Cybersecurity Switch

Kernel S12

Industrial Managed Ethernet Switch

(POE / Layer2 / Layer3)

GUI Manual

V1.2

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:

(in default , LLDP is enable , VLAN = 1 , each other feature all is disable)

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.10.254**

User name : admin

Password : follow password protection .

Password protection

The device is password-protected. The first time that any user accesses the device, the device will prompt the user to set a password at the service Policies.

Note :

About Password security Policies

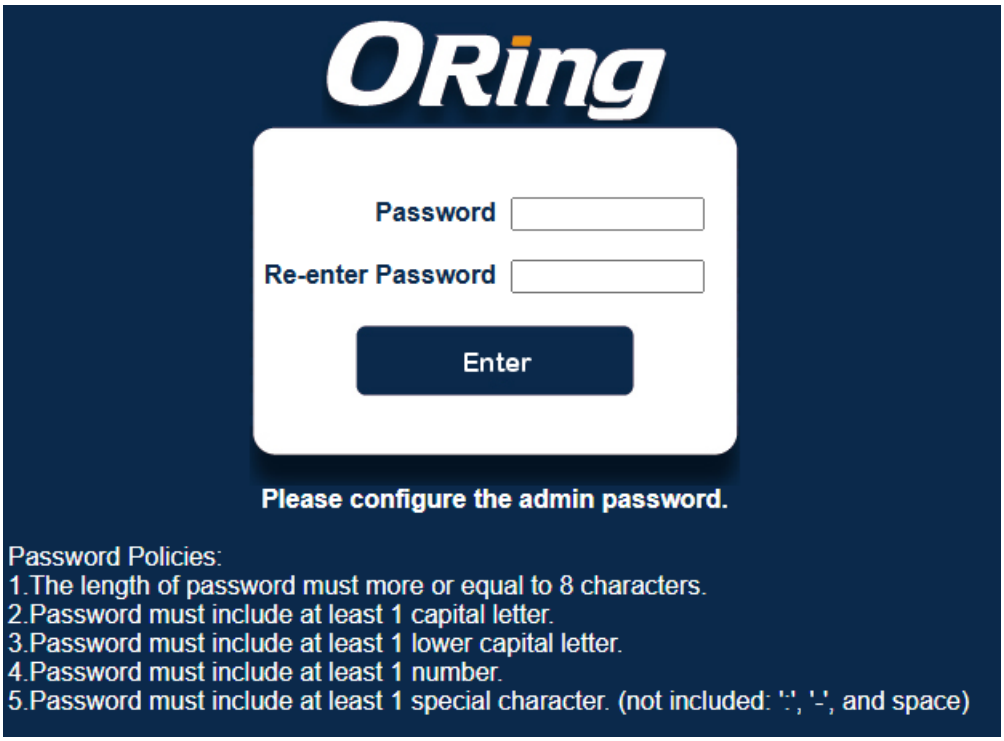
1.The length of password must more or equal to 8 characters.

2.Password must include at least 1 capital letter.

3.Password must include at least 1 lower capital letter.

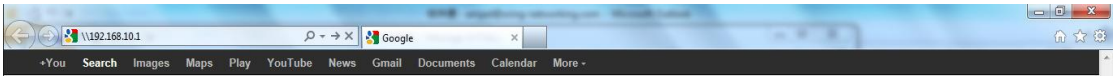
4.Password must include at least 1 number.

5.Password must include at least 1 special character. (not included: ':', '-', and space)



System Login

1. Launch the Internet Explorer.
2. Type https:// 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.

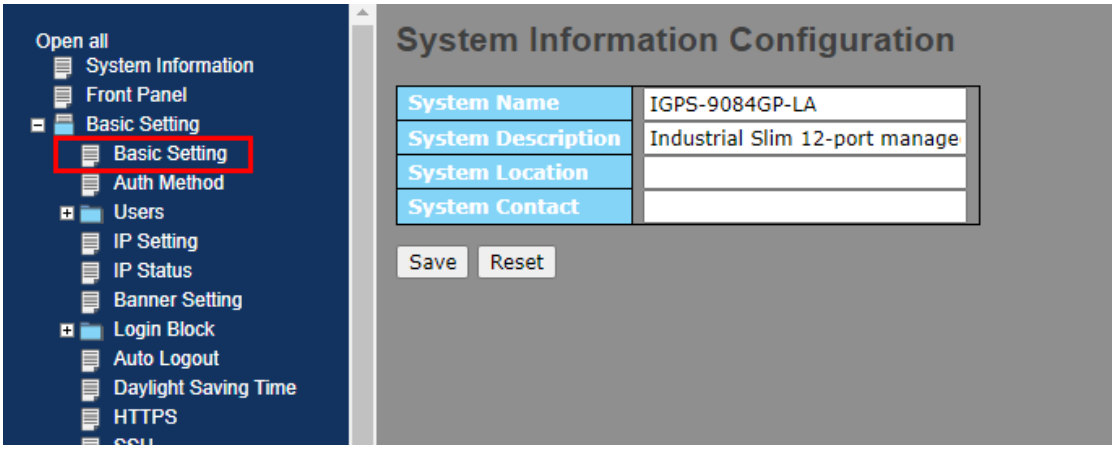
After logging in, you can see the information of the switch as below.

