is not allowed access. This setting applies to ports running Single 802.1X, Multi 802.1X, or MAC-based authentication. By default, hold time is set to 10 seconds. The allowed range is 10 - 1000000 seconds.

**Parameters:**

<10-1000000>: Specify a value between 10 and 1000000 (seconds).

**Example:** Set hold time to 30 seconds.

```
# config t
(config)# dot1x timeout quiet-period 30
```

**Negation:** (config)# no dot1x timeout quiet-period

### *1.9.8.7 (config)# dot1x feature*

**Syntax:** (config)# dot1x feature { [ guest-vlan ] [ radius-qos ] [ radius-vlan ] }

**Explanation:** Enable the specified feature.

**Parameters:**

{ [ guest-vlan ] [ radius-qos ] [ radius-vlan ] }:

[guest-vlan]: Enable guest VLAN. A Guest VLAN is a special VLAN typically with limited network access. 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.

[radius-qos]: Enable RADIUS assigned QoS.

[radius-vlan]: Enable RADIUS VLAN. 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.

**Example:** Enable guest VLAN service.

```
# config t
(config)# dot1x feature guest-vlan
```

**Negation:** (config)# no dot1x feature { [ guest-vlan ] [ radius-qos ] [ radius-vlan ] }

### *1.9.8.8 (config)# dot1x guest-vlan*

**Syntax:** (config)# dot1x guest-vlan <value>

**Explanation:** Configure a guest VLAN ID.

**Parameters:**

<value:1-4095>: Specify the guest VLAN ID. The allowed VLAN ID range is from 1 to 4095.

**Negation:** (config)# no dot1x guest-vlan

### *1.9.8.9 (config)# dot1x guest-vlan supplicant*

**Syntax:** (config)# dot1x guest-vlan supplicant

**Explanation:** Enable Guest VLAN supplicant function. 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. When enabled, the switch does not maintain the EAPOL packet history and allows clients that fail authentication to access the guest VLAN, regardless of whether EAPOL packets had been detected on the interface. Clients that fail authentication can access the guest VLAN.

**Negation:** (config)# no dot1x guest-vlan supplicant

### *1.9.8.10 (config)# dot1x max-requth-req*

**Syntax:** (config)# dot1x max-reauth-req <value>

**Explanation:** The maximum number of times the switch transmits an EAPOL Request Identity frame without receiving a response before adding a port to the Guest VLAN. The value can only be changed when the Guest VLAN option is globally enabled. The range is 1 – 255.

**Parameters:**

<value:1-255>: Specify a value between 1 and 255.

**Negation:** (config)# no dot1x max-reauth-req

### *1.9.8.11 (config-if)# dot1x port-control*

**Syntax:** (config-if)# dot1x port-control { force-authorized **|** force-unauthorized **|** auto **|** single **|** multi **|** mac-based }

**Parameters:**

{ force-authorized | force-unauthorized | auto | single | multi | mac-based }: Specify one of the authentication modes on the selected interfaces. This setting works only when NAS is globally enabled. The following modes are available:

**force-authorized:** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

**force unauthorized:** In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

**auto (Port-Based 802.1X):** This mode requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.

**single (802.1X):** In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the “Port Security” module is used to secure a supplicant's MAC address once successfully authenticated.

**multi (802.1X):** In 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.

**mac-based:** Unlike port-based 802.1X, MAC-based authentication do not transmit or receive EAPOL frames. In MAC-based authentication, 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.

**Example:** Set Gigabit Ethernt port 1-10's admin state to "auto"

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x port-control auto
```

**Negation:** (config-if)# no dot1x port-control

### *1.9.8.12 (config-if)# dot1x guest-vlan*

**Syntax:** (config-if)# dot1x guest-vlan

**Explanation:** Enable the guest VLAN on the selected interfaces.

**Parameters:** None.

**Example:** Enable guest VLAN on port 1-10.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x guest-vlan
```

**Negation:** (config-if)# no dot1x guest-vlan

### *1.9.8.13 (config-if)# dot1x radius-qos*

**Syntax:** (config-if)# dot1x radius-qos

**Explanation:** Enable RADIUS Assigned QoS on the selected interfaces.

**Parameters:** None.

**Example:** Enable RADIUS Assigned QoS on port 1-10.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x radius-qos
```

**Negation:** (config-if)# no dot1x radius-qos

#### *1.9.8.14 (config-if)# dot1x radius-vlan*

**Syntax:** (config-if)# dot1x radius-vlan

**Explanation:** Enable RADIUS Assigned VLAN on the selected interfaces.

**Parameters:** None.

**Example:** Enable RADIUS Assigned VLAN on port 1-10.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x radius-vlan
```

**Negation:** (config-if)# no dot1x radius-vlan

#### *1.9.8.15 (config-if)# dot1x re-authenticate*

**Syntax:** (config-if)# dot1x re-authenticate

**Explanation:** Schedules reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. This command only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

**Show:** > show dot1x statistics { eapol | radius | all } [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show dot1x statistics { eapol | radius | all } [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### *1.9.9 (config-if)# duplex*

**Syntax:** (config-if)# duplex { half **|** full **|** auto [ half **|** full ] }

**Explanation:** Configure port's duplex mode.

**Parameters:**

{ half **|** full **|** auto [ half **|** full ] }: Specify the duplex mode for this specific interface.

**Example:** Set port 1's duplex mode to auto.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# duplex auto
```

**Negation:** (config-if)# no duplex

**Show:** > show interface ( <port_type> [ <v_port_type_list> ] ) status
# show interface ( <port_type> [ <v_port_type_list> ] ) status

## *1.9.10 (config)# enable*

### *1.9.10.1 (config)# enable password*

**Syntax:** (config)# enable password <password>

**Explanation:** Configure enable password.

**Parameters:**

password <password>: Specify the enable mode password.

### *1.9.10.2 (config)# enable password level*

**Syntax:** (config)# enable password [level <priv: 1-15>] <password>

**Explanation:** Configure enable password and privilege level.

**Parameters:**

[level <priv: 1-15>]: Specify the privilege level for this password.

<password>: Specify the enable mode password.

**Negation:** (config)# no enable password [ level <priv> ]

### *1.9.10.3 (config)# enable secret*

**Syntax:** (config)# enable secret { 0 **|** 5 } [ level <priv: 1-15> ] <password>

**Parameters:**

{0**|**5}: Specify "0" to denote unencrypted secret (cleartext). Specify "5" to denote encrypted secret (MD5).

[level <priv: 1-15>]: Specify the privilege level for this password.

<password>: Specify the enable mode password.

**Explanation:** Configure enable secret password and privilege level.

**Negation:** (config)# no enable secret { [ 0 **|** 5 ] } [ level <priv> ]

## *1.9.11 (config-if)# excessive-restart*

**Syntax:** (config-if)# excessive-restart

**Explanation:** Restart backoff algorithm after 16 collisions (No excessive-restart means discard frames after 16 collisions.)

**Negation:** (config-if)# no excessive-restart

**Show:** > show interface ( <port_type> [ <v_port_type_list> ] ) status
# show interface ( <port_type> [ <v_port_type_list> ] ) status

### *1.9.12 (config-if)# flowcontrol { on | off }*

**Syntax:** (config-if)# flowcontrol { on | off }

**Explanation:** Enable or disable flow confrol for this specific interface.

**Parameters:**

{ on | off }: Enable or disable flow control.

**Negation:** (config-if)# no flowcontrol

**Show: >** show interface ( <port_type> [ <v_port_type_list> ] ) status
# show interface ( <port_type> [ <v_port_type_list> ] ) status

### *1.9.13 (config)# hostname*

**Syntax:** (config)# hostname <WORD>

**Explanation:** Specify a descriptive name for this switch.

**Parameters:**

<WORD32>: Specify a descriptive name for this device. Indicate the hostname for this device. Alphabets (A-Z; a-z), digits (0-9) and minus sign (-) can be used. However, space characters are not allowed. The first character must be an alphabet character. The first and last character must not be a minus sign. The allowed string length is 0 – 255.

**Example:** Set the hostname to AccessSW.

```
# config t
(config)# hostname AccessSW
AccessSW(Config)#
```

**Negation:** (config)# no hostname

**Show:** > show version
# show version

### *1.9.14 (config)# interface*

#### *1.9.14.1(config)# interface ( <port_type> [ <plist> ] )*

**Syntax:** (config)# interface ( <port_type> [ <plist> ] )

**Explanation:** Enter Config Interface mode for this specific interface.

**Parameters:**

<port_type> [ <plist> ]: Specify the port type and port number.

**Example:** Enter Config Interface mode for Gigabit Ethernet port 1.

```
# config t
(config)#
(config)# interface GigabitEthernet 1/1
(config-if)#
```

**Show:** > show interface ( <port_type> [ <in_port_list> ] ) switchport [ access | trunk | hybrid ]
> show interface ( <port_type> [ <v_port_type_list> ] ) capabilities
> show interface ( <port_type> [ <v_port_type_list> ] ) statistics [ { packets | bytes | errors | discards | filtered | { priority [ <priority_v_0_to_7> ] } } ] [ { up | down } ]
> show interface ( <port_type> [ <v_port_type_list> ] ) status
> show interface ( <port_type> [ <v_port_type_list> ] ) veriphy
> show interface vlan [ <vlist> ]

# show interface ( <port_type> [ <in_port_list> ] ) switchport [ access | trunk | hybrid ]
# show interface ( <port_type> [ <v_port_type_list> ] ) capabilities

# show interface ( <port_type> [ <v_port_type_list> ] ) statistics [ { packets | bytes | errors | discards | filtered | { priority [ <priority_v_0_to_7> ] } } ] [ { up | down } ]
# show interface ( <port_type> [ <v_port_type_list> ] ) status #
show interface ( <port_type> [ <v_port_type_list> ] ) veriphy #
show interface vlan [ <vlist> ]

**Clear:** # clear statist9000 { [ interface ] ( <port_type> [ <v_port_type_list> ] ) }

#### *1.9.14.2 (config)# interface vlan*

**Syntax:** (config)# interface vlan <vlist>

**Explanation:** Enter Config Interface VLAN mode for this specific interface.

**Example:** Enter Config Interface VLAN 1 for port 1.

```
# config t
(config)#
(config)# interface vlan 1
(config-if-vlan)#
```

### *1.9.15 (config)# ip*

#### *1.9.15.1 (config)# ip dhcp excluded-address*

**Syntax:** (config)# ip dhcp excluded-address <low_ip> [ <high_ip> ]

**Parameters:**

<low_ip> [ <high_ip> ]: Specify the IP address range that will not be used for DHCP IP assignment.

**Explanation:** Configure IP addresses that are not used for DHCP IP allocation.

**Example:** Exclude IP address 1.2.3.4 to 1.2.3.10 from DHCP IP allocation pool..

```
# config t
(config)# ip dhcp excluded-address 1.2.3.4 1.2.3.10
(config)# exit
# show ip dhcp excluded-address
     Low Address          High Address
     ---------------      ---------------
01   1.2.3.4              1.2.3.10

#
```

**Negation:** (config)# no ip dhcp excluded-address <low_ip> [ <high_ip> ]

**Show:** # show ip dhcp excluded-address

#### *1.9.15.2 (config)# ip dhcp pool*

**Syntax:** (config)# ip dhcp pool <pool_name>

**Parameters:**

<pool_name>: Specify the DHCP pool name in 32 characters.

**Explanation:** Configure the pool name for DHCP IP addresses.

**Negation:** (config)# no ip dhcp pool <pool_name>

**Show:** # show ip dhcp pool

#### *1.9.15.3 (config)# ip dhcp relay*

**Syntax:** (config)# ip dhcp relay

**Explanation:** Enable DHCP relay function.

**Example:** Enable DHCP relay function.

```
# config t
(config)# ip dhcp relay
```

**Negation:** (config)# no ip dhcp relay

**Show:** > show ip dhcp relay [statistics]
# show ip dhcp relay [statistics]

**Clear:** # clear ip dhcp relay statistics

#### *1.9.15.4 (config)# ip dhcp relay information circuit-id format*

**Syntax:** (config)# ip dhcp relay information circuit-id format { standard **|** tr101 **|** alias }

**Parameters:**

{ standard **|** tr101 **|** alias }: Specify the DHCP relay circuit ID format.

standard: Used for defining the switch port and VLAN ID according to RFC 3046.

tr-101: Used for defining the switch IP, switch port and VLAN ID according to TR-101.

alias: Use the individual values for port Alias.

**Explanation:** Specify the appropriate circuit ID format.

**Negation:** (config)# no ip dhcp relay information circuit-id format

#### *1.9.15.5 (config)# ip dhcp relay information option*

**Syntax:** (config)# ip dhcp relay information option

**Explanation:** Enable DHCP Relay option 82 function. Please note that "Relay Mode" must be enabled before this function is able to take effect.

**Example:** Enable DHCP Relay option 82 function

```
# config t
(config)# ip dhcp relay information option
```

**Negation:** (config)# no ip dhcp relay information option

#### *1.9.15.6 (config)# ip dhcp relay information policy {drop | keep |replace}*

**Syntax:** (config)# ip dhcp relay information policy {drop | keep | replace}

**Explanation:** Specify DHCP Relay information reforwarding policy action.

**Parameters:**

{ drop **|** keep **|** replace }: Specify one of the relay information policy options.

**drop:** Drop the packet when it receives a DHCP message that already contains relay information.

**keep:** Keep the client's DHCP information.

**replace:** Replace (rewrite) the DHCP client packet information with the switch's relay information. This is the

default setting.

**Example:** Keep the client's DHCP information.

```
# config t
(config)# ip dhcp relay information policy keep
```

**Negation:** (config)# no ip dhcp relay information policy

### *1.9.15.7 (config)# ip dhcp relay information remote-id*

**Syntax:** (config)# ip dhcp relay information remote-id <v_line63>

**Parameters:**

<v_line63>: Specify remote ID string.

**Explanation:** Specify the remoted ID inserted in DHCP Relay information option.

**Negation:** (config)# no ip dhcp relay information remote-id

**Show:** # show ip dhcp relay

### *1.9.15.8 (config)# ip dhcp relay information remote-id format*

**Syntax:** (config)# ip dhcp relay information remote-id format { none **|** mac **|** configured }

**Parameters:**

{ none | mac | configured }: Specify remote ID format.

none: Sub-option 2 is not used.

mac: Add MAC address to Option 82 information.

configured: Use the desire remote ID format.

**Explanation:** Specify the remoted ID format inserted in DHCP Relay information option.

**Negation:** (config)# no ip dhcp relay information remote-id format

**Show:** # show ip dhcp relay

### *1.9.15.9 (config)# ip dhcp server*

**Syntax:** (config)# ip dhcp server

**Explanation:** Enable DHCP server function globally.

**Example:** Enable DHCP server function.

```
# config t
(config)# ip dhcp server
```

**Negation:** (config)# no ip dhcp server

**Show:** > show ip dhcp server
# show ip dhcp server

### *1.9.15.10 (config-if)# dhcp ip-port-binding*

**Syntax:** (config)# interface gigabitethernet 1/1
(config-if)# dhcp ip-port-binding

**Explanation:** Setting DHCP IP Port binding function , let DHCP Server by port Assign specified IP Address . .

**Example:** Setting interface GI 1/1 Binding IP Address = 192.168.10.101

```
# config t
(config)# interface GigabitEthernet 1/1
(Config-if)# dhcp ip-port-binding 192.168.10.101
```

**Negation:** (config-if)# no ip-port–Binding 192.168.10.101

**Show:** # show ip dhcp server binding

### *1.9.15.11 (config)# ip helper-address*

**Syntax:** (config)# ip helper-address <v_ipv4_ucast>

**Explanation:** Configure DHCP Relay server IPv4 address.

**Parameters:**

<v_ipv4_ucast>: Specify DHCP Relay server IPv4 address that is used by the switch's DHCP relay agent

**Negation:** (config)# no ip helper-address

### *1.9.15.12 (config)# ip http secure-server*

**Syntax:** (config)# ip http secure-server

**Explanation:** Enable the HTTPS operation mode. When the current connection is HTTPS and HTTPS mode operation is disabled, web browser will automatically redirect to an HTTP connection.

**Example:** Enable the HTTPS operation mode.

```
# config t
(config)# ip http secure-server
```

**Negation:** (config)# no ip http secure-server

**Show:** # show ip http server secure status

### *1.9.15.13 (config)# ip http secure-redirect*

**Syntax:** (config)# ip http secure-redirect

**Explanation:** Enable the HTTPS redirect mode operation. It applies only if HTTPS mode is "Enabled". Automatically redirects HTTP of web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled.

**Example:** Enable HTTPs automatic redirect mode.

```
# config t
(config)# ip http secure-redirect
```

**Negation:** (config)# no ip http secure-redirect

**Show:** # show ip http server secure status

### *1.9.15.14 (config)# ip igmp host-proxy*

**Syntax:** (config)# ip igmp host-proxy [ leave-proxy ]

**Explanation:** When enabled, the switch suppresses leave messages unless received from the last member port in the group. IGMP leave proxy suppresses all unnecessary IGMP leave messages so that a non-querier switch forwards an IGMP leave packet only when the last dynamic member port leaves a multicast group.

**Parameters:**

[leave-proxy]: The parameter is optional. Enable leave-proxy function.

**Negation:** (config)# no ip igmp host-proxy [leave-proxy]

**Show:** # show ip igmp snooping detail

### *1.9.15.15 (config)# ip igmp snooping*

**Syntax:** (config)# ip igmp snooping

**Explanation:** Globally enable IGMP Snooping feature. When enabled, this device will monitor network traffic and determine which hosts will receive multicast traffic. The switch can passively monitor or snoop on IGMP Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

**Negation:** (config)# no ip igmp snooping

**Show:** # show ip igmp snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

**Clear:** # clear ip igmp snooping [ vlan <v_vlan_list> ] statistics

### *1.9.15.16 (config)# ip igmp snooping vlan*

**Syntax:** (config)# ip igmp snooping vlan <v_vlan_list>

**Explanation:** Enable IGMP function for specific VLANs**.**

**Parameters:**

<v_vlan_list>: Specify valid IGMP VLANs.

**Negation:** (config)# no ip igmp snooping vlan [ <v_vlan_list> ]

**Show:** # show ip igmp snooping

**Clear:** # clear ip igmp snooping [ vlan <v_vlan_list> ] statistics

### *1.9.15.17 (config)# ip igmp ssm-range*

**Syntax:** (config)# ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>

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

**Parameters:**

<v_ipv4_mcast>: Specify valid IPv4 multicast address.

<ipv4_prefix_length>: Specify the prefix length ranging from 4 to 32.

**Negation:** (config)# no ip igmp ssm-range

#### *1.9.15.18 (config)# ip igmp unknown-flooding*

**Syntax:** (config)# ip igmp unknown-flooding

**Explanation:** Set forwarding mode for unregistered (not-joined) IP multicast traffic. Select the checkbox to flood traffic.

**Negation:** (config)# no ip igmp unknown-flooding

#### *1.9.15.19 (config)# ip route*

**Syntax:** (config)# ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>

**Explanation:** Configure a static IP route.

**Parameters:**

<v_ipv4_addr>: Specify IPv4 address. The IP route is the destination IP network or host address of this route. Valid format is dotted decimal notation.

<v_ipv4_netmask>: The route mask is a 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. Only a default route will have a mask length of 0 (as it will match anything).

<v_ipv4_gw>: This is the IP address of the gateway. Valid format is dotted decimal notation. Gateway and Network must be of the same type.

**Example:** Add a new ip route with the following settings.

```
# config t
(config)# ip route 192.168.1.240 255.255.255.0 192.168.1.254
```

**Negation:** (config)# no ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>

**Show:** > show ip route
# show ip route

### *1.9.15.20 (config)# ip ssh*

**Syntax:** (config)# ip ssh

**Explanation:** Enable SSH mode.

**Example:** Enable SSH mode.