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.



.

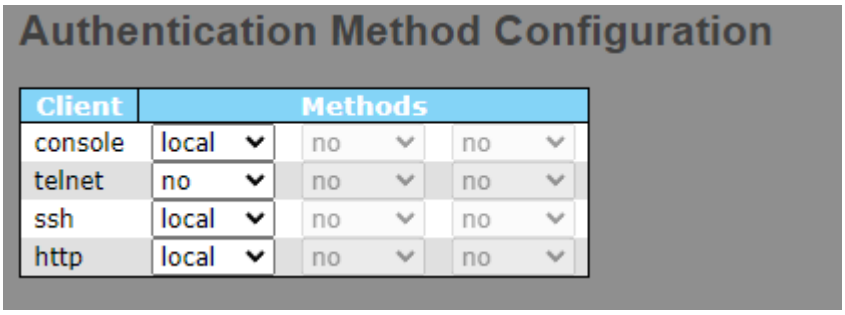
Label	Description
System Name	An administratively assigned name for the managed node. By convention, this is the node's fully-qualified domain name. A

	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.

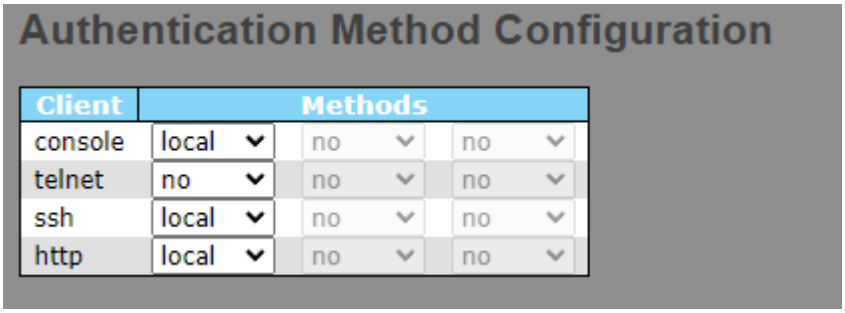


Label	Description
Client	The management client for which the configuration below applies.
Methods	Method can be set to one of the following values: · **no**: Authentication is disabled and login is not possible. · **local**: Use the local user database on the switch for authentication. · **radius**: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

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

Command Authorization Method Configuration

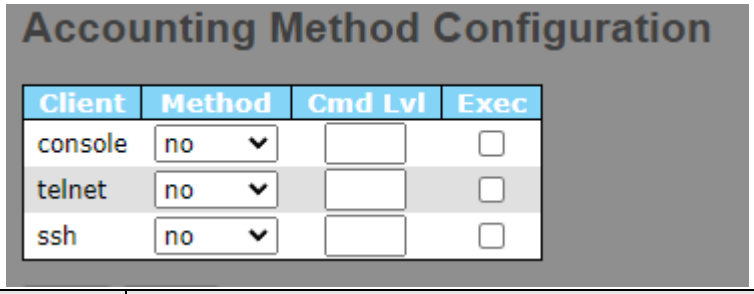
The command authorization section allows you to limit the CLI commands available to a user.



Label	Description
Client	The management client for which the configuration below applies.
Methods	Method can be set to one of the following values: · **no**: Command authorization is disabled. User is granted access to CLI commands according to his privilege level. · **tacacs**: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.

Accounting Method Configuration

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



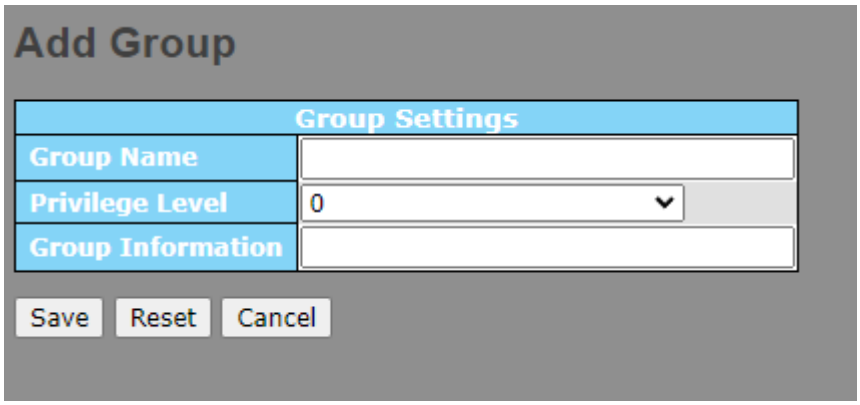
Label	Description
Client	The management client for which the configuration below applies.
Methods	Method can be set to one of the following values: · **no**: Accounting is disabled. · **tacacs**: Use remote TACACS+ server(s) for accounting.
Cmd Lvl	Enable accounting of all commands with a privilege level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

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

1.1.3 Users

Group List

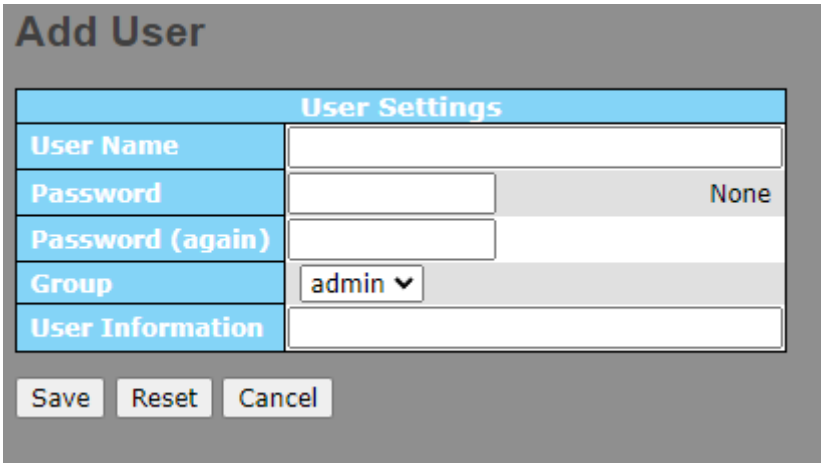
The name identifying the group. This is also a link to Add/Edit Group.



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

User List

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.

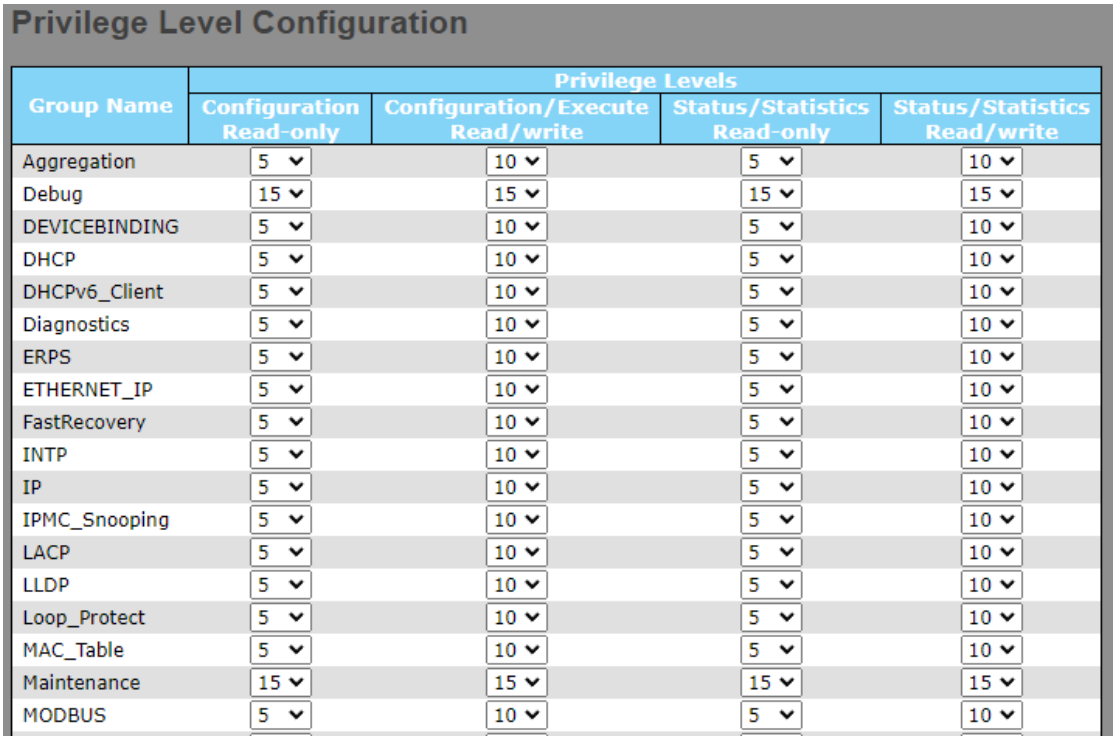


Label	Description
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31. The valid user name can be letters, numbers and underscores.
Password/Password(again)	The password of the user. The allowed string length is 0 to 31. Any printable characters including space are accepted.
Group	The group that the user belong to.
User Information	Information about the user.

* Password Policies:
The length of password must more or equal to 8 characters.
Password must include at least 1 capital letter.
Password must include at least 1 lower capital letter.
Password must include at least 1 number.
Password must include at least 1 special character. (not included: ':', '-', and space)
* It is recommended to change password every three months. Password lifecycle management

Privilege Levels

This page provides an overview of the privilege levels.