```
# config t
(config)# ip ssh
```

**Negation:** (config)# no ip ssh

**Show:** # show ip ssh

***NOTE:*** *SSH is preferred to Telnet, unless the management network is trusted. Telnet passes authentication credentials in plain text, making those credentials susceptible to packet capture and analysis. SSH provides a secure authentication method. The SSH in this device uses version 2 of SSH protocol.*

### *1.9.15.21 (config)# ip verify source*

**Syntax:** (config)# ip verify source

**Explanation:** Enable IP source guard function.

**Negation:** (config)# no ip verify source

**Show:** > show ip verify source [interface (<port_type> [<in_port_type_list>])]
# show ip verify source [interface (<port_type> [<in_port_type_list>])]

### *1.9.15.22 (config-if)# ip dhcp relay information subscriber-id*

**Syntax:** (config-if)# ip dhcp relay information subscriber-id <v_line63>

**Explanation:** Use this command to configure DHCP Option 82 subscriber ID on a per port basis.

**Parameters:**

<v_line63>: Specify DHCP Option 82 suboption 6 (subscriber ID).

**Show:** > show ip dhcp relay [ statistics ]
# show ip dhcp relay [ statistics ]

### *1.9.15.23 (config-if-vlan)# ip address*

**Syntax:** (config-if-vlan)# ip address { { <address> <netmask> } **|** { dhcp [ fallback <fallback_address> <fallback_netmask> [ timeout <fallback_timeout> ] ] } }

**Explanation:** Configure IPv4 address for this VLAN interface.

**Parameters:**

<address> <netmask>: Specify IPv4 address and subnet mask.

dhcp [ fallback <fallback_address> <fallback_netmask> [ timeout <fallback_timeout> ] ]: Use DHCP server to automatically assign IP address.

**fallback <fallback_address> <fallback_netmask>:** specify Fallback IP address and subnet mask.

**timeout <fallback_timeout>:** Specify Fallback timeout value.

**Negation:** (config-if-vlan)# no ip address

**Show:** > show ip interface brief
# show ip interface brief

### *1.9.15.24 (config-if-vlan)# ip dhcp server*

**Syntax:** (config-if-vlan)# ip dhcp server

**Explanation:** Eanble DHCP server on this specific VLAN.

**Negation:** (config-if-vlan)# no ip dhcp server

**Show:** > show ip dhcp server
# show ip dhcp server

### *1.9.15.25 (config-if-vlan)# ip igmp snooping*

**Syntax:** (config-if-vlan)# ip igmp snooping

**Explanation:** Eanble IGMP Snooping on this specific VLAN.

**Negation:** (config-if-vlan)# no ip igmp snooping

**Show:** > show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
# show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]

### *1.9.15.26 (config-if-vlan)# ip igmp snooping compatibility*

**Syntax:** (config-if-vlan)# ip igmp snooping compatibility {auto | v1 | v2 | v3}

**Explanation:** Configure IGMP Snooping version used for this specific VLAN.

**Parameters:**

{auto | v1 | v2 | v3}: Specify one of the IGMP Snooping options.

**auto:** Compatible with Version 1, Version 2, and Version 3.

**v1:** Compatible with IGMP version 1.

**v2:** Compatible with IGMP version 2.

**v3:** Compatible with IGMP version 3.

**Negation:** (config-if-vlan)# no ip igmp snooping compatibility

### *1.9.15.27 (config-if-vlan)# ip igmp snooping last-member-query-interval*

**Syntax:** (config-if-vlan)# ip igmp snooping last-member-query-interval <ipmc_lmqi>

**Explanation:** LMQI stands for Last Member Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The allowed range is 0~31744 tenths of a second.

**Parameters:**

<ipmc_lmqi: 0-31744>: Specify LMQI (Last Member Query Interval) value.

**Negation:** (config-if-vlan)# no ip igmp snooping last-member-query-interval

### *1.9.15.28 (config-if-vlan)# ip igmp snooping priority*

**Syntax:** (config-if-vlan)# ip igmp snooping priority <cos_priority>

**Explanation:** Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0 -7.

**Parameters:**

<cos_priority: 0-7>: Specify COS for this specific VLAN. The valid range is 0 to 7.

**Negation:** (config-if-vlan)# no ip igmp snooping priority

### *1.9.15.29 (config-if-vlan)# ip igmp snooping querier*

**Syntax:** (config-if-vlan)# ip igmp snooping querier { election **|** address <v_ipv4_ucast> }

**Parameters:**

{ election | address <v_ipv4_ucast> }: Elect the IGMP Snooping querier or use the specified IPv4 unicast address as a querier.

**Explanation:** Elect or specify IGMP Snooping querier IP address.

**Negation:** (config-if-vlan)# no ip igmp snooping querier { election **|** address }

### *1.9.15.30 (config-if-vlan)# ip igmp snooping query-interval*

**Syntax:** (config-if-vlan)# ip igmp snooping query-interval <ipmc_qi>

**Explanation:** Specify IPMC Query interval value.

**Parameters:**

<ipmc_qi: 1-31744>: Specify IPMC Query interval value. The valid value is 1~31744.

**Negation:** (config-if-vlan)# no ip igmp snooping query-interval

### *1.9.15.31 (config-if-vlan)# ip igmp snooping query-max-response-time*

**Syntax:** (config-if-vlan)# ip igmp snooping query-max-response-time <ipmc_qri>

**Explanation:** Specify IPMC Query Response time value.

**Parameters:**

<ipmc_qri>: Specify IPMC Query Response time value. The valid value is 1~31744.

**Negation:** (config-if-vlan)# no ip igmp snooping query-max-response-time

### *1.9.15.32 (config-if-vlan)# ip igmp snooping robustness-variable*

**Syntax:** (config-if-vlan)# ip igmp snooping robustness-variable <ipmc_rv>

**Explanation:** The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

**Parameters:**

<ipmc_rv: 1-255>: Specify IPMC Robustness Variable value. The valid value is 1~255.

**Negation:** (config-if-vlan)# no ip igmp snooping robustness-variable

### *1.9.15.33 (config-if-vlan)# ip igmp snooping unsolicited-report-interval*

**Syntax:** (config-if-vlan)# ip igmp snooping unsolicited-report-interval <ipmc_uri>

**Explanation:** The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. The allowed range for URI is 0 -31744 seconds.

**Parameters:**

<ipmc_uri: 0-31744>: Specify Unsolicited Report Interval value. The valid value is 0~31744.

**Negation:** (config-if-vlan)# no ip igmp snooping unsolicited-report-interval

### *1.9.15.34 (config-if-vlan)# ipv6 address*

**Syntax:** (config-if-vlan)# ipv6 address <subnet>

**Explanation:** Configure IPv6 address for this VLAN interface.

**Parameters:**

<subnet>: Specify IPv6 address in X:X:X:X::X/<0-128> format.

**Negation:** (config-if-vlan)# no ipv6 address [ <ipv6_subnet> ]

**Show:** > show ip interface brief
> show ipv6 interface [vlan <v_vlan_list> { brief | statistics }]
# show ip interface brief
# show ipv6 interface [ vlan <v_vlan_list> { brief | statistics } ]

### *1.9.15.35 (config-if-vlan)# ipv6 mld snooping*

**Syntax:** (config-if-vlan)# ipv6 mld snooping

**Explanation:** Eanble MLD (Multicast Listener Discovery) Snooping on this specific VLAN.

**Negation:** (config-if-vlan)# no ipv6 mld snooping

**Show:** > show ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]
# show ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

### *1.9.15.36 (config-if-vlan)# ipv6 mld snooping compatibility*

**Syntax:** (config-if-vlan)# ipv6 mld snooping compatibility { auto | v1 | v2 }

**Explanation:** Configure MLD Snooping version used for this specific VLAN.

**Parameters:**

{ auto **|** v1 **|** v2 **|** v3 }: Specify one of the MLD Snooping options.

**auto:** Compatible with Version 1, Version 2.

**v1:** Compatible with MLD version 1.

**v2:** Compatible with MLD version 2.

**Negation:** (config-if-vlan)# no ipv6 mld snooping compatibility

### *1.9.15.37 (config-if-vlan)# ipv6 mld snooping last-member-query-interval*

**Syntax:** (config-if-vlan)# ipv6 mld snooping last-member-query-interval <ipmc_lmqi>

**Explanation:** LMQI stands for Last Member Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The allowed range is 0~31744 tenths of a second.

**Parameters:**

<ipmc_lmqi: 0-31744>: Specify LMQI (Last Member Query Interval) value.

**Negation:** (config-if-vlan)# no ipv6 mld snooping last-member-query-interval

### *1.9.15.38 (config-if-vlan)# ipv6 mld snooping priority <cos_priority>*

**Syntax:** (config-if-vlan)# ipv6 mld snooping priority <cos_priority>

**Explanation:** Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0 -7.

**Parameters:**

<cos_priority: 0-7>: Specify COS for this specific VLAN. The valid range is 0 to 7.

**Negation:** (config-if-vlan)# no ipv6 mld snooping priority

### *1.9.15.39 (config-if-vlan)# ipv6 mld snooping querier election*

**Syntax:** (config-if-vlan)# ipv6 mld snooping querier election

**Explanation:** Enable MLD Snooping querier election function.

**Negation:** (config-if-vlan)# no ipv6 mld snooping querier election

### *1.9.15.40 (config-if-vlan)# ipv6 mld snooping query-interval <ipmc_qi>*

**Syntax:** (config-if-vlan)# ipv6 mld snooping query-interval <ipmc_qi>

**Explanation:** Specify MLD Query interval value.

**Parameters:**

<ipmc_qi: 1-31744>: Specify IPMC Query interval value. The valid value is 1~31744.

**Negation:** (config-if-vlan)# no ipv6 mld snooping query-interval

### *1.9.15.41 (config-if-vlan)# ipv6 mld snooping query-max-response-time <ipmc_qri>*

**Syntax:** (config-if-vlan)# ipv6 mld snooping query-max-response-time <ipmc_qri>

**Explanation:** Specify MLD Query Response time value.

**Parameters:**

<ipmc_qri>: Specify MLD Query Response time value. The valid value is 1~31744.

**Negation:** (config-if-vlan)# no ipv6 mld snooping query-max-response-time

### *1.9.15.42 (config-if-vlan)# ipv6 mld snooping robustness-variable <ipmc_rv>*

**Syntax:** (config-if-vlan)# ipv6 mld snooping robustness-variable <ipmc_rv>

**Explanation:** The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

**Parameters:**

<ipmc_rv: 1-255>: Specify IPMC Robustness Variable value. The valid value is 1~255.

**Negation:** (config-if-vlan)# no ipv6 mld snooping robustness-variable

### *1.9.15.43 (config-if-vlan)# ipv6 mld snooping unsolicited-report-interval <ipmc_uri>*

**Syntax:** (config-if-vlan)# ipv6 mld snooping unsolicited-report-interval <ipmc_uri>

**Explanation:** The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. The allowed range for URI is 0 -31744 seconds.

**Parameters:**

<ipmc_uri: 0-31744>: Specify Unsolicited Report Interval value. The valid value is 0~31744.

**Negation:** (config-if-vlan)# no ipv6 mld snooping unsolicited-report-interval

## 1.9.16 (config)# ipmc

### 1.9.16.1 (config)# ipmc profile

**Syntax:** (config)# ipmc profile

**Explanation:** Enable IPMC (IP multicast) profile globally.

**Negation:** (config)# no ipmc profile

**Show:** # show ipmc profile

### 1.9.16.2 (config)# ipmc profile <profile_name>

**Syntax:** (config)# ipmc profile <profile_name>

**Parameters:**

<profile_name: word16>: Specify the desired profile name in 16 characters. When entered is pressed, the command will change to (config-ipmc-profile)#.

**Explanation:** Set up an IPMC profile.

**Example:** Create an IPMC profile named "goldpass".

```
# config t
(config)# ipmc profile goldpass
(config-ipmc-profile)#
```

**Negation:** (config)# no ipmc profile <profile_name>

**Show:** # show ipmc profile [ <profile_name> ] [ detail ]

### 1.9.16.3 (config)# ipmc range

**Syntax:** (config)# ipmc range <entry_name> {<v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [ <v_ipv6_mcast_1> ]}

**Explanation:** Specify the multicast IP range. The available IP range is from 224.0.0.0~239.255.255.255.

**Parameters:**

<entry_name>: The name used in specifying the address range.

{<v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [<v_ipv6_mcast_1>]}: Specify the multicast IP range. The available IP range is from 224.0.0.0~239.255.255.255.

**Negation:** (config)# no no ipmc range <entry_name>

**Show:** # show ipmc profile [ <profile_name> ] [ detail ]

### *1.9.16.4 (config-ipmc-profile)# default range*

**Syntax:** (config-ipmc-profile)# default range <entry_name>

**Parameters:**

<entry_name: word16>: Specify an entry name in 16 characters for this IPMC profile.

**Explanation:** To set default IPMC Profile Rule for a specific IPMC Profile.

**Example:** To default IPMC Profile Rule (Entry 1) for specific IPMC Profile.

```
# config t
(config)# ipmc profile goldpass
(config-ipmc-profile)# default range 1
```

**Negation:** (config-ipmc-profile)# no range <entry_name>

**Show:** # show ipmc profile
#show ipmc profile [ <profile_name> ] [ detail ]

### *1.9.16.5 (config-ipmc-profile)# description*

**Syntax:** (config-ipmc-profile)# description <profile_desc>

**Parameters:**

<profile_desc: line 64>: Additional description for the designated profile in 64 characters.

**Explanation:** Specify descriptive information for the designated profile.

**Example:** Provide descriptive information for IPMC profile goldpass.

```
# config t
(config)# ipmc profile goldpass
(config-ipmc-profile)# description 1stclasscustomer
```

**Negation:** (config-ipmc-profile)# no description

**Show:** # show ipmc profile
#show ipmc profile [ <profile_name> ] [ detail ]

#### *1.9.16.6 (config-ipmc-profile)# range*

**Syntax:** (config-ipmc-profile)# range <entry_name> { permit **|** deny } [ log ] [ next <next_entry> ]

**Parameters:**

<entry_name>: Specify an entry name.

{ permit **|** deny }: Specify the action taken upon receiving the Join/Report frame that has the group address matches the address range of the rule.

**Permit:** Group address matches the range specified in the rule will be learned.

**Deny:** Group address matches the range specified in the rule will be dropped.

[ log ]: Log when matching

[ next <next_entry> ]: Specify next entry used in profile

**Explanation:** To set action of an entry for a specific IPMC profile.

**Negation:** (config-ipmc-profile)# no range <entry_name>

**Show:** # show ipmc profile
#show ipmc profile [ <profile_name> ] [ detail ]

### *1.9.17 (config)# ipv6 mld host-proxy*

#### *1.9.17.1 (config)# ipv6 mld host-proxy*

**Syntax:** (config)# ipv6 mld host-proxy

**Explanation:** Enable IPv6 MLD proxy. When MLD proxy is enabled, the switch exchanges MLD messages with the router on its upstream interface, and performs the host portion of the MLD task on the upstream interface as follows:

- When queried, it sends multicast listener reports to the group.
- When a host joins a multicast group to which no other host belongs, it sends unsolicited multicast listener reports to that group.
- When the last host in a particular multicast group leaves, it sends an unsolicited multicast listener done report to the all-routers address (FF02::2) for MLDv1.

**Example:** Enable IPv6 MLD Proxy.

```
# config t
(config)# ipv6 mld host-proxy
(config)#
```

**Negation:** (config)# no ipv6 mld host-proxy

**Show:** > show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type>
[ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### *1.9.17.2 (config)# ipv6 mld host-proxy leave-proxy*

**Syntax:** (config)# ipv6 mld host-proxy leave-proxy

**Explanation:** Enable IPv6 MLD leave proxy. To prevent multicast router from becoming overloaded with leave messages, MLD snooping suppresses leave messages unless received from the last member port in the group. When the switch acts as the querier, the leave proxy feature will not function.

**Example:** Enable IPv6 MLD leave proxy.

```
# config t
(config)# ipv6 mld host-proxy leave-proxy
(config)#
```

**Negation:** (config)# no ipv6 mld host-proxy leave-proxy

**Show:** > show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### *1.9.17.3 (config)# ipv6 mld snooping*

**Syntax:** (config)# ipv6 mld snooping

**Explanation:** Enable MLD Snooping feature globally. When enabled, this device will monitor network traffic and determine which hosts would like to receive multicast traffic. The switch can passively monitor or snoop on MLD Listener Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

**Example:** Enable IPv6 MLD snooping.

```
# config t
(config)# ipv6 mld snooping
(config)#
```

**Negation:** (config)# no ipv6 mld snooping

**Show:** > show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### *1.9.17.4 (config)# ipv6 mld snooping vlan*

**Syntax:** (config)# ipv6 mld snooping vlan <v_vlan_list>

**Parameters:**

<v_vlan_list>: Specify VLAN ID for MLD.

**Negation:** (config)# no ipv6 mld snooping vlan [ <v_vlan_list> ]

**Show:** > show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type>
[ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
> show ipv6 mld snooping mrouter [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type>
[ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping mrouter [ detail ]

**Clear:** # clear ipv6 mld snooping [ vlan <v_vlan_list> ] statistics

### *1.9.17.5 (config)# ipv6 mldssm-range*

**Syntax:** (config)# ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>

**Parameters:**

<v_ipv6_mcast>: Specify valid IPv6 mluticast address.

<ipv6_prefix_length>: Specify prefix length range from 8 to 128.

**Explanation:** Specify SSM (Source-Specific Multicast) Range. This setting allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

**Example:** Configure MLD SSM with the ff3e::7728/128 settings.

```
# config t
(config)# ipv6 mld ssm-range ff3e::7728 128
```

**Negation:** (config)# no ipv6 mld ssm-range

**Show:** > show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type>
[ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type>
[ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### *1.9.17.6 (config)# ipv6 mld unknown-flooding*

**Syntax:** (config)# ipv6 mld unknown-flooding

**Explanation:** Enable forwarding mode for unregistered (not-joined) IP multicast traffic.

**Example:** To flood unregistered IPv6 multicast traffic

```
# config t
(config)# ipv6 mld unknown-flooding
```

**Negation:** (config)# no ipv6 mld unknown-flooding

**Show:** > show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
> show ipv6 mld snooping mrouter [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping mrouter [ detail ]

### *1.9.17.7 (config)# ipv6 route*

**Syntax:** (configure)# ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> **|** interface vlan <v_vlan_id> <v_ipv6_addr> }

**Parameters:**

<v_ipv6_subnet>: Specify IPv6 route address.

{ <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }: Specify one of the options. This could be either IPv6 next hop unicast address or an interface.

**Explanation:** Configure a static IPv6 route.

**Negation:** (config)# no ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> **|** interface vlan <v_vlan_id> <v_ipv6_addr> }

**Show:** # show ipv6 route [ interface vlan <v_vlan_list> ]

### *1.9.17.8 (config-if)# ipv6 mld snooping filter*

**Syntax:** (config-if)# ipv6 mld snooping filter <profile_name>

**Explanation:** Use this command to filter specific multicast traffic on a per port basis.

**Parameters:**

<profile_name>: Specify the configured multicast groups that are denied on a port. When a certain multicast group is selected on a port, IGMP join reports received on a port are dropped.

**Negation:** (config-if)# no ipv6 mld snooping filter

**Show:** > show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### *1.9.17.9 (config-if)# ipv6 mld snooping immediate-leave*

**Syntax:** (config-if)# ipv6 igmp snooping immediate-leave

**Explanation:** Enable fast leave function on a specific port. When a leave packet is received, the switch immediately removes it from a multicast service without sending an IGMP group-specific (GS) query to that interface.

**Negation:** (config-if)# no ipv6 mld snooping immediate-leave

**Show:** > show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type>
[ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type>
[ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### *1.9.17.10 (config-if)# ipv6 mld snooping max-groups*

**Syntax:** (config-if)# ip igmp snooping max-groups <throttling>

**Explanation:** Specify the maximum number of multicast groups that a port can join at the same time.

**Parameters:**

<throttling>: This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new IGMP join reports will be dropped. By default, unlimited is selected. The allowed range can be specified is 1 to 10.

**Negation:** (config-if)# no ipv6 mld snooping max-groups

**Show:** > show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type>
[ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type>
[ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### *3. 9.19.11 (config-if)# ipv6 mld snooping mrouter*

**Syntax:** (config-if)# ipv6 mld snooping mrouter

**Explanation:** Set this interface to Router port. If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

**Negation:** (config-if)# no ipv6 mld snooping mrouter

**Show:** > show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type>
[ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
> show ipv6 mld snooping mrouter [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type>
[ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping mrouter [ detail ]

## 1.9.18 (config)# lacp

### 1.9.18.1 (config)# lacp system-priority

**Syntax:** (configure)# lacp system-priority <v_1_to_65535>

**Parameters:**

<v_1_to_65535>: The priority of the port. The allowed value range is from 1 to 65535.

**Explanation:** Configure system priority for LACP function. The lower number means greater priority. This priority value controls which ports will be active and which ones will be in a backup role.

**Example:** Set LACP system priority value to 100.