Privilege Level Configuration

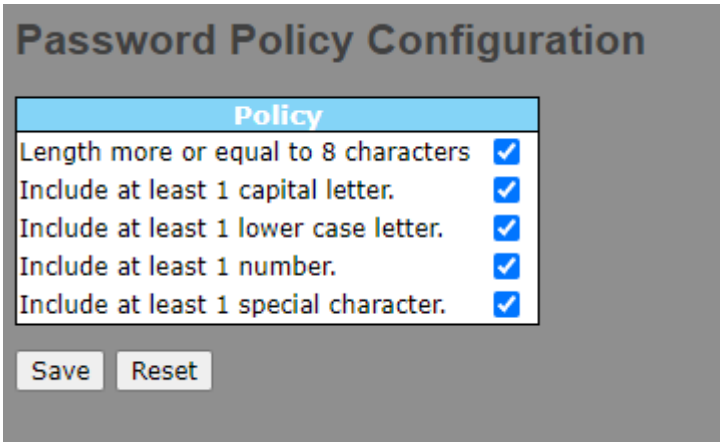
Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Debug	15	15	15	15
DEVICEBINDING	5	10	5	10
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
ERPS	5	10	5	10
ETHERNET_IP	5	10	5	10
FastRecovery	5	10	5	10
INTP	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
MODBUS	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: **System**: Contact, Name, Location, Timezone, Daylight Saving Time, Log. **Security**: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, IP source guard. **IP**: Everything except 'ping'. **Port**: Everything except 'VeriPHY'. **Diagnostics**: 'ping' and 'VeriPHY'. **Maintenance**: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

	Debug: Only present in CLI.
Privilege Levels	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.

Password Policy Configuration

This page is used to configure the password policy.



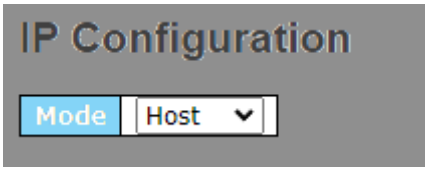
Label	Description
Policy	● **Length more or equal to 8 characters** The length of password must more or equal to 8 characters. By default, this option is enabled. ● **Include at least 1 capital letter** Password must include at least 1 capital letter. By default, this option is enabled. ● **Include at least 1 lower capital letter** Password must include at least 1 lower capital letter. By default, this option is enabled. ● **Include at least 1 number** Password must include at least 1 number. By default, this option is enabled. ● **Include at least 1 special character** Password must include at least 1 special character(not included: ':', '-', and space). By default, this option is enabled.

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)

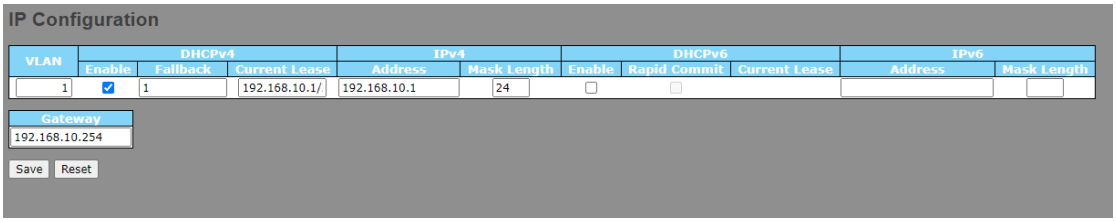
the item provides user setting switch mode .



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

IP Interface

This page provides an overview of the privilege levels.



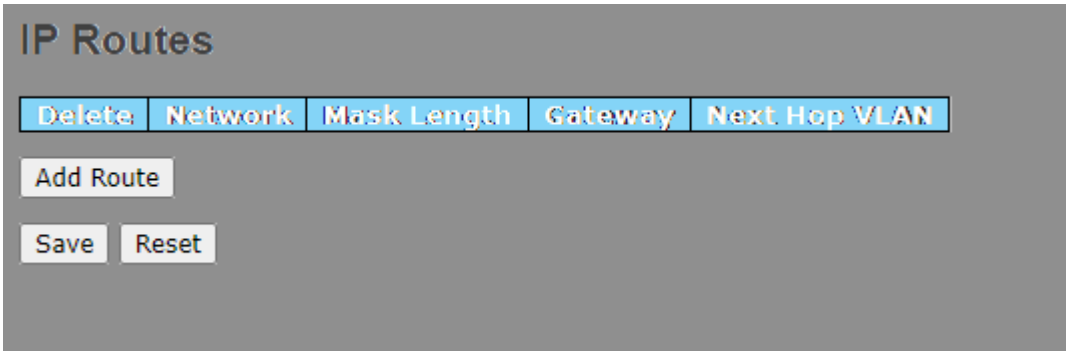
Label	Description
VLAN	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.
IPv4 DHCP Enabled	Enable the DHCPv4 client by checking this box. If this option is enabled, the system 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. 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. If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
DHCPv6 Enable	Enable the DHCPv6 client by checking this box. If this option is enabled, the system will configure the IPv6 address of the interface using the DHCPv6 protocol.
DHCPv6 Rapid Commit	Enable the DHCPv6 Rapid-Commit option by checking this box. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received. This option is only manageable when DHCPv6 client is enabled.
DHCPv6 Current Lease	For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.
IPv6 Address	The IPv6 address of the interface. 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. System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address. 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. 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. At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or there is indeed other device occupying the same hardware address as the device in the VLAN. After making sure the specific link-local address is unique on the IPv6 link in use, delete and then add the specific IPv6 interface to restart the IPv6 operations on this interface.
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

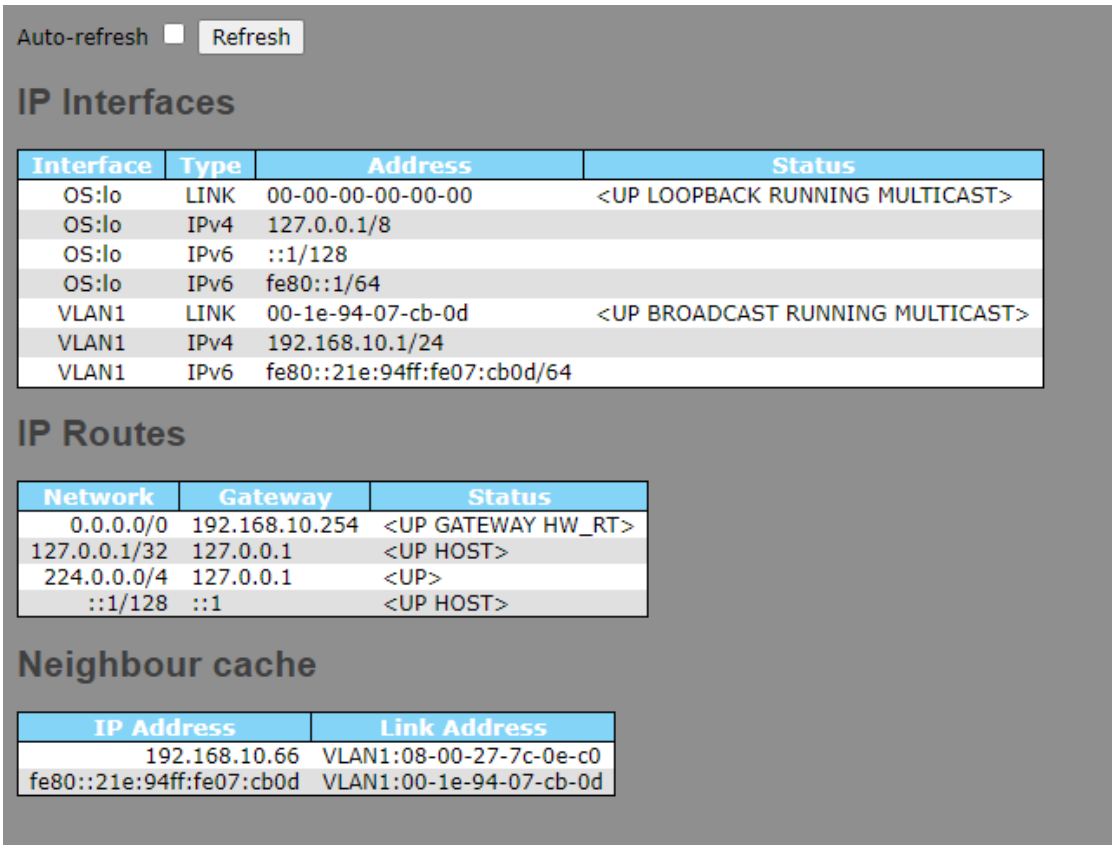


Label	Description
Delete	Select this option to delete an existing IP route.
Network	The destination IP network or host address of this route. Valid format is dotted decimal notationor a valid IPv6 notation. A default route can use the value 0.0.0.0or IPv6 :: notation.
Mask Length	The destination IP network 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. The given VID ranges from 1 to 4095 and will be effective only when the corresponding IPv6 interface is valid. If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway. If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

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.

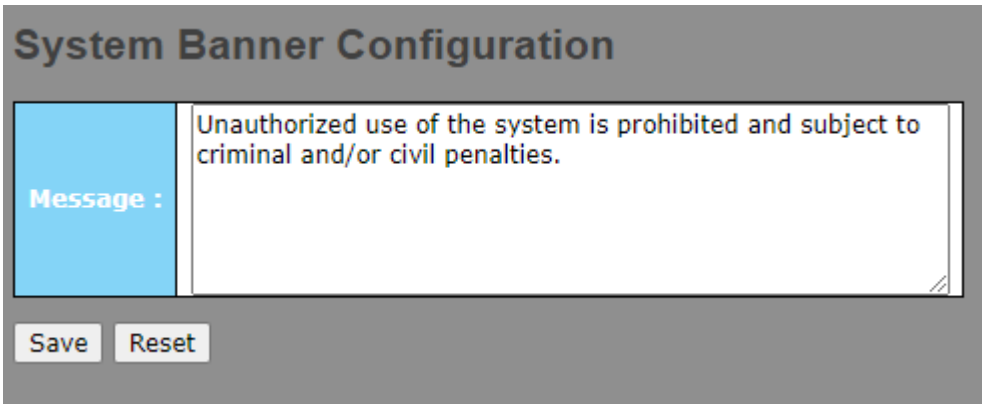


Label	Description
IP Interface	

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 System Banner Configuration

Users can edit the text message on the welcome screen when the device starts up here.