```
# config t
(config)# lacp system-priority 100
```

**Negation:** (config)# no lacp system-priority <v_1_to_65535>

**Show:** # show lacp { internal **|** statistics **|** system-id **|** neighbour }

### 1.9.18.2 (config-if)# lacp

**Syntax:** (config-if)# lacp

**Explanation:** Enable LACP on this interface.

**Example:** Enable LACP on port 1.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# lacp
(config-if)#
```

**Negation:** (config-if)# no lacp

**Show:** # show lacp { internal **|** statistics **|** system-id **|** neighbour }

**Clear:** # clear lacp statistics

### 1.9.18.3 (config-if)# lacp key

**Syntax:** (config-if)# lacp key { <v_1_to_65535> | auto }

**Explanation:** Configure a LACP key for this interface.

**Parameters:**

{ <v_1_to_65535> | auto }: Specify a LACP key for this interface. The “auto” setting sets the key as appropriate by the physical link speed. If you want a user-defined key value, enter a value between 1 and 65535. Ports in an

aggregated link group must have the same LACP port Key. In order to allow a port to join an aggregated group, the port Key must be set to the same value.

**Negation:** (config-if)# no lacp key { <v_1_to_65535> **|** auto }

**Show:** # show lacp { internal **|** statistics **|** system-id **|** neighbour }

### *1.9.18.4 (config-if)# lacp port-priority <v_1_to_65535>*

**Syntax:** (config-if)# lacp port-priority <v_1_to_65535>

**Explanation:** Configure a LACP key for this interface.

**Parameters:**

<v_1_to_65535>}: Specify a LACP port priority for this interface. The lower number means greater priority. This priority value controls which ports will be active and which ones will be in a backup role.

**Negation:** (config-if)# no lacp port-priority <v_1_to_65535>

**Show:** # show lacp { internal **|** statistics **|** system-id **|** neighbour }

### *1.9.18.5 (config-if)# lacp role { active | passive }*

**Syntax:** (config-if)# lacp role { active **|** passive }

**Explanation:** Configure LACP role for this interface.

**Parameters:**

{ active **|** passive }: Specify either "Active" or "Passive" role depending on the device's capability of negotiating and sending LACP control packets. Ports that are designated as "Active" are able to process and send LACP control frames. Hence, this allows LACP compliant devices to negotiate the aggregated like so that the group may be changed dynamically as required. In order to add or remove ports from the group, at least one of the participating devices must set to "Active" LACP ports.

**Negation:** (config-if)# no lacp role { active **|** passive }

**Show:** # show lacp { internal **|** statistics **|** system-id **|** neighbour }

### *1.9.18.6 (config-if)# lacp timeout { fast | slow }*

**Syntax:** (config-if)# lacp timeout { fast **|** slow }

**Explanation:** Configure timeout mode.

**Parameters:**

{ fast **|** slow }: 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.

**Negation:** (config-if)# no lacp timeout { fast **|** slow }

**Show:** # show lacp { internal **|** statistics **|** system-id **|** neighbour }

## *1.9.19 (config)# line*

### *1.9.19.1 (config)# line*

**Syntax:** (configure)# line { <0~16> **|** console 0 **|** vty <0~15> }

**Explanation:** Enter the specific line. When Enter is pressed, the command line changes to "(config-line)#".

**Parameters:**

{ <0~16> **|** console 0 **|** vty <0~15> }: Specify one of the options.

**<0~16> :** List of line numbers.

**console 0:** Console line connection.

**vty <0~15>:** VTY lines are the Virtual Terminal lines of the device, used solely to control inbound Telnet connections. They are virtual, in the sense that they are a function of software - there is no hardware associated with them.

**Example:** Enter Console 0 mode.

```
# config t
(config)# line console 0
(config-line)#
```

**Show:** >show line [alive]
#show line [alive]

### *1.9.19.2 (config-line)# do*

**Syntax:** (config-line)# do <command>

**Explanation:** To run EXEC. commands.

**Parameters:**

<command>: Enter the EXEC. command

**Example:** Show aaa settings.

```
# config t
(config)# line console 0
(config-line)# do show aaa
console : local
telnet  : local
ssh     : local
http    : local
(config-line)#
```

### *1.9.19.3 (config-line)# editing*

**Syntax:** (config-line)# editing

**Explanation:** Enable command line editing.

**Negation:** (config-line)# no editing

**Show:** >show line [alive]
#show line [alive]

### *1.9.19.4 (config-line)# end*

**Syntax:** (config-line)# end

**Explanation:** Return to EXEC. mode.

**Example:** Return to EXEC. mode.

```
# config t
(config)# line console 0
(config-line)# end
#
```

### *1.9.19.5 (config-line)# exec-banner*

**Syntax:** (config-line)# exec-banner

**Explanation:** Enable the display of EXEC banner.

**Example:** Enable the display of EXEC banner.

```
# config t
(config)# line console 0
(config-line)# exec-banner
```

**Negation:** (config-line)# no exec-banner

**Show:** >show line [alive]
#show line [alive]

### *1.9.19.6 (config-line)# exec-timeout*

**Syntax:** (config-line)# exec-timeout <min> [ <sec> ]

**Parameters:**

<min>: Specify timeout in minutes. The allowed range is 0 to 1440. Specify "0" to disable timeout function (CLI session will never timeout.)

[<sec>]: Specify timeout in seconds. The allowed range is 0 to 3600.

**Negation:** (config-line)# no exec-timeout

**Show:** >show line [alive]
#show line [alive]

### *1.9.19.7 (config-line)# exit*

**Syntax:** (config-line)# exit

**Explanation:** Return to Config mode.

**Example:** Return to Config mode.

```
# config t
(config)# line console 0
(config-line)# exit
(config)#
```

### *1.9.19.8 (config-line)# help*

**Syntax:** (config-line)# help

**Explanation:** Show the Help explanation.

**Example:** Show Help explanation.

```
# config t
(config)# line console 0
(config-line)# help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what Parameters match the input
   (e.g. 'show pr?'.)
```

#### *1.9.19.9 (config-line)# history size*

**Syntax:** (config-line)# history size <history_size>

**Explanation:** Control how many history commands are displayed.

**Parameters:**

<history_size>: The allowed range is 0 to 32. 0 means “disable”.

**Example:** Set history size to 10.

```
# config t
(config)# line console 0
(config-line)# history size 10
```

**Negation:** (config-line)# no history size

**Show:** >show line [alive]
#show line [alive]

#### *1.9.19.10 (config-line)# length*

**Syntax:** (config-line)# length <length>

**Explanation:** Configure the number of lines displayed on the screen.

**Parameters:**

<length>: Specify the number of lines displayed on the screen. The allowed range is 3 to 512. Specify “0” for no pausing.

**Example:** Display 20 lines on the screen.

```
# config t
(config)# line console 0
(config-line)# length 20
(config-line)#
```

**Negation:** (config-line)# no length

**Show:** >show line [alive]
#show line [alive]

### *1.9.19.11 (config-line)# location*

**Syntax:** (config-line)# location <location>

**Explanation:** Configure the descriptive location of this device.

**Parameters:**

<location>: Location description for the terminal. The characters allowed are 32.

**Example:** Configure the location “cabinet5a”.

```
# config t
(config)# line console 0
(config-line)# location cabinet5a
(config-line)#
```

**Negation:** (config-line)# no location

**Show:** >show line [alive]
#show line [alive]

### *1.9.19.12 (config-line)# motd-banner*

**Syntax:** (config-line)# motd-banner

**Explanation:** Enable the display of motd (message of the day) banner.

**Example:** Enable motd banner.

```
# config t
(config)# line console 0
(config-line)# motd-banner
(config-line)#
```

**Negation:** (config-line)# no motd-banner

**Show:** >show line [alive]
#show line [alive]

### *1.9.19.13 (config-line)# privilege level*

**Syntax:** (config-line)# privilege level <privileged_level>

**Explanation:** Configure the privilege level for the terminal line.

**Parameters:**

<privileged_level>: Privilege level for the terminal line. The allowed range is 0 to 15.

**Example:** Change the privilege level to 5 for vty 1.

```
# config t
(config)# line vty 1
(config-line)# privilege level 5
(config-line)#
```

**Negation:** (config-line)# no privilege level

**Show:** >show line [alive]
#show line [alive]

### *1.9.19.14 (config-line)# width*

**Syntax:** (config-line)# width <width>

**Explanation:** Configure the width of the terminal line.

**Parameters:**

<width>: Specify the width of the terminal line. The allowed range is 40 to 512. Specify “0” for unlimited width.

**Example:** Change of width of vty 1 to 60.

```
# config t
(config)# line vty 1
(config-line)# width 60
(config-line)#
```

**Negation:** (config-line)# no width

**Show:** >show line [alive]
#show line [alive]

### *1.9.20 (config)# lldp*

#### *1.9.20.1 (config)# lldp holdtime*

**Syntax:** (config)# lldp holdtime <val>

**Explanation:** This setting defines how long LLDP frames are considered valid and is used to compute the TTL. The default is 4.

**Parameters:**

<val>: Specify the holdtime value. The allowed value is 2 to 10.

**Example:** Set the holdtime to 5.

```
# config t
(config)# lldp holdtime 5
```

**Negation:** (config)# no lldp holdtime

#### *1.9.20.2 (config)# lldp reinit*

**Syntax:** (config)# lldp reinit <val>

**Explanation:** Configure a delay between the shutdown frame and a new LLDP initialization.

**Parameters:**

<val>: Specify a value between 1 and 10 (seconds).

**Example:** Set the LLDP re-initiation value to 3.

```
# config t
(config)# lldp reinit 3
```

**Negation:** (config)# no lldp reinit

#### *1.9.20.3 (config)# lldp timer*

**Syntax:** (config)# lldp timer <val>

**Explanation:** Configure the interval between LLDP frames are sent to its neighbors for updated discovery information. The default is 30 seconds.

**Parameters:**

<val>: Specify a value between 5 and 32768 (seconds).

**Example:** Set the LLDP timer value to 35.

```
# config t
(config)# lldp timer 35
```

**Negation:** (config)# no lldp timer

### *1.9.20.4 (config)# lldp transmission-delay*

**Syntax:** (config)# lldp transmission-delay <val>

**Parameters:**

<val>: Specify a value between 1 and 8192 (seconds).

**Explanation:** Configure a delay between the LLDP frames that contain changed configurations. Tx Delay cannot be larger than 1/4 of the Tx interval value.

**Example:** Set the LLDP transmission delay value to 2.

```
# config t
(config)# lldp transmission-delay 2
```

**Negation:** (config)# no lldp transmission-delay

### *1.9.20.5 (config)# lldp med datum*

**Syntax:** (config)# lldp med datum { wgs84 **|** nad83-navd88 **|** nad83-mllw }

**Explanation:** The Map Datum is used for the coordinates given in above options.

**Parameters:**

{ wgs84 **|** nad83-navd88 **|** nad83-mllw }: Specify one of the options.

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

**Example:** Set the map datum to wgs84.

```
# config t
(config)# lldp med datum wgs84
```

**Negation:** (config)# no lldp med datum

### *1.9.20.6 (config)# lldp med fast*

**Syntax:** (config)# lldp med fast <v_1_to_10>

**Explanation:** Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy. With this in mind, LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. With Fast start repeat count it is possible to specify the number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including between Network Connectivity Devices, or to other types of links.

**Parameters:**

<v_1_to_10>: Specify a valid value between 1 and 10.

**Example:** Set the value to 5.

```
# config t
(config)# lldp med fast 5
```

**Negation:** (config)# no lldp med fast

### *1.9.20.7 (config)# lldp med location-tlv altitude*

**Syntax:** (config)# lldp med location-tlv altitude { meters **|** floors } <v_word11>

**Explanation:** Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). “meters” means meters of Altitude defined by the vertical datum specified; while, “floors” means altitude in a form more relevant in buildings which have different floor-to-floor dimensions.

**Parameters:**

{ meters **|** floors }: Specify one of the options.

<v_word11>: Specify a value for the specified option.

**Example:** Set the altitude value to “floors 10”.

```
# config t
(config)# lldp med location-tlv altitude floors 10
```

**Negation:** (config)# no lldp med location-tlv altitude

### *1.9.20.8 (config)# lldp med location-tlv civic-addr*

**Syntax:** (config)# lldp med location-tlv civic-addr {country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code }<v_string250>

**Explanation:** Configure civic address information.

**Parameters:**

{country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code}: Specify one of the options.

**country:** 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.

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

**block:** Neighbourhood, block.

**street:** Street - Example: Poppelvej.

**leading-street-direction:** Example: N.

**trailings-street-suffix:** Example: SW.

**street-suffix:** Ave, Platz.

**house-no:** Specify house number.

**house-no-suffix:** Example: A, 1/2.

**landmark:** Landmark or vanity address - Example: Columbia University.

**additional-info:** Example: South Wing.

**Name:** Example: Flemming Jahn.

**zip-code:** Postal/zip code - Example: 2791.

**building:** Building (structure). Example: Low Library.

**apartment:** Unit (Apartment, suite). Example: Apt 42.

**floor:** Example: 4.

**room-number:** Room number - Example: 450F.

**place-type:** Example: Office.

**postal-community-name:** Example: Leonia.

**p-o-box:** Example: 12345.

**additional code:** Example: 1320300003.

**Example:** Set the country code to “UK”.

```
# config t
(config)# lldp med location-tlv civic-addr country UK
```

**Negation:** (config)# no lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code }

### *1.9.20.9 (config)# lldp med location-tlv elin-addr*

**Syntax:** (config)# lldp med location-tlv elin-addr <v_word25>

**Explanation:** Configure a value for Emergency Location Information.

**Parameters:**

<v_word25>: A value for Emergency Location Information (ELIN).

**Example:** Set the emergency location information to “911”.

```
# config t
(config)# lldp med location-tlv elin-addr 911
```

**Negation:** (config)# no lldp med location-tlv elin-addr

### *1.9.20.10 (config)# lldp med location-tlv latitude*

**Syntax:** (config)# lldp med location-tlv latitude { north | south } <v_word8>

**Explanation:** Configure a value for latitude. Latitude value should be between 0 and 90.

**Parameters:**

{ north | south }: Specify one of the options, either north or south.

<v_word8>: Specify latitude value for the selected option.

**Example:** Set the north latitude to 5.

```
# config t
(config)# lldp med location-tlv latitude north 5
```

**Negation:** (config)# no lldp med location-tlv latitude

### *1.9.20.11 (config)# lldp med location-tlv longitude*

**Syntax:** (config)# lldp med location-tlv longitude { west **|** east } <v_word9>

**Explanation:** Configure a value for longitude. Longitude value should be between 0 and 180.

**Parameters:**

{ west **|** east }: Specify one of the options, either west or east.

<v_word9>: Specify longitude value for the selected option.

**Example:** Set the west longitude to 90.

```
# config t
(config)# lldp med location-tlv longitude west 90
```

**Negation:** (config)# no lldp med location-tlv longitude

### *1.9.20.12 (config)# lldpmed media-vlan-policy*

**Syntax:** (config)# lldp med media-vlan-policy <policy_index> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { tagged <v_vlan_id> | untagged } [ l2-priority <v_0_to_7> ] [ dscp <v_0_to_63> ]

**Explanation:** Configure a LLDP MED policy ID for a service.

**Parameters:**

<policy_index>: Specify a policy ID. The valid range is from 0 to 31.

{ voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video **|** video-signaling }: Specify one of the services for this policy ID.

{ tagged <v_vlan_id> | untagged }: Specify whether this service is tagged or untagged. When “tagged” is specified, a VLAN ID should be provided.

[ l2-priority <v_0_to_7> ]: Specify a value for L2 priority. The valid value is from 0 to 7.

[ dscp <v_0_to_63> ]: Specify a value for DSCP. The valid value is from 0 to 63.

**Example:** Create a policy ID 1 for tagged Voice VLAN.

```
# config t
(config)# lldp med media-vlan-policy 1 voice tagged 100 l2-priority 7 DSCP 63
```

**Negation:** (config)# no lldp med media-vlan-policy <policies_list>

**Show:** > show lldp med media-vlan-policy [ <v_0_to_31> ]

# show lldp med media-vlan-policy [ <v_0_to_31> ]

### *1.9.20.13 (config-if)# lldp cdp-aware*

**Syntax:** (config-if)# lldp cdp-aware

**Explanation:** Configures if the interface shall be CDP aware (CDP discovery information is added to the LLDP neighbor table).

**Example:** Set interface 1 to CDP aware.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# lldp cdp-aware
```

**Negation:** (config-if)# no lldp cdp-aware

**Show: >** show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### *1.9.20.14 (config-if)# lldp med media-vlan policy-list*

**Syntax:** (config-if)# lldp med media-vlan policy-list <v_range_list>

**Explanation:** To apply MED Media-VLAN policy of LLDP on this interface.

**Parameters:**

<v_range_list>: Assign a policy to this interface.

**Negation:** (config-if)# no lldp med media-vlan policy-list <v_range_list>

**Show:** > show lldp med media-vlan-policy [ <v_0_to_31> ]
# show lldp med media-vlan-policy [ <v_0_to_31> ]

### *1.9.20.15 (config-if)# lldp med transmit-tlv*

**Syntax:** (config-if)# lldp med transmit-tlv [ capabilities ] [ location ] [ network-policy ]

**Explanation:** To configure LLDP-MED TLV Type for specific interface.

**Parameters:**

[ capabilities ]: Enable transmission of the optional capabilities TLV.

[ location ]: Enable transmission of the optional location TLV.

[ network-policy ]: Enable transmission of the optional network policy TLV.

**Negation:** (config-if)# no lldp med transmit-tlv [ capabilities ] [ location ] [ network-policy ]

**Show:** > show lldp med media-vlan-policy [ <v_0_to_31> ]
# show lldp med media-vlan-policy [ <v_0_to_31> ]

#### 1.9.20.16 (config-if)# lldp receive

**Syntax:** (config-if)# lldp receive

**Explanation:** The switch will analyze LLDP information received from neighbours.

**Negation:** (config-if)# no lldp receive

**Show:** > show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]

#### 1.9.20.17 (config-if)# lldp tlv-select

**Syntax:** (config-if)# lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }

**Explanation:** To configure LLDP-MED TLV attributes for specific interface.

**Parameters:**

{ management-address | port-description | system-capabilities | system-description | system-name }: Specify a LLDP TLV attribute. LLDP uses several attributes to discover neighbour devices. These attributes contains type, length, and value descriptions and are referred to TLVs. Details such as port description, system name, system description, system capabilities, management address can be sent from this device.

**Negation:** (config-if)# no lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }

**Show:** > show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]

#### 1.9.20.18 (config-if)# lldp transmit

**Syntax:** (config-if)# lldp transmit

**Explanation:** To configure LLDP Tx only mode for specific interface

**Negation:** (config-if)# no lldp transmit

**Show:** # show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### 1.9.21 (config)# logging

#### 1.9.21.1 (config)# logging on

**Syntax:** (config)# logging on

**Explanation:** This sets the server mode operation. When the mode of operation is enabled (on), the syslog message will send out to syslog server (at the server address). The syslog protocol is based on UDP communication and received on UDP port 514. Syslog server will not send acknowledgments back to the 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. When the mode of operation is disabled, no syslog packets are sent out.

**Example:** Enable log server operation.

```
# config t
(config)# logging on
```

**Negation:** (config)# no logging on

**Show:** # show logging

Clear: # clear logging [ info ] [ warning ] [ error ] [ switch <switch_list> ]

### *1.9.21.2 (config)# logging host*

**Syntax:** (config)# logging host { <v_ipv4_ucast> **|** <v_word45> }

**Parameters:**

{ <hostname> | <ipv4_ucast> }: Specify one of the options. The hostname is the domain name of the log server; while the latter is IPv4 address of the log server.

**Explanation:** Configure log server address.

**Example:** Use IPv4 address to configure log server.

```
# config t
(config)# logging host 192.168.1.253
```

**Negation:** (config)# no logging host

**Show:** # show logging
# show logging <logging_id: 1-4294967295>
# show logging [info] [warning] [error]

### *1.9.21.3 (config)# logging level*

**Syntax:** (config)# logging level { info **|** warning **|** error }

**Explanation:** Configure what kind of messages will send to syslog server.

**Parameters:**

{ info **|** warning **|** error }: Specify one of the log message options.

**Info:** Send information, warnings and errors.

**Warning:** Send warnings and errors.

**Error:** Send errors only.

**Example:** Send error messages to log server.

```
# config t
(config)# logging level error
```

**Show:** # show logging
# show logging <logging_id: 1-4294967295>
# show logging [info] [warning] [error]

## *1.9.22 (config)# loop-protect*

### *1.9.22.1 (config)# loop-protect*

**Syntax:** (config)# loop-protect

**Explanation:** Enable loop protection function.

**Example:** Enable loop protection function.

```
# config t
(config)# loop-protect
```

**Negation:** (config)# no loop-protect

**Show:** # show loop-protect [ interface ( <port_type> [ <plist> ] ) ]

### *1.9.22.2 (config)# loop-protect shutdown-time*

**Syntax:** (config)# loop-protect shutdown-time <t>

**Explanation:** Configure the period for which a port will be kept disabled.

**Parameters:**

**<t: 0-604800>:** Specify a shutdown time value. The valid values are from 0 to 604800 seconds. 0 means that a port is kept disabled until next device restart.

**Example:** Set the shutdown time value to 180 seconds.

```
# config t
(config)# loop-protect shutdown-time 180
```

**Negation:** (config)# no loop-protect shutdown-time

**Show:** # show loop-protect [ interface ( <port_type> [ <plist> ] ) ]

### *1.9.22.3 (config)# loop-protect transmit-time*

**Syntax:** (config)# loop-protect transmit-time <t>

**Explanation:** Configure the interval between each loop protection PDU sent on each port.

**Parameters:**

<t: 1-10>: Specify a transmit time value. The valid values are from 1 to 10 seconds.

**Example:** Set the transmit time value to 5 seconds.

```
# config t
(config)# loop-protect transmit-time 5
```

**Negation:** (config)# no loop-protect transmit-time

**Show:** # show loop-protect [ interface ( <port_type> [ <plist> ] ) ]

### *1.9.22.4 (config-if)# loop-protect*

**Syntax:** (config-if)# loop-protect

**Explanation:** Enable loop protection function on this interface.

**Negation:** (config-if)# no loop-protect

**Show:** # show loop-protect [ interface ( <port_type> [ <plist> ] ) ]

### *1.9.22.5 (config-if)# loop-protect action*

**Syntax:** (config-if)# loop-protect action { [ shutdown ] [ log ] }

**Explanation:** Configure the action taken when loops are detected on a port.

**Parameters:**

{ [ shutdown ] [ log ] }: When a loop is detected on a port, the loop protection will immediately take appropriate actions. Actions will be taken include “Shutdown Port”, “Shutdown Port and Log” or “Log Only”.

**Negation:** (config-if)# no loop-protect action

**Show:** # show loop-protect [ interface ( <port_type> [ <plist> ] ) ]

### *1.9.22.6 (config-if)# loop-protect tx-mode*

**Syntax:** (config-if)# loop-protect tx-mode

**Explanation:** Enable a port to actively generate loop protection PDUs.

**Negation:** (config-if)# no loop-protect tx-mode

**Show:** # show loop-protect [ interface ( <port_type> [ <plist> ] ) ]

### 1.9.23 (config)# mac

#### 1.9.23.1 (config)# mac address-table aging-time

**Syntax:** (config)# mac address-table aging-time <v_0_10_to_1000000>

**Explanation:** Configure the aging time for a learned MAC to be appeared in MAC learning table.

**Parameters:**

<v_0_10_to_1000000>: Specify an aging time value for MAC address table. The valid values are from 10 to 1000000 (seconds). Using “0” to disable aging time function.

**Example:** Set the aging time to 600 seconds.

```
# config t
(config)# mac address-table aging-time 600
```

**Negation:** (config)# no mac address-table aging-time
(config)# no mac address-table aging-time <v_0_10_to_1000000>

**Show:** > show mac address-table [ conf | static | aging-time | { { learning | count } [ interface ( <port_type> [<v_port_type_list>])]}|{address<v_mac_addr>[vlan<v_vlan_id>]}|vlan<v_vlan_id_1>|interface ( <port_type> [ <v_port_type_list_1> ] ) ]
# show mac address-table [ conf | static | aging-time | { { learning | count } [ interface ( <port_type> [<v_port_type_list>])]}|{address<v_mac_addr>[vlan<v_vlan_id>]}|vlan<v_vlan_id_1>|interface ( <port_type> [ <v_port_type_list_1> ] ) ]
# show mac address-table aging-time

#### 1.9.23.2 (config)# mac address-table static

**Syntax:** (config)# mac address-table static <v_mac_addr> vlan <v_vlan_id> interface ( <port_type> [ <v_port_type_list> ])

**Explanation:** Configure the static MAC address mapping table.

**Parameters:**

<v_mac_addr>: Specify MAC address in “xx:xx:xx:xx:xx:xx” format.

vlan <v_vlan_id>: Specify the VLAN ID for this entry.

interface ( <port_type> [ <v_port_type_list> ] ): Specify the interface port type and the port number.

**Example:** Add a static MAC address “11:11:22:22:33:33” to MAC address table.

```
# config t
(config)# mac address-table static 11:11:22:22:33:33 vlan 1 interface
GigabitEthernet 1/1-10
```

**Negation:** (config)# no mac address-table static <v_mac_addr> vlan <v_vlan_id> interface ( <port_type> [ <v_port_type_list> ])

**Show:** > show mac address-table [ conf **|** static **|** aging-time **|** { { learning **|** count } [ interface ( <port_type> [<v_port_type_list>])]}|{address<v_mac_addr>[vlan<v_vlan_id>]}|vlan<v_vlan_id_1>|interface ( <port_type> [ <v_port_type_list_1> ] ) ]
# show mac address-table [ conf **|** static **|** aging-time **|** { { learning **|** count } [ interface ( <port_type> [<v_port_type_list>])]}|{address<v_mac_addr>[vlan<v_vlan_id>]}|vlan<v_vlan_id_1>|interface ( <port_type> [ <v_port_type_list_1> ] ) ]

**Clear:** # clear mac address-table

#### *1.9.23.3 (config-if)# mac address-table learning*

**Syntax:** (config)# mac address-table learning [ secure ]

**Explanation:** Set this interface to secure mode.

**Parameters:**

[ secure ]: Only static MAC entries listed in “Static MAC Table Configuration” are learned. Others will be dropped.

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

**Negation:** (config-if)# no mac address-table learning [ secure ]

**Show:** > show mac address-table [ conf **|** static **|** aging-time **|** { { learning **|** count } [ interface ( <port_type> [<v_port_type_list>])]}|{address<v_mac_addr>[vlan<v_vlan_id>]}|vlan<v_vlan_id_1>|interface ( <port_type> [ <v_port_type_list_1> ] ) ]
# show mac address-table [ conf **|** static **|** aging-time **|** { { learning **|** count } [ interface ( <port_type> [<v_port_type_list>])]}|{address<v_mac_addr>[vlan<v_vlan_id>]}|vlan<v_vlan_id_1>|interface ( <port_type> [ <v_port_type_list_1> ] ) ]

**Clear:** # clear mac address-table

### *1.9.24 (config-if)# media-type*

**Syntax:** (config-if)# media-type { rj45 **|** sfp **|** dual }

**Explanation:** Configure the media type supported for this specific interface.

**Parameters:**

{ rj45 **|** sfp **|** dual }: The options are RJ-45, SFP, or dual (both RJ-45 & SFP are supported.).

**Negation:** (config-if)# no media-type

### *1.9.25 (config-if)# mtu*

**Syntax:** (config-if)# mtu <max_length>

**Explanation:** Configure the maximum transmission unit for this specific interface.

**Parameters:**

<max_length: 1518-9600>}: Specify the MTU. The range is 1518 to 9600 bytes.

**Negation:** (config-if)# no mtu

**Show:** # show interface ( <port_type> [ <v_port_type_list> ] ) status

## *1.9.26 (config)# monitor*

### *1.9.26.1 (config)# monitor destination interface*

**Syntax:** (config)# monitor destination interface <port_type> <in_port_type>

**Explanation:** Configure which port traffic should be mirrored to.

**Parameters:**

<port_type>: Specify the interface type.

<in_port_type>: Specify the port number.

**Example:** Set the traffic to be mirrored to Gigabit Ethernet port 10.

```
# config t
(config)# monitor destination interface gigabitethernet 1/10
```

**Negation:** (config)# no monitor destination

#### *1.9.26.2 (config)# monitor source*

**Syntax:** (config)# monitor source{ [ interface ( <port_type>) [ <v_port_type_list> ] ]} **|** { cpu [ <cpu_switch_range> ] } { both **|** rx **|** tx }

**Explanation:** Configure which source ports' RX or TX traffic should be mirrored to the destination port.

**Parameters:**

{ [ interface ( <port_type>) [ <v_port_type_list> ] ]}: Specify one of the options. * means all interfaces.

{ both **|** rx **|** tx }: Specify which direction of traffic should be mirrored to the destination port. "both" means both received and transmitted traffic. "rx" means received traffic. "tx" means transmitted traffic.

**Example:** Set port 1 to 5's RX traffic to be mirrored to the destination port.

```
# config t
(config)# monitor source interface GigabitEthernet 1/1-5 rx
```

**Negation:** (config)# no monitor source{{interface (<port_type> [<v_port_type_list>])} **|** {cpu [ <cpu_switch_range> ] } }

### *1.9.27 (config)# ntp*

#### *1.9.27.1 (config)# ntp*

**Syntax:** (config)# ntp

**Explanation:** Enable NTP function.

**Example:** Enable NTP function.

```
# config t
(config)# ntp
```

**Negation:** (config)# no ntp

**Show:** # show ntp status

#### *1.9.27.2 (config)# ntp server*

**Syntax:** (config)# ntp server <index_var> ip-address { <ipv4_var> **|** <ipv6_var> **|** <name_var> }

**Explanation:** Configure a list of NTP server's address.

**Parameters:**

< index_var: 1-5>: Specify the index number of NTP server. The allowed range is from 1 to 5. The NTP servers are tried in numeric order. If 'Server 1' is unavailable, the NTP client will try to contact 'Server 2'.

{ <ipv4_var> **|** <ipv6_var> **|** <name_var> }: Specify one of the three options.

**<ipv4_var>:** IPv4 address.

**<ipv6_var>:** 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.

**<name_var>:** The domain name for NTP server.

**Example:** Set the NTP server 1 to 192.168.1.253.

```
# config t
(config)# ntp server 1 ip-address 192.168.1.253
```

**Negation:** (config)# no ntp server <index_var>

**Show:** # show ntp status

## *1.9.28 (config)# port-security*

### *1.9.28.1 (config)# port-security*

**Syntax:** (config)# port-security

**Explanation:** Enable port security function globally.

**Example:** Enable port security function globally.

```
# config t
(config)# port-security
```

**Negation:** (config)# no port-security

**Show: >** show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### *1.9.28.2 (config)# port-security aging*

**Syntax:** (config)# port-security aging

**Explanation:** Enable port security aging function. If enabled, secured MAC addresses are subject to aging as discussed in "Aging time" command. 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.

**Example:** Enable port security aging function.

```
# config t
(config)# port-security aging
```

**Negation:** (config)# no port-security aging

**Show:** > show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### *1.9.28.3 (config)# port-security aging time*

**Syntax:** (config)# port-security aging time <v_10_to_10000000>

**Explanation:** Configure a desired aging time value. If "Aging" is enabled, secured MAC addresses are subject to aging as discussed this command. 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.

**Parameters:**

<v_10_to_10000000>: Specify the aging time value. The allowed range is between 10 and 10,000,000 seconds.

**Example:** Set the aging time value to 1800 seconds.

```
# config t
(config)# port-security aging time 1800
```

**Negation:** (config)# no port-security aging time

**Show:** > show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### *1.9.28.4 (config-if)# port-security*

**Syntax:** (configt-if)# port-security

**Explanation:** Enable the port security function on the selected ports.

**Example:** Enable Gigabit Ethernet port 1-10's port security function.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# port-security
```

**Negation:** (configt-if)# no port-security

**Show:** > show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### *1.9.28.5 (config-if)# port-security maximum*

**Syntax:** (configt-if)# port-security maximum [ <v_1_to_1024> ]

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

**Parameters:**

[ <v_1_to_1024> ]: Specify a value between 1 and 1024.

**Example:** Limit Gigabit Ethernet port 1-10's MAC addresses can be learnt to 5.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# port-security maximum 5
```

**Negation:** (configt-if)# no port-security maximum

**Show:** > show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### *1.9.28.6 (config-if)# port-security violation*

**Syntax:** (configt-if)# port-security violation { protect **|** trap **|** trap-shutdown **|** shutdown }

**Explanation:** If the limit is exceeded, the specified action will take effect.

**Parameters:**

{ protect **|** trap **|** trap-shutdown **|** shutdown }: Specify one of the actions taken when the limit is exceeded.

**protect:** Do not allow more than the specified limit of MAC addresses to access on a port. No action is further taken.

**trap:** If Limit + 1 MAC addresses are 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 is exceeded.

**trap-shutdown:** If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

**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 addresses 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:
* Boot the switch
* Disable and re-enable Limit Control on the port or the switch
* Click the "Reopen" button

**Example:** Send a SNMP trap when the limit is exceeded.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# port-security violation trap
```

**Negation:** (configt-if)# no port-security violation

**Show:** > show port-security port [interface (<port_type> [<v_port_type_list>])]
# show port-security port [interface (<port_type> [<v_port_type_list>])]

### *1.9.29 (config)# privilege*

**Syntax:** (config)# privilege { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr **|** dhcp-pool **|** rfc2544-profile } level <privilege> <cmd>

**Explanation:** This command is used to change the privilege level of commands available in Configuration mode.

**Parameters:**

{exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile }: Specify the group command that you want to configure.

level <privilege>: Specify the privilege level. The allowed range is 0 to 15.

<cmd>: Initial valid words and literals of the command to modify, in 128 characters.

**Example:** The following example sets the privilege level to 15 for any Exec mode (user or privileged) command that start with the letter"v"

```
# config t
(config)# privilege exec level 15 host
```

**Negation**: (config)# no privilege { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr **|** dhcp-pool **|** rfc2544-profile } level <0-15> <cmd>

**Show:** > show privilege
# show privilege

## *1.9.30 (config-if)# pvlan*

### *1.9.30.1 (config-if)# pvlan*

**Syntax:** (config-if)# pvlan <pvlan_list>

**Explanation:** This command is used to configure private VLANs. New Private VLANs can be added and existing VLANs can be modified. Private VLANs are based on the source port mask and there are no connections to VLANs which 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.

**Parameters:**

<pvlan_list>: Specify the private VLAN ID.

**Negation:** (config-if)# no pvlan <pvlan_list>

**Show:** # show pvlan <pvlan_list>

### *1.9.30.2 (config-if)# pvlan isolation*

**Syntax:** (config-if)# pvlan isolation

**Explanation:** Enable Port Isolation function on this specific interface. Port Isolation is used to prevent communications between customer ports in a same Private VLAN. The port that is isolated from others cannot forward any unicast, multicast or broadcast traffic to any other ports in the same PVLAN.

**Negation:** (config-if)# no pvlan isolation

**Show:** # show pvlan isolation [ interface ( <port_type> [<plist>] ) ]

## *1.9.31 (config)# qos*

### *1.9.31.1 (config)# qos map cos-dscp*

**Syntax:** (config)# qos map cos-dscp <cos> dpl <dpl> dscp { <dscp_num> **|** { be **|** af11 **|** af12 **|** af13 **|** af21 **|** af22 **|** af23 **|** af31 **|** af32 **|** af33 **|** af41 **|** af42 **|** af43 **|** cs1 **|** cs2 **|** cs3 **|** cs4 **|** cs5 **|** cs6 **|** cs7 **|** ef **|** va } }

**Parameters:**

cos-dscp <cos>: Map COS to DSCP. Indicate the Class of Service level. The allowed range is 0 to 7. A CoS class of 0 has the lowest priority, while 7 has the highest priority.

dpl <dpl>: Specify the Drop Precedence Level. The allowed range is 0 to 7.

dscp { <dscp_num> **|** { be **|** af11 **|** af12 **|** af13 **|** af21 **|** af22 **|** af23 **|** af31 **|** af32 **|** af33 **|** af41 **|** af42 **|** af43 **|** cs1 **|** cs2 **|** cs3 **|** cs4 **|** cs5 **|** cs6 **|** cs7 **|** ef **|** va } }: Specify one of the DSCP values.

**<dscp_num: 0-63>:** The allowed number is from 0 to 63.
be: Default PHB (DSCP 0) for best effort traffic.

**af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43:** Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

**cs1|cs2|cs3|cs4|cs5|cs6|cs7:** Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

**ef:** Expedited Forwarding PHB (DSCP 46).

**va:** Voice Admit PHB (DSCP 44).

**Explanation:** Configure the COS-DSCP mapping.

**Example:** The following example sets DPL to 4, DSCP to cs4.

```
# config t
(config)# qos map cos-dscp 4 dpl 4 dscp cs4
```

**Negation**: (config)# no qos map cos-dscp <cos> dpl <dpl>

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } **|** wred **|** { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } **|** storm **|** { qce [ <qce> ] } ]

### *1.9.31.2 (config)# qos map dscp-classify*

**Syntax:** (config)# qos map dscp-classify { <dscp_num> **|** { be **|** af11 **|** af12 **|** af13 **|** af21 **|** af22 **|** af23 **|** af31 **|** af32 **|** af33 **|** af41 **|** af42 **|** af43 **|** cs1 **|** cs2 **|** cs3 **|** cs4 **|** cs5 **|** cs6 **|** cs7 **|** ef **|** va } }

**Parameters:**

dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

**<dscp_num: 0-63>:** The allowed number is from 0 to 63.

**be:** Default PHB (DSCP 0) for best effort traffic.

**af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43:** Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

**cs1|cs2|cs3|cs4|cs5|cs6|cs7:** Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

**ef:** Expedited Forwarding PHB (DSCP 46).

**va:** Voice Admit PHB (DSCP 44).

**Explanation:** Configure the DSCP Ingress classification.

**Example:** The following example sets DSCP Ingress classification to cs4.

```
# config t
(config)# qos map dscp-classify cs4
```

**Negation**: (config)# no qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.3 (config)# qos map dscp-cos*

**Syntax:** (config)# qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } cos <cos> dpl <dpl>

**Explanation:** Configure the DSCP-based QoS Ingress classification.

**Parameters:**

dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

**<dscp_num: 0-63>:** The allowed number is from 0 to 63.

**be:** Default PHB (DSCP 0) for best effort traffic.

**af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43:** Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

**cs1|cs2|cs3|cs4|cs5|cs6|cs7:** Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

**ef:** Expedited Forwarding PHB (DSCP 46).

**va:** Voice Admit PHB (DSCP 44).

cos <cos>: Indicate the Class of Service level. The allowed range is 0 to 7. A CoS class of 0 has the lowest priority, while 7 has the highest priority.

dpl <dpl>: Specify the Drop Precedence Level. The allowed range is 0 to 7.