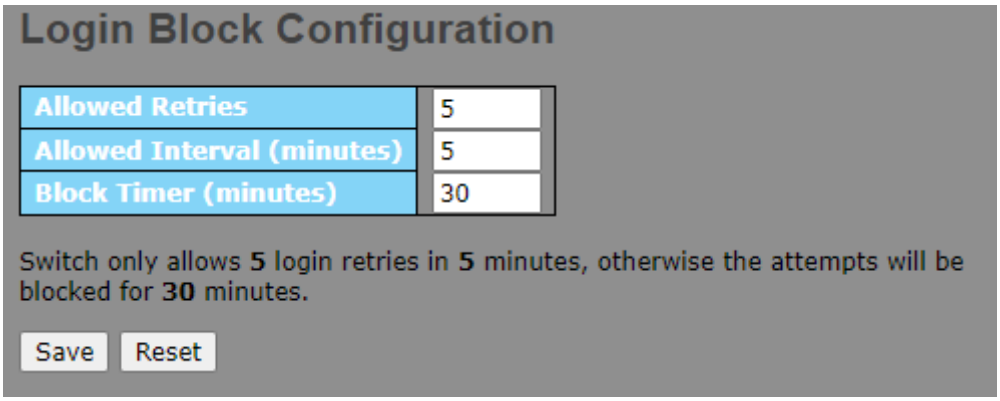


Label	Description
Message	Users can enter any text in this field and the text will be displayed on the welcome screen before logging in.

1.1.7 Login Block

Configuration

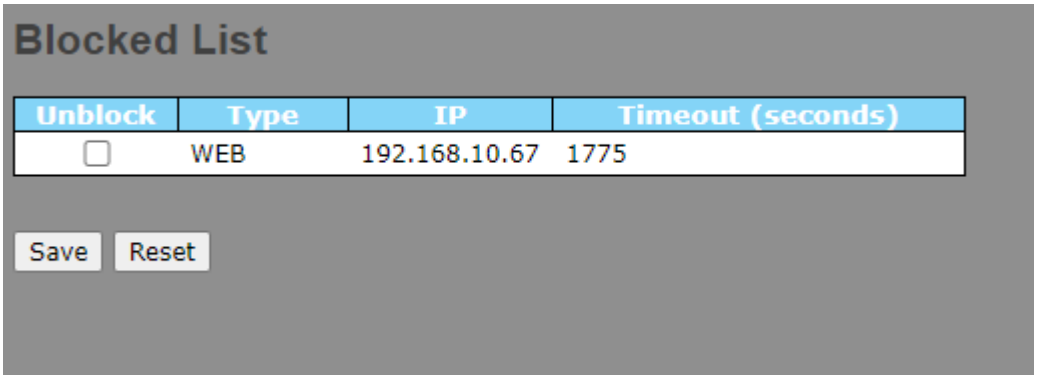
This page could specify Login Block timer.



Label	Description
Allowed Retries	Allowed retries for failed login attempts.
Allowed Interval	Allowed interval for failed login attempts.
Block Timer	Timer for blocking login.

Blocked List

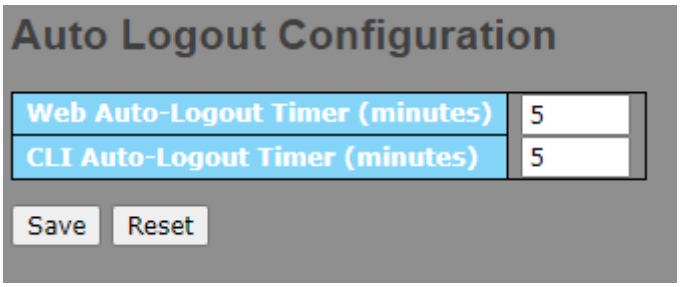
The page will show lock devices information.



Label	Description
Unblock	When a user attempts to log in to SWITCH and the number of failed login attempts exceeds Allowed Retries, SWITCH will record the user's information and lock them.