**Negation**: (config)# no qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.4 (config)# qos map dscp-egress-translation*

**Syntax:** (config)# qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}}to{<dscp_num_tr> | {be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va }}

**Explanation:** Configure the DSCP Egress Mapping Table.

**Parameters:**

dscp-egress-translation{<dscp_num> | {be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va }}: Specify one of the DSCP values.

**<dscp_num: 0-63>:** The allowed number is from 0 to 63.

**be:** Default PHB (DSCP 0) for best effort traffic.

**af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43:** Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

**cs1|cs2|cs3|cs4|cs5|cs6|cs7:** Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

**ef:** Expedited Forwarding PHB (DSCP 46).

**va:** Voice Admit PHB (DSCP 44).

**Example:** The following example maps cs4 to cs5.

```
# config t
(config)# qos map dscp-egress-translation cs4 to cs5
```

**Negation**: (config)# no qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } <dpl>

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.5 (config)# qos map dscp-ingress-translation*

**Syntax:** (config)# qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}}to{<dscp_num_tr>|{be|af11| af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|cs3|cs4|cs5|cs6|cs7|ef| va }}

**Explanation:** Configure the DSCP Ingress Mapping Table.

**Parameters:**

dscp-ingress-translation{<dscp_num>|{be|af11|af12|af13|af21|af22|af23|af31|af32|af33|af41| af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va }}: Specify one of the DSCP values.

**<dscp_num: 0-63>:** The allowed number is from 0 to 63.

**be:** Default PHB (DSCP 0) for best effort traffic.

**af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43:** Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

**cs1|cs2|cs3|cs4|cs5|cs6|cs7:** Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

**ef:** Expedited Forwarding PHB (DSCP 46).

**va:** Voice Admit PHB (DSCP 44).

**Example:** The following example maps cs4 to cs5.

```
# config t
(config)# qos map dscp-ingress-translation cs4 to cs5
```

**Negation**: (config)# no qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.6 (config)# qos qce refresh*

**Syntax:** (config)# qos qce refresh

**Explanation:** To refresh QCE.

**Example:** Refresh QCE.

```
# config t
(config)# qos qce refresh
```

### *1.9.31.7 (config)# qos qce update*

**Syntax:** (config)# qos qce { [ update ] } <qce_id> [ { next <qce_id_next> } | last ] [ interface ( <port_type> [ <port_list> ] ) ] [ smac { <smac> | <smac_24> | any } ] [ dmac { <dmac> | unicast | multicast | broadcast | any } ] [ tag { [ type { untagged | tagged | c-tagged | s-tagged | any } ] [ vid { <ot_vid> | any } ] [ pcp { <ot_pcp> | any } ] [ dei {<ot_dei> | any}]}*1][inner-tag{[type{untagged | tagged | c-tagged | s-tagged | any}][vid{<it_vid> | any}] [pcp{<it_pcp> | any}][dei{<it_dei> | any}]}*1][frame-type{any | {etype[{<etype_type> | any}]} | {llc [dsap{<llc_dsap> | any}][ssap{<llc_ssap> | any}][control{<llc_control> | any}]} | {snap[{<snap_data> | any}]} | {ipv4[proto{<pr4> | tcp | udp | any}][sip{<sip4> | any}][dip{<dip4> | any}][dscp{<dscp4> | {be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any } ] [ fragment { yes | no | any } ] [ sport { <sp4> | any } ] [ dport { <dp4> | any } ] } | { ipv6 [ proto {<pr6> | tcp | udp | any}][sip{<sip6> | any}][dip{<dip6> | any}][dscp{<dscp6> | {be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va} | any}] [sport{<sp6> | any}][dport{<dp6> | any}]}}][action{[cos{<action_cos> | default}][dpl{<action_dpl> | default}][pcp-dei{<action_pcp><action_dei> | default}][dscp{<action_dscp_dscp> | {be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va} | default}] [policy { <action_policy> | default } ] }*1 ]

**Explanation:** To update the QCE.

**Parameters:**

{ [ update ] }: Update the QCE.

<qce_id>: Specify the QCE ID.

[ { next <qce_id_next> } | last ]: Put this QCE next to the specified one or to the last one.

[interface (<port_type> [<port_list>])]: Specify port type and port number that apply to this updated QCE rule.

[ smac { <smac> | <smac_24> | any } ]: Set up the matched SMAC.

[ dmac { <dmac> | unicast | multicast | broadcast | any } ]: Set up the matached DMAC.

[tag{[type{untagged | tagged | c-tagged | s-tagged | any}]: Set up the matched tag type.
[vid{<ot_vid> | any}]: Specify a specific VID or VID range or specify “any” to allow any VIDs.

[pcp{<ot_pcp> | any}]: Specify a specific PCP or PCP range or specify “any” to allow any PCP values.

[ dei { <ot_dei> | any } ] } ]: Specify a specific DEI or specify “any” to allow any DEI.

[ frame-type { any | { etype [ { <etype_type> | any } ] } | { llc [ dsap { <llc_dsap> | any } ] [ ssap { <llc_ssap> | any } ] [ control { <llc_control> | any } ] } | { snap [ { <snap_data> | any } ] } | { ipv4 [ proto { <pr4> | tcp | udp | any } ] [ sip { <sip4> | any } ] [ dip { <dip4> | any } ] [ dscp { <dscp4> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any } ] [ fragment { yes | no | any } ] [ sport { <sp4> | any } ] [ dport { <dp4> | any } ] } | { ipv6 [ proto { <pr6> | tcp | udp | any } ] [ sip { <sip6> | any } ] [ dip { <dip6> | any } ] [ dscp { <dscp6> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any } ] [ sport { <sp6> | any } ] [ dport { <dp6> | any } ] } } ]: Specify the frame type that applies to this QCE rule.

**any:** By default, any is used which means that all types of frames are allowed.

**etype:** This option can only be used to filter Ethernet II formatted packets. (Options: Any, Specific – 600-ffff hex; Default: ffff). Note that 800 (IPv4) and 86DD (IPv6) are excluded. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

**llc:** LLC refers to Link Logical Control and further provides three options.

**dsap:** DSAP stands for Destination Service Access Point address. By default, any is used. Specify “any” or indicate a value (0x00 to 0xFF).

**ssap:** SSAP stands for Source Service Access Point address. By default, any is used. Specify “any” or indicate a value (0x00 - 0xFF).

**control:** Control field may contain command, response, or sequence information depending on whether the LLC frame type is Unnumbered, Supervisory, or Information. By default, any is used. Specify “any” or indicate a value (0x00 to 0xFF).

**snap:** SubNetwork Access Protocol can be distinguished by an OUI and a Protocol ID. (Options for PID: Any, Specific (0x00-0xffff); Default: Any) 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 that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI is other than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

**ipv4:**

**proto:** IPv4 frame type includes Any, TCP, UDP, Other. If “TCP” or “UDP” is specified, you might further define Sport (Source port number) and Dport (Destination port number).

**sip:** Specify source IP type. By default, any is used. Indicate self-defined source IP and submask format. The address and mask must be in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero

**dscp:** By default, any is used. Indicate a DSCP value or a range of DSCP value.

**fragment:** By default, any is used. Datagrams sometimes may be fragmented to ensure they can pass through a network device that uses a maximum transfer unit smaller than the original packet’s size.

**ipv6:**

**proto:** IPv6 protocol includes Any, TCP, UDP, Other. If “TCP” or “UDP” is specified, you may need to further define Sport (Source port number) and Dport (Destination port number).

**sip:** Specify source IP type. By default, any is used. You can also indicate self-defined source IP and submask format.

**dscp:** By default, any is used. You can also indicate a DSCP value or a range of DSCP value.

[action{[cos{<action_cos> **|** default}]: Specify the classification action taken on ingress frame if the parameters match the frame's content. If a frame matches the QCE, it will be put in the queue corresponding to the specified QoS class or placed in a queue based on basic classification rules.

[dpl{<action_dpl> **|** default}]: If a frame matches the QCE, the drop precedence level will be set to the specified value or left unchanged.

[pcp-dei{<action_pcp><action_dei>|default}]: If a frame matches the QCE, the PCP or DEI value will be set to the specified one.

[ dscp { <action_dscp_dscp> **|** { be **|** af11 **|** af12 **|** af13 **|** af21 **|** af22 **|** af23 **|** af31 **|** af32 **|** af33 **|** af41 **|** af42 **|** af43 **|** cs1 **|** cs2 **|** cs3 **|** cs4 **|** cs5 **|** cs6 **|** cs7 **|** ef **|** va } **|** default } ] [ policy { <action_policy> **|** default } ] }*1 ]: If a frame matches the QCE, the DSCP value will be set to the specified one.

**Negation**: (config)# no qos qce <qce_id_range>

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } **|** wred **|** { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } **|** storm **|** { qce [ <qce> ] } ]

### *1.9.31.8 (config)# qos wred queue*

**Syntax:** (config)# qos wred queue <queue> min-th <min_th> mdp-1 <mdp_1> mdp-2 <mdp_2> mdp-3 <mdp_3>

**Explanation:** Apply RED on a particular queue or set up the minimum threshold & drop probability value.

**Parameters:**

queue <queue>: Specify the queue number. Queue 0 to 5 can apply to Random Early Detection (RED). However, RED cannot be applied to Queue 6 and 7.

min-th <min_th>: Specify the lowest RED threshold. If the average queue filling level is below this threshold, the drop probability is zero. This valid value for this field is 0~100.

mdp-1 <mdp_1>: Controls the drop probability for the frames marked in drop precedence level 1 when the average queue filling level is 100%. The valid value is 0~100.

mdp-2 <mdp_2>: Controls the drop probability for the frames marked in drop precedence level 2 when the average queue filling level is 100%. The valid value is 0~100.

mdp-3 <mdp_3>: Controls the drop probability for the frames marked in drop precedence level 3 when the average queue filling level is 100%. The valid value is 0~100.

**Negation**: (config)# no qos wred queue <queue>

**Show:** # show qos [ { interface [ ( <port_type> [ <port> ] ) ] } **|** wred **|** { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } **|** storm **|** { qce [ <qce> ] } ]

### *1.9.31.9 (config-if)# qos dscp-classify*

**Syntax:** (config-if)# qos dscp-classify { zero **|** selected **|** any }

**Explanation:** Configure a classification method.

**Parameters:**

{ zero **|** selected **|** any }: Specify a classification method.

**zero:** Classify if incoming DSCP is 0.

**selected:** Classify only selected DSCP for which classification is enabled in DSCP Translation table

**any:** Classify all DSCP.

**Negation**: (config-if)# no qos dscp-classify

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } **|** wred **|** { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } **|** storm **|** { qce [ <qce> ] } ]

### *1.9.31.10 (config-if)# qos dscp-remark*

**Syntax:** (config-if)# qos dscp-remark { rewrite **|** remap **|** remap-dp }

**Explanation:** Configure port egress rewriting of DSCP values.

**Parameters:**

{ rewrite **|** remap **|** remap-dp }: Specify an option.

**rewrite:** Rewrite DSCP field with classified DSCP value.

**remap:** Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. Depending on the frame's DP level, the remapped DSCP value is either taken from the DSCP Translation table, Egress Remap DP0 or DP1 field.

**remap-dp:** Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. The remapped DSCP value is always taken from the DSCP Translation table, Egress Remap DP0 field.

**Negation**: (config-if)# no qos dscp-remark

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } **|** wred **|** { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } **|** storm **|** { qce [ <qce> ] } ]

### *1.9.31.11 (config-if)# qos dscp-translate*

**Syntax:** (config-if)# qos dscp-translate

**Explanation:** Configure DSCP ingress translation of QoS for specific interface.

**Negation**: (config-if)# no qos dscp-translate

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.12 (config-if)# qos map cos-tag*

**Syntax:** (config-if)# qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei>

**Explanation:** Configure (QoS class, DP level) to (PCP, DEI) Mapping of QoS for specific interface.

**Parameters:**

cos <cos: 0-7>: Specify a QoS class value.

dpl <dpl:0-1>: Specify a DPL value (0 or 1).

pcp <pcp: 0-7>: Specify a PCP (Priority Code Point) value.

dei <dei: 0-1>: Specify a DEI value (0 or 1).

**Negation**: (config-if)# no qos map cos-tag cos <cos> dpl <dpl>

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.13 (config-if)# qos ingress queue-shaper*

**Syntax:** (config-if)# qos egress queue-shaper queue <queue> <rate> [ excess ]

**Explanation:** Configure Egress Queue shaper Rate of QoS for specific interface.

**Parameters:**

<queue: 0-7>: Specify a queue or a range.

<rate: 100-13200000>: Specify shaper rate in kbps.

[ excess ]: Allow all excess bandwidth.

**Negation**: (config-if)# no qos egress queue-shaper queue <queue>

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.14 (config-if)# qos egress shaper*

**Syntax:** (config-if)# qos egress shaper <rate>

**Explanation:** Configure Egress Queue Policers Rate of QoS for specific interface.

**Parameters:**

<rate: 100-13200000>: Specify shaper rate in kbps.

**Negation**: (config-if)# no qos egress shaper

**Show:** # show qos
# show qos [{ interface [( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.15 (config-if)# qos egress tag-remark*

**Syntax:** (config-if)# qos egress tag-remark { pcp <pcp> dei <dei> | mapped }

**Explanation:** Configure the appropriate egress remarking mode used by this port.

**Parameters:**

{ pcp <pcp> dei <dei> | mapped }: Specify a remarking mode.

**pcp <pcp> dei <dei>:** Specify PCP and DEI value.

**mapped:** Use the mapping of the classified QoS class values and DP levels to PCP/DEI values.

**Negation**: (config-if)# no qos egress tag-remark

**Show:** # show qos
# show qos [{ interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.16 (config-if)# qos egress wrr*

**Syntax:** (config-if)# qos egress wrr <w0> <w1> <w2> <w3> <w4> <w5>

**Explanation:** Assign egress weight for QoS queueing method. WRR stands for Weighted Round Robin and uses default queue weights. The number of packets serviced during each visit to a queue depends on the percentages you configure for the queues.

**Parameters:**

<w0: 1-100>: Specify weight for queue 0.

<w1: 1-100>: Specify weight for queue 1.

<w2: 1-100>: Specify weight for queue 2.

<w3: 1-100>: Specify weight for queue 3.

<w4: 1-100>: Specify weight for queue 4.

<w5: 1-100>: Specify weight for queue 5.

**Negation**: (config-if)# no qos egress wrr

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.17 (config-if)# qos ingress cos*

**Syntax:** (config-if)# qos ingress cos <cos>

**Explanation:** Configure CoS value on this selecte infterface.

**Parameters:**

<cos>: Specify COS value (1-7).

**Negation**: (config-if)# no qos ingress cos

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.18 (config-if)# qos ingress dei*

**Syntax:** (config-if)# qos ingress dei <dei>

**Explanation:** Configure DEI (Drop Eligible Indicator) value on this selecte infterface.

**Parameters:**

<dei>: Specify DEI for untagged frames.

**Negation**: (config-if)# no qos ingress dei

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.19 (config-if)# qos ingress dpl*

**Syntax:** (config-if)# qos ingress dpl <dpl>

**Explanation:** Configure DPL value on this selecte infterface.

**Parameters:**

<dpl>: Specify the default Drop Precedence Level

**Negation**: (config-if)# no qos ingress dpl

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.20 (config-if)# qos ingress map tag-cos*

**Syntax:** (config-if)# qos ingress map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl>

**Explanation:** Configure (QoS class, DP level) to (PCP, DEI) Mapping of QoS for specific interface.

**Parameters:**

pcp <pcp: 0-7>: Specify a PCP (Priority Code Point) value.

dei <dei: 0-1>: Specify a DEI value (0 or 1).

cos <cos: 0-7>: Specify a QoS class value.

dpl <dpl:0-1>: Specify a DPL value (0 or 1).

**Negation**: (config-if)# no qos ingress map tag-cos pcp <pcp> dei <dei>

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.21 (config-if)# qos ingress pcp*

**Syntax:** (config-if)# qos ingress pcp <pcp>

**Explanation:** Configure PCP value for specific interface.

**Parameters:**

pcp <pcp: 0-7>: Specify a PCP (Priority Code Point) value.

**Negation**: (config-if)# no qos ingress pcp

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.22 (config-if)# qos policer*

**Syntax:** (config-if)# qos policer <rate> [ fps ] [ flowcontrol ]

**Explanation:** Configure PCP value for specific interface.

**Parameters:**

<rate>: Indicate the rate for the policer. By default, 500kbps is used. The allowed range for kbps and fps is 100 to 1000000. The allowed range for Mbps and kfps is 1 to 3300Mbps.

[ fps ]: Rate is fps. By default, kbps is used.

[ flowcontrol ]: Enable Flow Control. If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames

**Negation**: (config-if)# no qos ingress policer

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.23 (config-if)# qos ingress queue-policer*

**Syntax:** (config-if)# qos ingress queue-policer queue <queue> <rate>

**Explanation:** Configure Egress Queue shaper Rate of QoS for specific interface.

**Parameters:**

<queue: 0-7>: Specify a queue or a range.

<rate: 100-13200000>: Specify shaper rate in kbps.

**Negation**: (config-if)# no qos ingress queue-policer queue <queue>

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.24 (config-if)# qos ingress shaper*

**Syntax:** (config-if)# qos ingress shaper <rate> [ burst <has_burst_size> ]

**Explanation:** Configure ingress shaper rate of QoS for specific interface.

**Parameters:**

<rate: 100-13200000>: Specify shaper rate in kbps.

[ burst <has_burst_size> ]: Specify the burst size. The allowed range is 0-252Kbytes. By default, the burst size is 4Kbytes.

**Negation**: (config-if)# no qos ingress shaper

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.25 (config-if)# qos ingress trust dscp*

**Syntax:** (config-if)# qos ingress trust dscp

**Explanation:** Enable DSCP Classification of QoS for specific interface.

**Negation**: (config-if)# no qos ingress trust dscp

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.26 (config-if)# qos ingress trust tag*

**Syntax:** (config-if)# qos ingress trust tag

**Explanation:** Enable VLAN tag Classification of QoS for specific interface.

**Negation**: (config-if)# no qos ingress trust tag

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### *1.9.31.27 (config-if)# qos storm*

**Syntax:** (config-if)# qos storm { unicast | broadcast | unknown } <rate> [ fps ]

**Explanation:** Configure broadcast storm control rate for QoS on the selected ports.

**Parameters:**

{ unicast | multicast | broadcast }: Specify the storm type that you want to configure.

{ { <rate> [ kfps ] } | { 1024 kfps } }: User-define storm frame rate or set storm rate to 1024 kfps.

**Example:** The following example sets broadcast storm control for QoS to 1024 kfps.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# qos storm broadcast 1024 kfps
```

**Negation**: (config-if)# no qos storm { unicast | multicast | broadcast }

**Show:** # show qos storm

### 1.9.32 (config)# radius-server

#### 1.9.32.1 (config)# radius-server attribute 32

**Syntax:** (config)# radius-server attribute 32 <id>

**Explanation:** Configure Radius attribute 32 string.

**Parameters:**

<id>: Specify Radius server identifier. The allowed characters are 1 to 253.

```
# config t
(config)# radius-server attribute 32 cabinet5aSW
```

**Negation:** (config)# no radius-server attribute 32

**Show:** # show radius-server [statistics]

#### 1.9.32.2 (config)# radius-server attribute4

**Syntax:** (config)# radius-server attribute 4 <ipv4>

**Explanation:** Configure NAS IPv4 address.

**Parameters:**

<ipv4>: Specify NAS IPv4 address.

**Example:** Set NAS IPv4 address to 100.1.1.25.

```
# config t
(config)# radius-server attribute 4 100.1.1.25
```

**Negation:** (config)# no radius-server attribute 4

**Show:** # show radius-server [statistics]

#### 1.9.32.3 (config)# radius-server attribute 95

**Syntax:** (config)# radius-server attribute 95 <ipv6>

**Explanation:** Configure NAS IPv6 address.

**Parameters:**

<ipv6>: Specify NAS IPv6 address.

**Negation:** (config)# no radius-server attribute 95

**Show:** # show radius-server [statistics]

### *1.9.32.4 (config)# radius-server deadtime*

**Syntax:** (config)# radius-server deadtime <minutes>

**Explanation:** Configure RADIUS server deadtime value. Deadtime 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.

**Parameters:**

<deadtime>: Specify RADIUS server deadtime value. The valid range is 1 to 1440 (minutes).

**Example:** Set RADIUS server to 60.

```
# config t
(config)# radius-server deadtime 60
```

**Negation:** (config)# no radius-server deadtime

**Show:** # show radius-server [statistics]

### *1.9.32.5 (config)# radius-server host*

**Syntax:** (config)# radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port <acct_port> ] [ timeout <seconds> ] [ retransmit <retries> ] [ key <key> ]

**Explanation:** This command is used to configure Radius server.

**Parameters:**

<host_name>: Specify the hostname or IP address for the radius server. The allowed characters are 1 to 255.

[ auth-port <auth_port> ]: Specify the UDP port to be used on the RADIUS server for authentication.

[ acct-port <acct_port> ]: Specify the UDP port to be used on the RADIUS server for accounting.

[timeout <seconds>]: Specify a timeout value. If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

[retransmit <retries>]: Specify a value for retransmit retry. If retransmit value is specified here, it will replace the global retransmit value. If you prefer to use the global value, leave this field blank.

[key <key>]: Specify a secret key. If secret key is specified here, it will replace the global secret key. If you prefer to use the global value, leave this field blank.

**Negation:** (config)# no radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port <acct_port> ]

**Show:** # show radius-server [statistics]

### *1.9.32.6 (config)# radius-server key*

**Syntax:** (config)# radius-server key <key>

**Explanation:** Configure RADIUS server key value. This key is shared between the RADIUS sever and the switch.

**Parameters:**

<key>: Specify RADIUS server secret key value. The valid range is 1 to 63.

**Example:** Set RADIUS server secret key to 803321

```
# config t
(config)# radius-server key 803321
```

**Negation:** (config)# no radius-server key

### *1.9.32.7 (config)# radius-server retransmit*

**Syntax:** (config)# radius-server retransmit <retries>

**Explanation:** Configure the number of times to retransmit request packets to an authentication server that does not respond. If the server does not respond after the last retransmit is sent, the switch considers the authentication server is dead.

**Parameters:**

<retries>: Specify RADIUS server retransmit value. The valid range is 1 to 1000.

**Example:** Set RADIUS server retransmit value to 5

```
# config t
(config)# radius-server retransmit 5
```

**Negation:** (config)# no radius-server retransmit

**Show:** # show radius-server [statistics]

### *1.9.32.8 (config)# radius-server timeout*

**Syntax:** (config)# radius-server timeout <seconds>

**Explanation:** Configure the time the switch waits for a reply from an authentication server before it retransmits the request.

**Parameters:**

<seconds>: Specify RADIUS server timeout value. The valid range is 1 to 1000.

**Example:** Set RADIUS server timeout to 60

```
# config t
(config)# radius-server timeout 60
```

**Negation:** (config)# no radius-server timeout

**Show:** # show radius-server [statistics]

### *1.9.33 (config)# ring*

#### *1.9.33.1 (config)# ring <instance>chain*

**Syntax:** (config)# ring <instance> chain [ master ] east interface <port_type> <east_port> [ edge ] west interface <port_type> <west_port> [ edge ]

**Parameters:**

<instance: 0-5>: Specify the ring instance number.

chain: This is a chain ring.

[ master ]: Set this ring to master ring.

east interface <port_type> <east_port> [ edge ]: Specify the east port type (Fast Ethernet or Gigabit Ethernet) and port number. If this port is the edge port, add “edge” after the port number.

west interface <port_type> <west_port> [ edge ]: Specify the west port type (Fast Ethernet or Gigabit Ethernet) and port number. If this port is the edge port, add “edge” after the port number.

**Explanation:** Create a chain ring instance.

**Example:** Create a chain instance 1.

```
# config t
(config)# ring 1 chain east interface GigabitEthernet 1/1 west interface
GigabitEthernet 1/2
```

**Negation:** (config)# no ring <instance>

**Show:** # show ring [ <instances> ]

#### *1.9.33.2 (config)# ring <instance>ring*

**Syntax:** (config)# ring <instance> ring [ master ] east interface <port_type> <east_port> west interface <port_type> <west_port>

**Parameters:**

<instance: 0-5>: Specify the ring instance number.

ring: This is a closed ring type.

[ master ]: Set this ring to master ring.

east interface <port_type> <east_port>: Specify the east port type (Fast Ethernet or Gigabit Ethernet) and port number.

west interface <port_type> <west_port>: Specify the west port type (Fast Ethernet or Gigabit Ethernet) and port number.

**Explanation:** Create a closed ring instance.

**Example:** Create a ring instance 2.

```
# config t
(config)# ring 2 ring east interface GigabitEthernet 1/3 west interface
GigabitEthernet 1/4
```

**Negation:** (config)# no ring <instance>

**Show:** # show ring [ <instances> ]

#### *1.9.33.3 (config)# ring <instance> sub*

**Syntax:** (config)# ring <instance> sub [ master ] east interface <port_type> <east_port>

**Parameters:**

<instance: 0-5>: Specify the ring instance number.

sub: This is a sub-ring type.

[ master ]: Set this ring to master ring.

east interface <port_type> <east_port>: Specify the east port type (Fast Ethernet or Gigabit Ethernet) and port number.

**Explanation:** Create a sub ring instance.

**Example:** Create a ring instance 3.

```
# config t
(config)# ring 3 ring east interface GigabitEthernet 1/1
```

**Negation:** (config)# no ring <instance>

**Show:** # show ring [ <instances> ]

### *1.9.34 (config)# rmon*

#### *1.9.34.1 (config)# rmon alarm*

**Syntax:** (config)# rmon alarm <id> <oid_str> <interval> { absolute | delta } rising-threshold <rising_threshold> [ <rising_event_id> ] falling-threshold <falling_threshold> [ <falling_event_id> ] { [ rising | falling | both ] }

**Syntax:** (config)# rmon alarm <id> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors } <ifIndex> <interval> { absolute | delta } rising-threshold <rising_threshold> [ <rising_event_id> ] falling-threshold <falling_threshold> [ <falling_event_id> ] { [ rising | falling | both ] }

**Explanation:** Configure RMON alarm settings. RMON Alarm configuration defines specific criteria that will generate response events. It can be set to test data over any specified time interval and can monitor absolute or changing values. Alarms can also be set to respond to rising or falling thresholds.

**Parameters:**

<id>: Indicates the index of the entry. The range is from 1 to 65535.

<oid_str>: The object number of the MIB variable to be sampled. Only variables of the type ifEntry.n.n may be sampled. Possible variables are ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifOutDiscards, ifErrors, ifInUnknownProtos, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, ifOutDiscards, ifOutErrors.

<interval>: The polling interval for sampling and comparing the rising and falling threshold. The range is from 1to 2^31 (2147483647) seconds.

{ absolute | delta }: Test for absolute or relative change in the specified variable.

**Absolute:** The variable is compared to the thresholds at the end of the sampling period.

**Delta:** The last sample is subtracted from the current value and the difference is compared to the thresholds.

rising-threshold <rising_threshold>: If the current value is greater than the rising threshold and the last sample value is less than this threshold, then an alarm will be triggered. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. The threshold range is -2147483647 to 2147483647.

[ <rising_event_id> ]: Indicates the rising index of an event. The range is 1 - 65535.

falling-threshold <falling_threshold>: If the current value is less than the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold. (Range: -2147483647 to 2147483647)

[ <falling_event_id> ]: Indicates the falling index of an event. The range is 0 - 65535.

{ [ rising | falling | both ] }: Specify a method that is used to sample the selected variable and calculate the value to be compared against the thresholds.

**rising:** Trigger alarm when the first value is larger than the rising threshold.

**falling:** Trigger alarm when the first value is less than the falling threshold.

**both:** Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold.

**Negation:** (config)# no rmon alarm <id>

**Show:** # show rmon alarm [ <id_list> ]
# show rmon history [ <id_list> ]
# show rmon statistics [ <id_list> ]

#### *1.9.34.2 (config)# rmon event*

**Syntax:** (config)# rmon event <id> [ log ] [ trap <community> ] { [ description <description> ] }

**Explanation:** Configure RMON Event settings.

**Parameters:**

<id>: Specify an ID index. The range is 1 - 65535.

[ log ]: When the event is triggered, a RMON log entry will be generated.

[trap<community>]: A password-like community string sent with the trap. Although the community string can be set on this configuration page, it is recommended that it be defined on the SNMP trap configuration page prior to configuring it here. The allowed characters are 0 - 127.

{ [ description <description> ] }: Enter a descriptive comment for this entry.

**Negation:** (config)# no rmon event <id>

**Show:** # show rmon alarm [<id_list>]
# show rmon history [<id_list>]

### *1.9.35 (config-if)# shutdown*

**Syntax:** (config-if)# shutdown

**Explanation:** Shutdown this specific interface.

**Negation:** (config-if)# no shutdown

**Show:** # show interface ( <port_type> [ <v_port_type_list> ] ) status

### *1.9.36 (config)# snmp-server*

#### *1.9.36.1 (config)# snmp-server*

**Syntax:** (config)# snmp-server

**Explanation:** Enable SNMP server service.

**Example:** Enable SNMP server service.

```
# config t
(config)# snmp-server
```

**Negation:** (config)# no snmp-server

**Show:** # show snmp

#### *1.9.36.2 (config)# snmp-server access*

**Syntax:** (configt)# snmp-server access <group_name> model { v1 **|** v2c **|** v3 **|** any } level { auth **|** noauth **|** priv } [ read <view_name> ] [ write <write_name> ]

**Explanation:** Configure SNMP access settings.

**Parameters:**

<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 0x21 to 0x7E.

model{v1**|**v2c**|**v3**|**any}: Indicates the security model that this entry should belong to. Possible security models are:

**any:** Any security model accepted(v1|v2c|usm).

**v1 :** Reserved for SNMPv1.

**v2c:** Reserved for SNMPv2c.

**v3 :** User-based Security Model (USM) for SNMPv3.

level{auth**|**noauth**|**priv}: Indicates the security level that this entry should belong to. Possible security models are:

**auth:** Authentication and no privacy.

**noauth:** No authentication and no privacy.

**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 0x21 to 0x7E.

[ write <write_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 0x21 to 0x7E.

**Negation:** (config)# no snmp-server access <group_name> model { v1 **|** v2c **|** v3 **|** any } level { auth **|** noauth **|** priv }

**Show:** # show snmp access [ <group_name> { v1 **|** v2c **|** v3 **|** any } { auth **|** noauth **|** priv } ]

### *1.9.36.3 (config)# snmp-server community v2c*

**Syntax:** (config)# snmp-server community v2c <comm> [ ro **|** rw ]

**Explanation:** Configure Read or Write community string.

**Parameters:**

<comm >: Indicate a community read or write access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E.

[ro**|**rw]: Indicates whether the specified community applies to read only access string or read & write access string.

**Example:** Set Write community access string to private123.

```
# config t
(config)# snmp-server community v2c private124 rw
```

**Negation:** (config)# no snmp-server community v2c

**Show:** # show snmp

### *1.9.36.4 (config)# snmp-server community v3*

**Syntax:** (config)# snmp-server community v3 <v3_comm> [ <v_ipv4_addr> <v_ipv4_netmask> ]

**Explanation:** Configure SNMP server community v3 value.

**Parameters:**

<v3_comm>: Specify SNMPv3 community string.

[ <v_ipv4_addr> <v_ipv4_netmask> ]: Specify IPv4 address and subnet mask address.

**Negation:** (config)# no snmp-server community v3 <word127>

**Show:** # show snmp
# show snmp community v3

### *1.9.36.5 (config)# snmp-server contact*

**Syntax:** (config)# snmp-server contact <v_line255>

**Explanation:** Configure system contact information.

**Parameters:**

<v_line255>: Specify system contact information. This could be a person's name, email address or other descriptions. The allowed string length is 0 – 255 and the allowed content is the ASCII characters from 32 – 126.

**Example:** Set system contact information to "admin@acme.com"

```
# config t
(config)# snmp-server contact admin@acme.com
```

**Negation:** (config)# no snmp-server contact

### *1.9.36.6 (config)# snmp-server engine-id local*

**Syntax:** (config)# snmp-server engine-id local <engineID>

**Explanation:** Configure SNMP server v3 Engine ID value.

**Parameters:**

<engineID>: 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. Changes to the Engine ID will clear all original local users.

**Negation:** (config)# no snmp-server engined-id local

**Show:** # show snmp

### *1.9.36.7 (config)# snmp-server host*

**Syntax:** (config)# snmp-server host <conf_name>

**Explanation:** Configure SNMP server hostname.

**Parameters:**

<conf_name: word 32>**:** Specify a host name. Once "Enter" is pressed, the CLI prompt changes to (config-snmps-host)#.

**Example:** Set SNMP server hostname to RemoteSnmp

```
# config t
(config)# snmp-server host RemoteSnmp
```

**Negation:** (config)# snmp-server host <conf_name>

**Show:** # show snmp host [ <conf_name> ] [ system ] [ switch ] [ power ] [ interface ] [ aaa ]

### *1.9.36.8 (config)# snmp-server location*

**Syntax:** (config)# snmp-server location <v_line255>

**Parameters:**

<v_line255>: Specify the descriptive location of this device. The allowed string length is 0 – 255.

**Example:** Set the location to "Cabinet A22"

```
# config t
(config)# snmp-server location Cabinet A22
```

**Negation:** (config)# no snmp-server location

### *1.9.36.9 (config)# snmp-server security-to-group model*

**Syntax:** (configt)# snmp-server security-to-group model {v1 **|** v2c **|** v3} name <security_name> group <group_name>

**Explanation:** Configure SNMPv3 Group settings.

**Parameters:**

{ v1 **|** v2c **|** v3 }: Indicates the security model that this entry should belong to.

<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 0x21 to 0x7E.

<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 0x21 to 0x7E.

**Negation:** (config)# no snmp-server security-to-group model { v1 **|** v2c **|** v3 } name <security_name>

**Show:** # show snmp security-to-group [ { v1 **|** v2c **|** v3 } <security_name> ]

### *1.9.36.10 (config)# snmp-server trap*

**Syntax:** (config)# snmp-server trap

**Explanation:** Enable SNMP server trap function.

**Example:** Enable SNMP server trap function.

```
# config t
(config)# snmp-server trap
```

**Negation:** (config)# no snmp-server trap

**Show:** # show snmp

### *1.9.36.11 (config)# snmp-server user*

**Syntax:** (configt)# snmp-server user <username> engine-id <engineID> [ { md5 <md5_passwd> | sha <sha_passwd> } [ priv { des **|** aes } <priv_passwd> ] ]

**Explanation:** Configure SNMPv3 User settings.

**Parameters:**

<username: word 32>: 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 0x21 to 0x7E.

engine-id <engineID>: 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 is a remote user.

{ md5 <md5_passwd> | sha <sha_passwd> }: Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

**md5 <md5_passwd>:** An optional flag to indicate that this user uses MD5 authentication protocol. A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32 characters. For SHA authentication protocol, the allowed string length is 8 to 40 characters. The allowed content is ASCII characters from 0x21 to 0x7E.

**sha <sha_passwd>:** An optional flag to indicate that this user uses SHA authentication protocol. A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32 characters. For SHA authentication protocol, the allowed string length is 8 to 40 characters. The allowed content is ASCII characters from 0x21 to 0x7E.

[priv{des **|** aes}<priv_passwd>]]: Indicates the privacy protocol that this entry should belong to. Possible

privacy protocols are:

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

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

**<priv_passwd>:** A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

**Negation:** (config)# no snmp-server user <username> engine-id <engineID>

**Show:** #show snmp user [ <username> <engineID> ]

### *1.9.36.12 (config)# snmp-server version*

**Syntax:** (config)# snmp-server version { v1 **|** v2c **|** v3 }

**Explanation:** Configure SNMP server version.

**Parameters:**

{ v1 **|** v2c **|** v3 }: Specify which SNMP server version you want to use.

**Example:** Set SNMP server version to v3.

```
# config t
(config)# snmp-server version v3
```

**Negation:** (config)# no snmp-server version

**Show:** # show snmp

### *1.9.36.13 (config)# snmp-server view*

**Syntax:** (configt)# snmp-server view <view_name> <oid_subtree> { include **|** exclude }

**Explanation:** Configure SNMPv3 MIB view name.

**Parameters:**

<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 0x21 to 0x7E.

<oid_subtree>: The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128.

{ include **|** exclude }: Indicates the view type that this entry should belong to. Possible view types are:

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

**excluded:** An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.

**Negation:** (config)# no snmp-server view <view_name> <oid_subtree>

**Show:** # show snmp view [ <view_name> <oid_subtree> ]

#### *1.9.36.14 (config-if)# snmp-server host <conf_name> traps*

**Syntax:** (config-if)# snmp-server host <conf_name> traps [ linkup ] [ linkdown ] [ lldp ]

**Explanation:** Configure SNMP trap events for the selected interface.

**Parameters:**

<conf_name: word 32>: Specify the name of the trap.

traps [ linkup ] [ linkdown ] [ lldp ]: Enable the selected interfaces' trap events.

**[ linkup ]:** Port link up trap.

**[ linkdown ]:** Port link down trap.

**[ lldp ]:** LLDP (Link Layer Discovery Protocol) trap.

**Negation:** (config-if)# no snmp-server host <conf_name> traps

#### *1.9.36.15 (config-snmps-host)# alarm*

**Syntax:** (config-snmps-host)# alarm [ power [ power1 ] [ power2 ] ]

**Explanation:** Configure power alarms for this host.

**Parameters:**

[ power [ power1 ] [ power2 ] ]: Initiate power alarms when Power 1 or Power 2 fails.

#### *1.9.36.16 (config-snmps-host)# host <v_ipv6_ucast>*

**Syntax:** (config-snmps-host)# host <v_ipv6_ucast> [ <udp_port> ] [ traps **|** informs ]

**Explanation:** Indicates the SNMP trap destination address.

**Parameters:**

<v_ipv6_ucast>: Specify the IPv6 address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). Also allowed is a valid hostname. A valid hostname is a string drawn from the alphabet (A-Z; a-z), digits (0-9), dot (.) and dash (-). Spaces are not allowed. The first character must be an alpha character, and the first and last characters cannot be a dot or a dash.

[ <udp_port> ]: Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. The default SNMP trap port is 162.

[ traps **|** informs ]: Specify one of the options.

**Negation:** (config-snmps-host)# no host

### *1.9.36.17 (config-snmps-host)# host <v_ipv4_ucast>*

**Syntax:** (config-snmps-host)# host { <v_ipv4_ucast> **|** <v_word45> } [ <udp_port> ] [ traps **|** informs ]

**Explanation:** Configure the SNMP trap destination IPv4 address.

**Parameters:**

{<v_ipv4_ucast> **|** <v_word45>}: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). Also allowed is a valid hostname. A valid hostname is a string drawn from the alphabet (A-Z; a-z), digits (0-9), dot (.) and dash (-). Spaces are not allowed. The first character must be an alpha character, and the first and last characters cannot be a dot or a dash.

[ <udp_port> ]: Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. The default SNMP trap port is 162.

[ traps **|** informs ]: Specify one of the options.

**Negation:** (config-snmps-host)# no host

### *1.9.36.18 (config-snmps-host)# version*

**Syntax:** (config-snmps-host)# version { v1 [ <v1_comm> ] **|** v2 [ <v2_comm> ] **|** v3 [ probe **|** engineID <v_word10_to_32> ] [ <securtyname> ] }

**Parameters:**

{v1[<v1_comm>]|v2[<v2_comm>]|v3[probe|engineID <v_word10_to_32>][<securtyname>]}: Specify one of the SNMP versions.

**v1[v1_comm]:** Support SNMPv1 and trap community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 0x21 to 0x7E.

**v2[v2_comm]:** Support SNMPv2c and trap community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 0x21 to 0x7E.

**v3 [ probe | engineID <v_word10_to_32> ] [ <securtyname> ]:** Support SNMPv3.

**[ probe | engineID <v_word10_to_32> ]:** Indicates the SNMP trap probe security engine ID or SNMP trap security engine ID. SNMPv3 sends traps and informs use 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.

**[ <securtyname> ]:** Indicates the SNMP trap security name. SNMPv3 traps and informs use USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

**Explanation:** Configure SNMP version and its corresponding values.

**Example:** Support SNMPv2c version.