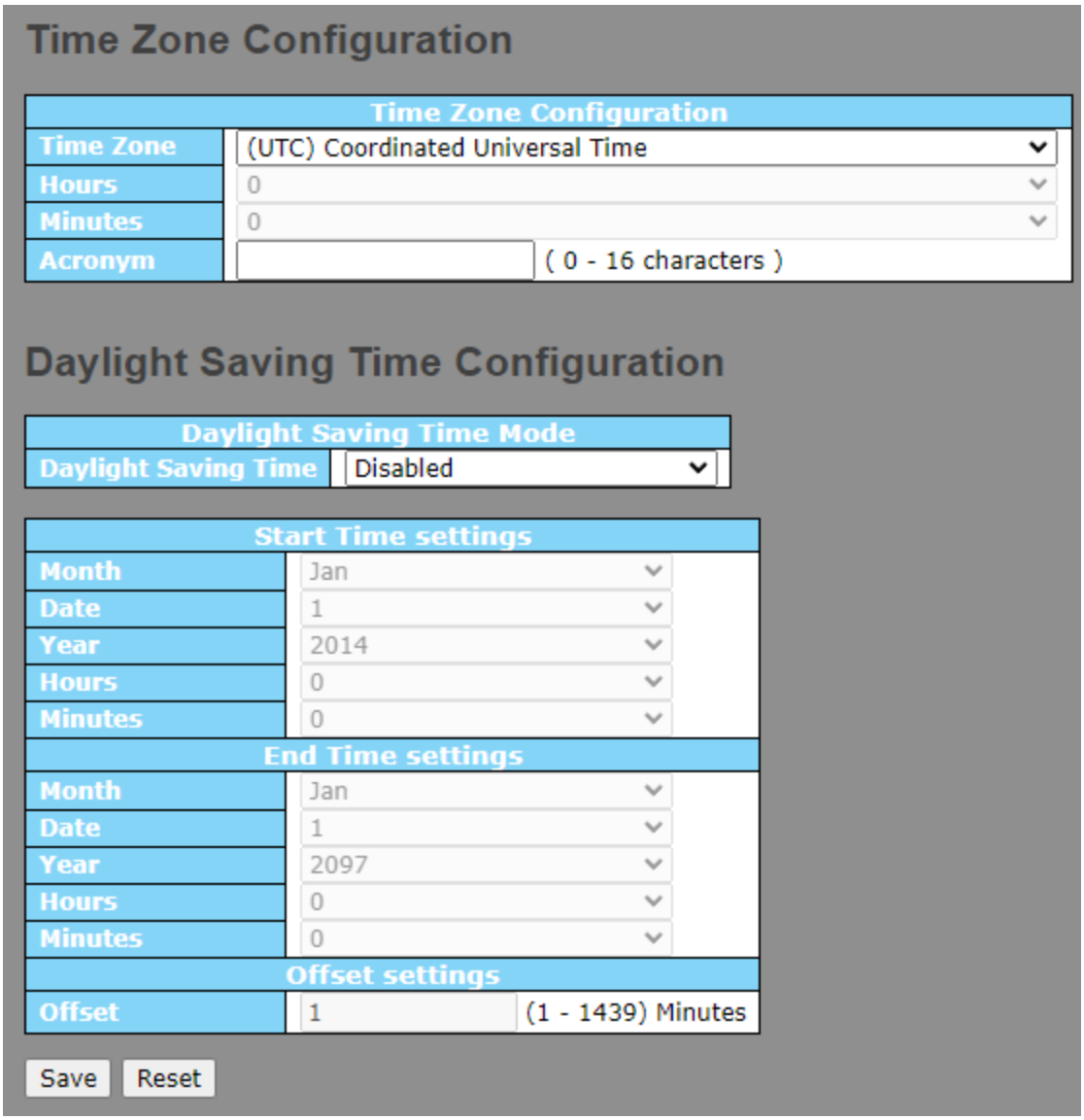
1.1.8 Auto Logout

The page can setting Web and CLI Mode auto-logout timer .



Label	Description
Web Auto-Logout Timer	Web Auto-Logout Timer in minutes.
CLI Auto-Logout Timer	CLI Auto-Logout Timer in minutes.

1.1.9 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

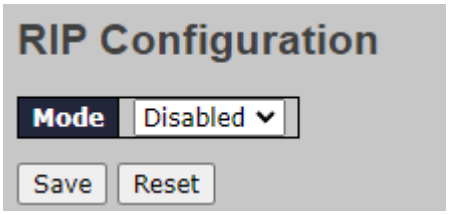
	disable the daylight saving time configuration. Select **'Recurring'** and configure the Daylight Saving Time duration to repeat the configuration every year. Select '**Non-Recurring**' and configure the daylight saving time duration for single time configuration. (Default : Disabled). Start Time Settings: Set up the start time of the daylight saving time period. End Time Settings: Set up the ending time of the daylight saving time period. 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 EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard 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 FWT - French Winter MET - Middle European MEWT - Middle European Winter 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 GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

1.1.10 RIP (only for Layer 3 Model)

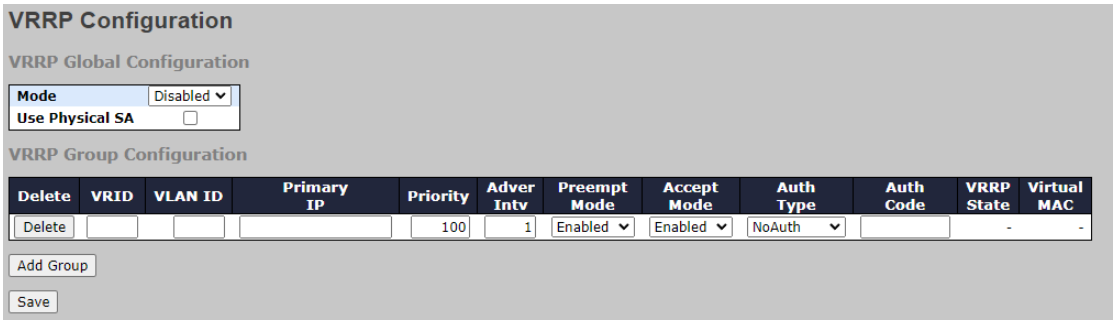
Configure RIP on this page.