```
# config t
(config-snmps-host)# version v2 public
```

**Negation:** (config-snmps-host)# no version

#### *1.9.36.19 (config-snmps-host)# informs retries*

**Syntax:** (config-snmps-host)# informs retries <retries> timeout <timeout>

**Explanation:** Configure SNMP trap retry times and timeout.

**Parameters:**

<retries>: Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

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

**Negation:** (config-snmps-host)# no informs

#### *1.9.36.20 (config-snmps-host)# shutdown*

**Syntax:** (config-snmps-host)# shutdown

**Parameters:** None.

**Explanation:** Disable the SNMP trap mode.

**Example:** Disable the SNMP trap mode.

```
# config t
(config-snmps-host)# shutdown
```

**Negation:** (config-snmps-host)# no shutdown

#### *1.9.36.21 (config-snmps-host)# traps*

**Syntax:** (config-snmps-host)# traps [ aaa authentication ] [ system [ coldstart ] [ warmstart ] ] [ switch [ stp ] [ rmon ] ]

**Explanation:** Configure SNMP trap events.

**Parameters:**

[ aaa authentication ]: Authentication, Authorization and Accounting. A trap will be issued at any authentication failure.

[ system [ coldstart ] [ warmstart ] ]: The system trap events include the following.

**coldstart:** The switch has booted from a powered off or due to power cycling (power failure).

**warmstart:** The switch has been rebooted from an already powered on state.

[switch [stp] [rmon]]: Indicates that the Switch group's traps. Possible traps are:

**stp:** Enable STP trap.

**rmon:** Enable RMON trap.

**Example:** Send a trap notice when any authentication fails.

```
# config t
(config-snmps-host)# traps aaa authentication
```

**Negation:** (config-snmps-host)# no traps

**Show:** # show snmp host [ <conf_name> ] [ system ] [ switch ] [ interface ] [ aaa ]

## *1.9.36(config)# spanning-tree*

### *1.9.36.1 (config)# spanning-tree aggregation*

**Syntax:** (config)# spanning-tree aggregation

**Explanation:** Enable aggregation mode of Spanning Tree.

```
# config t
(config)# spanning-tree aggregation
(config-stp-aggr)#
```

**Show:** # show spanning-tree

### *1.9.36.2 (config-stp-aggr)# spanning-tree*

**Syntax:** (config-stp-aggr)# spanning-tree

**Explanation:** Enable Spanning Tree under aggregation mode.

**Negation:** (config-stp-aggr)# no spanning-tree

**Show:** # show spanning-tree

### *1.9.36.3 (config-stp-aggr)# spanning-tree auto-edge*

**Syntax:** (config-stp-aggr)# spanning-tree auto-edge

**Explanation:** Enable auto edge function. When enabled, a port is automatically determined to be at the edge of the network when it receives no BPDUs.

**Negation:** (config-stp-aggr)# no spanning-tree auto-edge

**Show:** # show spanning-tree

#### *1.9.36.4 (config-stp-aggr)# spanning-tree bpdu-guard*

**Syntax:** (config-stp-aggr)# spanning-tree bpdu-guard

**Explanation:** Enable BPDU guard function. This feature protects ports from receiving BPDUs. It can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state. If enabled, the port will disable itself upon receiving valid BPDU's.

**Negation:** (config-stp-aggr)# no spanning-tree bpdu-guard

**Show:** # show spanning-tree

#### *1.9.36.5 (config-stp-aggr)# spanning-tree edge*

**Syntax:** (config-stp-aggr)# spanning-tree edge

**Explanation:** If an interface is attached to end nodes, you can set it to “Edge”.

**Negation:** (config-stp-aggr)# no spanning-tree edge

**Show:** # show spanning-tree

#### *1.9.36.6 (config-stp-aggr)# spanning-tree link-type*

**Syntax:** (config-stp-aggr)# spanning-tree link-type { point-to-point **|** shared **|** auto }

**Explanation:** Configure the link type attached to an interface.

**Parameters:**

{ point-to-point **|** shared **|** auto }: Select the link type attached to an interface.

**point-to-point:** It is a point-to-point connection.

**shared:** It is a shared medium connection

**auto:** The switch automatically determines whether the interface is attached to a point-to-point link or shared medium.

**Negation:** (config-stp-aggr)# no spanning-tree link-type

**Show:** # show spanning-tree

### *1.9.36.7 (config-stp-aggr)# spanning-tree mst <instance> cost*

**Syntax:** (config-stp-aggr)# spanning-tree mst <instance> cost { <cost> **|** auto }

**Explanation:** Configure MSTI and its' path cost value.

**Parameters:**

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1-15.

cost { <cost> **|** auto }: Specify a Path cost value that is used to determine the best path between devices. Valid values are 1 to 200000000. If "auto" mode is specified, the system automatically detects the speed and duplex mode to decide the path cost. Please note that path cost takes precedence over port priority.

**Negation:** (config-stp-aggr)# no spanning-tree mst <instance> cost

**Show:** # show spanning-tree

### *1.9.36.8 (config-stp-aggr)# spanning-tree mst <instance> port-priority*

**Syntax:** (config-stp-aggr)# spanning-tree mst <instance> port-priority <prio>

**Explanation:** Configure MSTI and its' port priority.

**Parameters:**

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1-15.

port-priority <prio>: Specify a port priority value.

**Negation:** (config-stp-aggr)# no spanning-tree mst <instance> port-priority

**Show:** # show spanning-tree

### *1.9.36.9 (config-stp-aggr)# spanning-tree restricted-role*

**Syntax:** (config-stp-aggr)# spanning-tree restricted-role

**Explanation:** Enable restricted role function. If enabled, this 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.

**Negation:** (config-stp-aggr)# no spanning-tree restricted-role

**Show:** # show spanning-tree

#### *1.9.36.10 (config-stp-aggr)# spanning-tree restricted-tcn*

**Syntax:** (config-stp-aggr)# spanning-tree restricted-tcn

**Explanation:** Enable restricted TCN function. If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports.

**Negation:** (config-stp-aggr)# no spanning-tree restricted-tcn

**Show:** # show spanning-tree

#### *1.9.36.11 (config)# spanning-tree edge bpdu-filter*

**Syntax:** (config)# spanning-tree edge bpdu-filter

**Explanation:** Enable edge BPDU filtering function. The purpose of Port BPDU Filtering is to prevent the switch from sending BPDU frames on ports that are connected to end devices.

**Example:** Enable edge BPDU filtering function.

```
# config t
(config)# spanning-tree edge bpdu-filter
```

**Negation:** (config)# no spanning-tree edge bpdu-filter

**Show:** # show spanning-tree

#### *1.9.36.12 (config)# spanning-tree edge bpdu-guard*

**Syntax:** (config)# spanning-tree edge bpdu-guard

**Explanation:** Enable edge BPDU guard function. Edge ports generally connect directly to PC, file servers or printers. Therefore, edge ports are configured to allow rapid transition. Under normal situations, edge ports should not receive configuration BPDUs. However, if they do, this probably is due to malicious attacks or mis-settings. When edge ports receive configuration BPDUs, they will be automatically set to non-edge ports and start a new spanning tree calculation process.

BPDU Guard is therefore used to prevent the device from suffering malicious attacks. With this function enabled, when edge ports receive configuration BPDUs, STP disables those affected edge ports. After a period of recovery time, those disabled ports are re-activated.

**Example:** Enable edge BPDU guard function.

```
# config t
(config)# spanning-tree edge bpdu-guard
```

**Negation:** (config)# no spanning-tree edge bpdu-guard

**Show:** # show spanning-tree

### 1.9.36.13 (config)# spanning-tree mode

**Syntax:** (config)# spanning-tree mode { stp **|** rstp **|** mstp }

**Parameters:**

{ stp **|** rstp **|** mstp }: Specify one of the STP protocol versions.

**Explanation:** Configure the desired STP protocol version.

**Example:** Set the spanning tree mode to MSTP.

```
# config t
(config)# spanning-tree mode mstp
```

**Negation:** (config)# no spanning-tree mode

**Show:** # show spanning-tree

### 1.9.36.14 (config)# spanning-tree mst <instance> priority <prio>

**Syntax:** (config)# spanning-tree mst <instance> priority <prio>

**Parameters:**

<instance: 0-7>: Specify an instance ID. “0” means CIST. “1-7” means MSTI 1-7.

<prio: 0-61440>: Specify a priority value.

**Explanation:** Specify an appropriate priority for a MSTI instance. Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Note that lower numeric values indicate higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

**Example:** Map MST Instance 1 to priority 61440.

```
# config t
(config)# spanning-tree mst 1 priority 61440
```

**Negation:** (config)# no spanning-tree mst <instance> priority

**Show:** # show spanning-tree

### 1.9.36.15 (config)# spanning-tree mst <instance> vlan <v_vlan_list>

**Syntax:** (config)# spanning-tree mst <instance> vlan <v_vlan_list>

**Parameters:**

<instance: 0-7>: Specify an instance ID. “0” means CIST. “1-7” means MSTI 1-7.

<v_vlan_list>: Specify a list of VLANs for the specified MST instance. Separate VLANs with a comma and use hyphen to denote a range of VLANs. (Example: 2,5,20-40)

**Explanation:** Specify VLANs mapped to a certain MSTI. Both a single VLAN and a range of VLANs are allowed.

**Example:** Map MST Instance 1 to VLAN 90 and VLAN 101-105.

```
# config t
(config)# spanning-tree mst 1 vlan 90,101-105
```

**Negation:** (config)# no spanning-tree mst <instance> vlan

### *1.9.36.16 (config)# spanning-tree mst forward-time*

**Syntax:** (config)# spanning-tree mst forward-time <fwdtime>

**Parameters:**

<fwdtime: 4-30>: Specify forward delay value between 4 and 30 (seconds).

**Explanation:** Fort STP bridges, the Forward Delay is the time spent in each Listening and Learning state before the Forwarding state is entered. This delay occurs when a new bridge comes onto a network.

**Example:** Set the forward delay to 15 seconds.

```
# config t
(config)# spanning-tree mst forward-time 15
```

**Negation:** (config)# no spanning-tree mst forward-time

**Show:** # show spanning-tree

### *1.9.36.17 (config)# spanning-tree mstmax-age*

**Syntax:** (config)# spanning-tree mst max-age <maxage> [ forward-time <fwdtime> ]

**Parameters:**

<maxage: 6-40>: Specify the max age value. The valid range is from 6 to 40.

[ forward-time <fwdtime> ]: Fort STP bridges, the Forward Delay is the time spent in each Listening and Learning state before the Forwarding state is entered. This delay occurs when a new bridge comes onto a network. Valid values are 4-30seconds.

**Explanation:** If another switch in the spanning tree does not send out a hello packet for a period of time, it is considered to be disconnected. Valid values are 6 to 40 seconds, and Max Age values must be smaller than or equal to (Forward Delay-1)*2.

**Example:** Set the max age to 20 seconds.

```
# config t
(config)# spanning-tree mst max-age 20
```

**Negation:** (config)# no spanning-tree mst max-age

**Show:** # show spanning-tree

#### *1.9.36.18 (config)# spanning-tree mst max-hops*

**Syntax:** (config)# spanning-tree mst max-hops <maxhops>

**Parameters:**

<maxhops>: Specify the maximum hop count value. The valid range is from 6 to 40.

**Explanation:** The maximum number of hops allowed for MST region before a BPDU is discarded. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the BPDU is discarded. The default hop count is 20. The allowed range is 6-40.

**Example:** Set the maximum hop count to 20.

```
# config t
(config)# spanning-tree mst max-hops 20
```

**Negation:** (config)# no spanning-tree mst max-hops

**Show:** # show spanning-tree

#### *1.9.36.19 (config)# spanning-treemst name*

**Syntax:** (config)# spanning-tree mst name <name> revision <v_0_to_65535>

**Parameters:**

name <name>: Specify a name for this MSTI. By default, the switch's MAC address is used. The maximum length is 32 characters. In order to share spanning trees for MSTI, bridges must have the same configuration name and revision value.

revision <v_0_to_65535>: Specify a revision number for this MSTI. The allowed range is 0 – 65535.

**Explanation:** Configure a name and revision number for this MSTI.

**Negation:** (config)# no spanning-tree mst name

**Show:** # show spanning-tree

### 1.9.36.20 (config)# spanning-tree recovery interval

**Syntax:** (config)# spanning-tree recovery interval <interval>

**Parameters:**

<interval>: The time that has to pass before a port in the error-disabled state can be enabled. The allowed range is 30 – 86400 (seconds).

**Explanation:** When enabled, a port that is in the error-disabled state can automatically be enabled after a certain time.

**Example:** Set the spanning tree recovery interval to 50.

```
# config t
(config)# spanning-tree recovery interval 50
```

**Negation:** (config)# no spanning-tree recovery interval

**Show:** # show spanning-tree

### 1.9.36.21 (config)# spanning-tree transmit hold-count

**Syntax:** (config)# spanning-tree transmit hold-count <holdcount>

**Parameters:**

<holdcount:1-10>: Specify the transmit hold-count. The allowed transmit hold count is 1 to 10.

**Explanation:** The number of BPDU sent by a bridge port per second. When exceeded, transmission of the next BPDU will be delayed. By default, it is set to 6. The allowed transmit hold count is 1 to 10. Please note that increasing this value might have a significant impact on CPU utilization and decreasing this value might slow down convergence. It is recommended to remain Transmit Hold Count to the default setting.

**Example:** Set the spanning tree transmit hold-count to 6.

```
# config t
(config)# spanning-tree transmit hold-count 6
```

**Negation:** (config)# no spanning-tree transmit hold-count

**Show:** # show spanning-tree

### 1.9.36.22 (config-if)# spanning-tree

**Syntax:** (config-if)# spanning-tree

**Explanation:** Enable Spanning Tree on this interface.

**Negation:** (config-if)# no spanning-tree

**Show:** # show spanning-tree

### *1.9.36.23 (config-if)# spanning-tree auto-edge*

**Syntax:** (config-if)# spanning-tree auto-edge

**Explanation:** Enable auto edge function on this interface. When enabled, a port is automatically determined to be at the edge of the network when it receives no BPDUs.

**Negation:** (config-if)# no spanning-tree auto-edge

**Show:** # show spanning-tree

### *1.9.36.24 (config-if)# spanning-tree bpdu-guard*

**Syntax:** (config-if)# spanning-tree bpdu-guard

**Explanation:** Enable BPDU guard function on this interface. This feature protects ports from receiving BPDUs. It can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state. If enabled, the port will disable itself upon receiving valid BPDU's.

**Negation:** (config-if)# no spanning-tree bpdu-guard

**Show:** # show spanning-tree

### *1.9.36.25 (config-if)# spanning-tree edge*

**Syntax:** (config-if)# spanning-tree edge

**Explanation:** If an interface is attached to end nodes, you can set it to “Edge”.

**Negation:** (config-if)# no spanning-tree edge

**Show:** # show spanning-tree

### *1.9.36.26 (config-if)# spanning-tree link-type*

**Syntax:** (config-if)# spanning-tree link-type { point-to-point **|** shared **|** auto }

**Explanation:** Configure the link type attached to an interface.

**Parameters:**

{ point-to-point **|** shared **|** auto }: Select the link type attached to an interface.

**point-to-point:** It is a point-to-point connection.

**shared:** It is a shared medium connection

**auto:** The switch automatically determines whether the interface is attached to a point-to-point link or shared medium.

**Negation:** (config-if)# no spanning-tree link-type

**Show:** # show spanning-tree

### *1.9.36.27 (config-if)# spanning-tree mst <instance> cost*

**Syntax:** (config-if)# spanning-tree mst <instance> cost { <cost> **|** auto }

**Explanation:** Configure MSTI and its' path cost value.

**Parameters:**

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1-15.

cost { <cost> **|** auto }: Specify a Path cost value that is used to determine the best path between devices. Valid values are 1 to 200000000. If "auto" mode is specified, the system automatically detects the speed and duplex mode to decide the path cost. Please note that path cost takes precedence over port priority.

**Negation:** (config-if)# no spanning-tree mst <instance> cost

**Show:** # show spanning-tree

### *1.9.36.28 (config-if)# spanning-tree mst <instance> port-priority*

**Syntax:** (config-if)# spanning-tree mst <instance> port-priority <prio>

**Explanation:** Configure MSTI and its' port priority.

**Parameters:**

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1-15.

port-priority <prio>: Specify a port priority value.

**Negation:** (config-if)# no spanning-tree mst <instance> port-priority

**Show:** # show spanning-tree

#### *1.9.36.29 (config-if)# spanning-tree restricted-role*

**Syntax:** (config-if)# spanning-tree restricted-role

**Explanation:** Enable restricted role function. If enabled, this 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.

**Negation:** (config-if)# no spanning-tree restricted-role

**Show:** # show spanning-tree

#### *1.9.36.30 (config-if)# spanning-tree restricted-tcn*

**Syntax:** (config-if)# spanning-tree restricted-tcn

**Explanation:** Enable restricted TCN function. If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports.

**Negation:** (config-if)# no spanning-tree restricted-tcn

**Show:** # show spanning-tree

### *1.9.36(config-if)# speed*

**Syntax:** (config-if)# speed { 10g| 1000 **|** 100 **|** 10 **|** twin| auto { [ 10 ] [ 100 ] [ 1000 ] } }

**Explanation:** Configure port speed for this specific interface.

**Negation:** (config-if)# no speed

**Show:** # show interface ( <port_type> [ <v_port_type_list> ] ) status

### *1.9.36(config)# switchport*

#### *1.9.36.1 (config)# switchport vlan mapping*

**Syntax:** (config)# switchport vlan mapping <group ID> <vlan_list> <translation_vlan>

**Explanation:** VLAN Translation is especially useful for users who want to translate the original VLAN ID to a new VLAN ID so as to exchange data across different VLANs and improve VLAN scaling. VLAN translation replaces an incoming C-VLAN tag with an S-VLAN tag instead of adding an additional tag. When configuring VLAN Translation, both ends of the link normally must be able to replace tags appropriately. In other words, both ends must be configured to translate the C-VLAN tag to S-VLAN tag and S-VLAN tag to C-VLAN tag appropriately in a network. Note that only access ports support VLAN translation. It is not recommended to configure VLAN Translation on trunk ports.

**Parameters:**

<group ID: 1-28>: Indicate the Group ID that applies to this translation rule.

<vlan_list>: Indicate the VLAN ID that will be mapped to a new VID.

<translation_vlan>: Indicate the new VID to which VID of ingress frames will be changed.

**Example:** Map the group ID 5 with VLAN ID 100 to be translated to 201.

```
# config t
(config)# switchport vlan mapping 5 100 201
```

**Negation:** (config)# no switchport vlan mapping <group> <v_vlan_id_from>

### *1.9.36.2 (config-if)# switchport access vlan*

**Syntax:** (config-if)# switchport access vlan <pvid>

**Explanation:** Configure access VLAN ID for this interface.

**Parameters:**

<pvid>: Indicate the access VLAN ID (PVID) for this interface.

**Example:** Set the interface 1's access VLAN ID to 10.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# switchport access vlan 10
(config-if)#
```

**Negation:** (config-if)# no switchport access vlan

**Show:** # show vlan status

### *1.9.36.3 (config-if)# switchport forbidden vlan*

**Syntax:** (config-if)# switchport forbidden vlan { add | remove } <vlan_list>

**Explanation:** Add or remove a port from the forbidden VLAN list.

**Parameters:**

{ add | remove }: Add or remove this specific interface from the forbidden VLAN list.

<vlan_list>: Specify the VLAN ID.

**Negation:** (config-if)# no switchport access vlan

**Show:** > show switchport forbidden [{ vlan <vid> } | { name <name> }]
# show switchport forbidden [{ vlan <vid> } | { name <name> }]

### *1.9.36.4 (config-if)# switchport hybrid acceptable-frame-type*

**Syntax:** (config-if)# switchport hybrid acceptable-frame-type { all **|** tagged **|** untagged }

**Explanation:** Configure the accepted frame types. Available options include “all” (accept all frames), “tagged” (accept only tagged frames), “untagged” (accept only untagged frames). This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, frame type is set to All.

**Parameters:**

{all **|** tagged **|** untagged}: Specify the frame type for this interface. Available options include “all” (accept all frames), “tagged” (accept only tagged frames), “untagged” (accept only untagged frames).

**Negation:** (config-if)# no switchport hybrid acceptable-frame-type

**Show:** # show vlan status

### *1.9.36.5 (config-if)# switchport hybrid allowed vlan*

**Syntax:** (config-if)# switchport hybrid allowed vlan { all **|** none **|** [ add **|** remove **|** except ] <vlan_list> }

**Explanation:** Configure allowed VLANs when this interface is in hybrid mode.

**Parameters:**

{ all **|** none **|** [ add **|** remove **|** except ] <vlan_list> }: Specify one of the options.

**all:** All VLANs.

**none:** No VLANs.

**add:** Add VLANs to the current list.

**remove:** Remove VLANs from the current list

**except:** All VLANs except the following specified in <vlan_list>.

**<vlan_list>:** Specify the VLAN list.

**Negation:** (config-if)# no switchport hybrid allowed vlan

**Show:** # show vlan status

### *1.9.36.6 (config-if)# switchport hybridegress-tag*

**Syntax:** (config-if)# switchport hybrid egress-tag { none **|** all [ except-native ] }

**Explanation:** Determines egress tagging of a port.

**Parameters:**

{ none | all [ except-native ] }: Determines egress tagging of a port.

**none:** All VLANs are untagged.

**all:** All VLANs are tagged.

**all [except-native]:** All VLANs except the configured PVID will be tagged.

**Negation:** (config-if)# no switchport hybrid egress-tag

**Show:** # show vlan status

### *1.9.36.7 (config-if)# switchport hybrid ingress-filtering*

**Syntax:** (config-if)# switchport hybrid ingress-filtering

**Explanation:** Enable ingress filtering function on this specific interface. If Ingress Filtering is enabled and the ingress port is not a member of a VLAN, the frame from the ingress port is discarded. By default, ingress filtering is disabled.

**Negation:** (config-if)# no switchport hybrid ingress-filtering

**Show:** # show vlan status

### *1.9.36.8 (config-if)# switchport hybrid native vlan*

**Syntax:** (config-if)# switchport hybrid native vlan <pvid>

**Explanation:** Configures the VLAN identifier in Hybrid mode for the port. The allowed values are from 1 through 4095. The default value is 1.

**Parameters:**

<pvid>: Specify the port VLAN ID for this specific interface.

**Negation:** (config-if)# no switchport hybrid native vlan

**Show:** # show vlan status

### *1.9.36.9 (config-if)# switchport hybrid port-type*

**Syntax:** (config-if)# switchport hybrid port-type { unaware **|** c-port **|** s-port **|** s-custom-port }

**Explanation:** Configures the port type in Hybrid mode for the port.

**Parameters:**

{unaware **|** c-port **|** s-port **|** s-custom-port}: There are four port types available. Each port type's ingress and egress action is described in the following table.

| Action<br>Port Type | Ingress Action | Egress Action |
|---|---|---|
| Unaware | When a tagged frame is received on a port,<br>1. If the tagged frame with TPID=0x8100, it becomes a double-tag frame and is forwarded.<br>2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded. | The TPID of frame transmitted by Unaware port will be set to 0x8100. The final status of the frame after egressing are also affected by egress rule. |
| | When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded. | |
| C-port | When a tagged frame is received on a port,<br>1. If a tagged frame with TIPID=0x8100, it is forwarded.<br>2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded. | The TPID of frame transmitted by C-port will be set to 0x8100. |
| | When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded. | |
| S-port | When a tagged frame is received on a port,<br>1. If a tagged frame with TPID=0x88A8, it is forwarded.<br>2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded. | The TPID of frame transmitted by S-port will be set to 0x88A8 |
| | When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded. | |
| S-custom port | When a tagged frame is received on a port,<br>1. If a tagged frame with TPID=0x88A8, it is forwarded.<br>2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded. | The TIPID of frame transmitted by S-custom-port will be set to an self-customized value, which can be set by the user using the column of Ethertype for Custom S-ports. |
| | When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded. | |

**Negation:** (config-if)# no switchport hybrid port-type

**Show:** # show vlan status

### *1.9.36.10 (config-if)# switchport mode*

**Syntax:** (config-if)# switchport mode { access **|** trunk **|** hybrid }

**Explanation:** Configure VLAN mode for this specific interface.

**Parameters:**

{ access **|** trunk **|** hybrid }: Specify the VLAN mode.

**Negation:** (config-if)# no switchport mode

**Show:** # show vlan status

### *1.9.36.11 (config-if)# switchport trunk allowed vlan*

**Syntax:** (config-if)# switchport trunk allowed vlan { all **|** none **|** [ add **|** remove **|** except ] <vlan_list> }

**Explanation:** Configure allowed VLANs when this interface is in trunk mode.

**Parameters:**

{ all **|** none **|** [ add **|** remove **|** except ] <vlan_list> }: Specify one of the options.

**all:** All VLANs.

**none:** No VLANs.

**add:** Add VLANs to the current list.

**remove:** Remove VLANs from the current list

**except:** All VLANs except the following specified in <vlan_list>.

**<vlan_list>:** Specify the VLAN list.

**Negation:** (config-if)# no switchport trunk allowed vlan

**Show:** # show vlan status

### *1.9.36.12 (config-if)# switchport trunk native vlan*

**Syntax:** (config-if)# switchport trunk native vlan <pvid>

**Explanation:** Configure native VLAN ID in trunk mode for this specific interface.

**Parameters:**

<pvid>: Specify the port VLAN ID for this specific interface.

**Negation:** (config-if)# no switchport trunk native vlan

**Show:** # show running-config

### *1.9.36.13 (config-if)# switchport trunk vlan tag native*

**Syntax:** (config-if)# switchport trunk vlan tag native

**Explanation:** Configure this specific interface to tag native VLAN traffic.

**Negation:** (config-if)# no switchport trunk vlan tag native

### *1.9.36.14 (config-if)# switchport vlan ip-subnet id*

**Syntax:** (config-if)# switchport vlan ip-subnet id <vce_id> <ipv4> vlan <vid>

**Explanation:** IP Subnet-based VLAN configuration is to map untagged ingress frames to a specific VLAN if the source address is found in the IP subnet-to-VLAN mapping table. When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

**Parameters:**

<vce_id: 1-128>: Specify index of the entry. Valid range is 1~128.

<ipv4>: Specify IP address and subnet mask. The format is xx.xx.xx.xx/mm.mm.mm.mm.

<vid>: Indicate the VLAN ID.

**Negation:** (config-if)# no switchport vlan ip-subnet id <vce_id_list>

**Show:** # show vlan ip-subnet [ id <subnet_id> ]

### *1.9.36.15 (config-if)# switchport vlan mac*

**Syntax:** (config-if)# switchport vlan mac <mac_addr> vlan <vid>

**Explanation:** This command is to set up VLANs based on source MAC addresses. When ingress untagged frames are received by a port, source MAC address is processed to decide which VLAN these untagged frames belong. When source MAC addresses does not match the rules created, untagged frames are assigned to the receiving port's native VLAN ID (PVID).

**Parameters:**

<mac_addr>: Indicate the source MAC address. Please note that the source MAC address can only map to one VLAN ID.

vlan <vid>: Map this MAC address to the associated VLAN ID.

**Negation:** (config-if)# no switchport vlan mac <mac_addr> vlan <vid>

**Show:** # show vlan mac [ address <mac_addr> ]

#### *1.9.36.16 (config-if)# switchport vlan mapping*

**Syntax:** (config-if)# switchport vlan mapping <group>

**Explanation:** Configure group VLAN mapping table for this specific interface.

**Parameters:**

<group: 1-20>: Indicate the Group ID that applies to this rule.

**Negation:** (config-if)# no switchport vlan mapping

#### *1.9.36.17 (config-if)# switchport vlan protocol group*

**Syntax:** (config-if)# switchport vlan protocol group <grp_id> vlan <vid>

**Explanation:** Configure VLAN protocol group for this specific interface.

**Parameters:**

<grp_id: word 16>: Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-Z) or integers (0-9).

<vid>: Specify the VLAN ID that applies to this rule.

**Negation:** (config-if)# no switchport vlan protocol group <grp_id> vlan <vid>

**Show:** # show vlan protocol [ eth2 { <etype> **|** arp **|** ip **|** ipx **|** at } ] [ snap { <oui> **|** rfc-1042 **|** snap-8021h } <pid> ] [ llc <dsap> <ssap> ]

### *1.9.36(config)# tacacs-server*

#### *1.9.36.1 (config)# tacacs-server timeout*

**Syntax:** (config)# tacacs-server timeout <seconds>

**Explanation:** The time the switch waits for a reply from a TACACS+ server before it retransmits the request.

**Parameters:**

<seconds:1-1000>: Specify a value for timeout. The allowed timeout range is between 1 and 1000.

**Negation:** (config)# no tacacs-server timeout

**Show:** # show tacacs-server

### *1.9.36.2 (config)# tacacs-server deadtime*

**Syntax:** (config)# tacacs-server deadtime <minutes>

**Explanation:** Deadtime 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.

**Parameters:**

<minutes:1-1440>: Specify a value for tacacs-server deadtime. The allowed deadtime range is between 1 to 1440 minutes.

**Negation:** (config)# no tacacs-server deadtime

**Show:** # show tacacs-server

### *1.9.36.3 (config)# tacacs-server key*

**Syntax:** (config)# tacacs-server key <key>

**Explanation:** Specify the secret key up to 63 characters. This is shared between a TACACS+ sever and the switch.

**Parameters:**

<key:1-63>: Specify a shared secret key value.

**Negation:** (config)# no tacacs-server key

**Show:** # show tacacs-server

### *1.9.36.4 (config)# tacacs-server host*

**Syntax:** (config)# tacacs-server host <host_name> [ port <port> ] [ timeout <seconds> ] [ key <key> ]

**Explanation:** Configure radius server settings.

**Parameters:**

<host_name>: Specify a hostname or IP address for the TACACS+ server.

[ port <port> ]: Specify the TCP port number to be used on a TACACS+ server for authentication.

[timeout <seconds>]: If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

[key <key>]: If secret key is specified here, it will replace the global secret key. If you prefer to use the global value, leave this field blank.

**Negation:** (config)# no tacacs-server host <host_name> [ port <port> ]

**Show:** # show tacacs-server

## *1.9.36(config)# username*

### *1.9.36.1 (config)# username<username>privilege<priv>password encrypted*

**Syntax:** (config)# username <username> privilege <priv> password encrypted <encry_password>

**Explanation:** By default, there is only one user, 'admin', assigned the highest privilege level of 15. Use this command to configure a new user account.

**Parameters:**

username <username: word31>: Specify a new username. The allowed characters are 31.

privilege <priv: 0-15>: Specify the privilege level for this new user account. The allowed range is 1 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 other values 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.

password encrypted <encry_password: 4-44>: Specify the encrypted password for this new user account. The ENCRYPTED (hidden) user password. Notice the ENCRYPTED password will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.

**Example:** Create the new user account with the following settings.

```
# config t
(config)# username mis4jack privilege 15 password encrypted jack30125
```

**Negation:** (config)# no username <username>

**Show:** > show users
#show users

### *1.9.36.2 (config)# username<username>privilege<priv>password none*

**Syntax:** (config)# username <username> privilege <priv> password none

**Explanation:** By default, there is only one user, 'admin', assigned the highest privilege level of 15. Use this command to configure a new user account without password

**Parameters:**

username <username: word31>: Specify a new username. The allowed characters are 31.

privilege <priv: 0-15>: Specify the privilege level for this new user account. The allowed range is 1 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 other values 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.

password none: No password for this user account.

**Example:** Create the new user account with the following settings.

```
# config t
(config)# username mis4jack privilege 15 password none
```

**Negation:** (config)# no username <username>

**Show:** > show users
# show users

### *1.9.36.3 (config)# username<username>privilege<priv>password unencrypted*

**Syntax:** (config)# username <username> privilege <priv> password unencrypted <password>

**Explanation:** By default, there is only one user, 'admin', assigned the highest privilege level of 15. Use this command to configure a new user account with unencrypted password.

**Parameters:**

username <username: word31>: Specify a new username. The allowed characters are 31.

privilege <priv: 0-15>: Specify the privilege level for this new user account. The allowed range is 1 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 other values 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.

password unencrypted <password: line31>: Specify the unencrypted password for this user account. The UNENCRYPTED (Plain Text) user password. Any printable characters including space is accepted.

**Example:** Create the new user account with the following settings.

```
# config t
(config)# username mis4jack privilege 15 password unencrypted jack30125
```

**Negation:** (config)# no username <username>

**Show:** > show users
# show users

## *1.9.36(config)# vlan*

### *1.9.36.1 (config)# vlan*

**Syntax:** (config)# vlan <vlist>

**Explanation:** Configure allowed VLANs.

**Parameters:**

<vlist>: This shows the allowed access VLANs. This setting only affects ports set in "Access" mode. Ports in other modes are members of all VLANs specified in "Allowed VLANs" field. By default, only VLAN 1 is specified. More allowed access VLANs can be entered by specifying the individual VLAN ID separated by comma. If you want to specify a range, separate it by a dash. For example, 1, 5,10,12-15,100. Once Enter is pressed, the prompt changes to (config-vlan)#

**Example:** Add VID 1,5,10,12-15,100 to the allowed VLAN list.

```
# config t
(config)# vlan 1,510,12-15,100
(config-vlan)#
```

**Negation:** (config)# no vlan { { ethertype s-custom-port } **|** <vlan_list> }

### *1.9.36.2 (config)# vlan ethertype s-custom-port*

**Syntax:** (config)# vlan ethertype s-custom-port <etype>

**Explanation:** Configure ether type used for customer s-ports.

**Parameters:**

ethertype s-custom-port <etype>: Specify ether type used for customer s-ports. The valid range is 0x0600 to 0xffff.

**Example:** Set ether type for customer s-port to 0x88a8.

```
# config t
(config)# vlan ethertype s-custom-port 0x88a8
```

**Negation:** (config)# no vlan { { ethertype s-custom-port } **|** <vlan_list> }

### *1.9.36(config)# web privilegegroup*

**Syntax:** (config)# web privilege group <group_name> level { [ cro <cro> ] [ crw <crw> ] [ sro <sro> ] [ srw <srw> ] }*1

**Explanation:** Assign web privilege level to the specified group.

**Parameters:**

group <group_name>: This name identifies the privilege group. Valid words are Aggregation' 'DHCP' 'Dhcp_Client' 'Diagnostics' 'EEE' 'ERPS' 'Green_Ethernet' 'IP2' 'IPMC_Snooping' 'LACP' 'LLDP' 'Loop_Protect' 'MAC_Table' 'MVR' 'Maintenance' 'Mirroring' 'NTP' 'POE' 'PTP' 'Ports' 'Private_VLANs' 'QoS' 'RPC' 'SMTP' 'Security' 'Smart_Config' 'Spanning_Tree' 'System' 'Timer' 'UPnP' 'VCL' 'VLAN_Translation' 'VLANs' 'XXRP' 'u-Ring'

level { [ cro <cro: 0-15> ] [ crw <crw: 0-15> ] [ sro <sro: 0-15> ] [ srw <srw: 0-15> ] }*1: Every group has an authorization Privilege level for the following sub groups:

cro (configuration read-only): The privilege level is 1 to 15.

crw (configuration/execute read-write): The privilege level is 1 to 15.

sro (status/statistics read-only): The privilege level is 1 to 15.

srw (status/statistics read-write): The privilege level is 1 to 15.

User Privilege should be the same or greater than the authorization Privilege level to have access to that group.

**Example:** Assign Aggregation group to crw (configuration/excute read-write) level 15.

```
# config t
(config)# web privilege group aggregation level crw 15
(config)# exit
# show web privilege group level
Group Name                          Privilege Level
                                   CRO   CRW   SRO   SRW
--------------------------------    ---   ---   ---   ---
Aggregation                           5    15     5    10
DHCP                                  5    10     5    10
Dhcp_Client                           5    10     5    10
Diagnostics                           5    10     5    10
EEE                                   5    10     5    10
ERPS                                  5    10     5    10
Green_Ethernet                        5    10     5    10
IP2                                   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
Maintenance                          15    15    15    15
Mirroring                             5    10     5    10
MVR                                   5    10     5    10
NTP                                   5    10     5    10
POE                                   5    10     5    10
Ports                                 5    10     1    10
-- more --, next page: Space, continue: g, quit: ^C
```

**Negation:** (config)# no web privilege group <group_name> level

**Show:** > show web privilege group <group_name> level

# show web privilege group <group_name> leve

## 1.10 POE Configuration

### 1.10.1 POE Mode

**Syntax:** (config-if)# poe mode

<etype> **Explanation:** Set POE MODE

**Example:** Set port 1 POE MODE

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)#poe mode [Plus / Standard]
```

### 1.10.2 POE power limit

**Syntax:** (config-if)# poe power limit

<etype> **Explanation:** Set POE power limit setting

**Example:** Set port 1 POE Power limit

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)#poe power limit [1~30]
```

### 1.10.3 POE Priority

**Syntax:** (config-if)# poe priority

<etype> **Explanation:** Set POE priority

**Example:** Set port 1 poe priority

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)#poe priority [Critical / high / low]
```

### 1.10.4 POE Schedule

**Syntax:** (config-if)# poe-schedule time

<etype> **Explanation:** Set poe-schedule day and time

**Example:** Set port 1 poe schedule

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)#poe-schedule time [Fri  Mon  Sat  Sun  Thu  Tue  Wed][0-23]
```

### 1.10.5 POE Auto ping check

**Syntax:** (config-if)# auto-ping

<etype> **Explanation:** Set POE AUTO PING CHECK

**Example:** Set port 1 auto ping

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)#auto-ping ip [ipv4_ucast] interval[10-120] retry [1-5] action
[nothing / power-off / power-on / restart-forever / restart-once] reboot [3-
120]
```

### 1.10.6 POE Global - Capcaitor detect

**Syntax:** (config)# poe capacitor-detect

<etype> **Explanation:** Set POE Capcaitor detect

**Example:** Set POE Global Capcaitor detect

```
# config t
(config)# poe capacitor-detect
```

**Example:** Disable POE Global Capcaitor detect

```
# config t
(config)# no poe capacitor-detect
```

### 1.10.7 POE Global – management mode

**Syntax:** (config)# poe management mode

<etype> **Explanation:** Set POE global management

**Example:** Set ether type for customer s-port to 0x88a8.

```
# config t
(config)# poe managedment mode [allocation-consumption / allocation-reserved-
power / class-consumption / class-reserved-power / lldp-consumption / lldp-
reserved-power]
```

### 1.10.8 POE Global – POE Supply

**Syntax:** (config)# poe supply

<etype> **Explanation:** Set POE Supply

**Example:** Set poe global POE Supply

```
# config t
(config)#poe supply [1-2000]
```