Label	Description
Mode	Indicates the RIP mode operation. Possible modes are: Enabled: Enable RIP mode operation. Disabled: Disable RIP mode operation.

1.1.11 VRRP (only for Layer 3 Model)

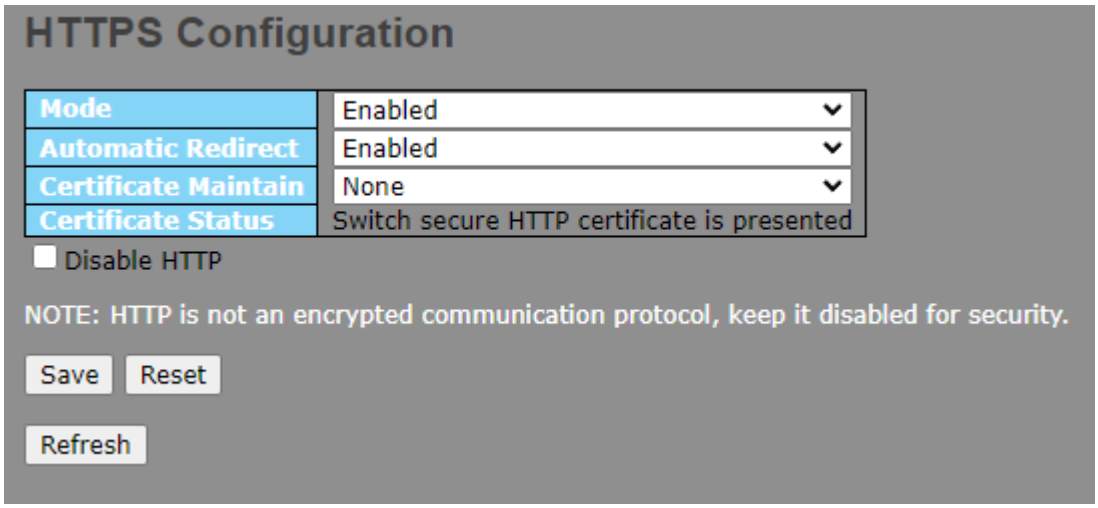
Configure VRRP on this page.



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

1.1.12 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: **None**: No operation. **Delete**: Delete the current certificate. **Upload**: Upload a certificate PEM file through a Web browser or URL. **Generate**: Generate a new self-signed RSA certificate.
Certificate Status	Display the current status of certificate on the switch. Possible statuses are: **Switch secure HTTP certificate is presented.** **Switch secure HTTP certificate is not presented.** **Switch secure HTTP certificate is generating**.
Disable HTTP	The check box can disable HTTP Service.

1.1.13 SSH

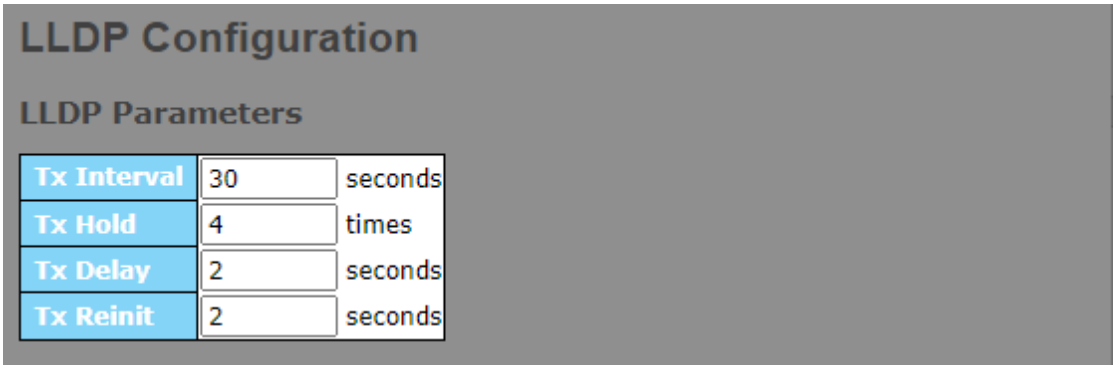
You can configure the SSH mode in this page.

Label	Description
Mode	Enable or disable SSH.
Disable Telnet	The check box can disable Telnet Service
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values.

1.1.14 LLDP

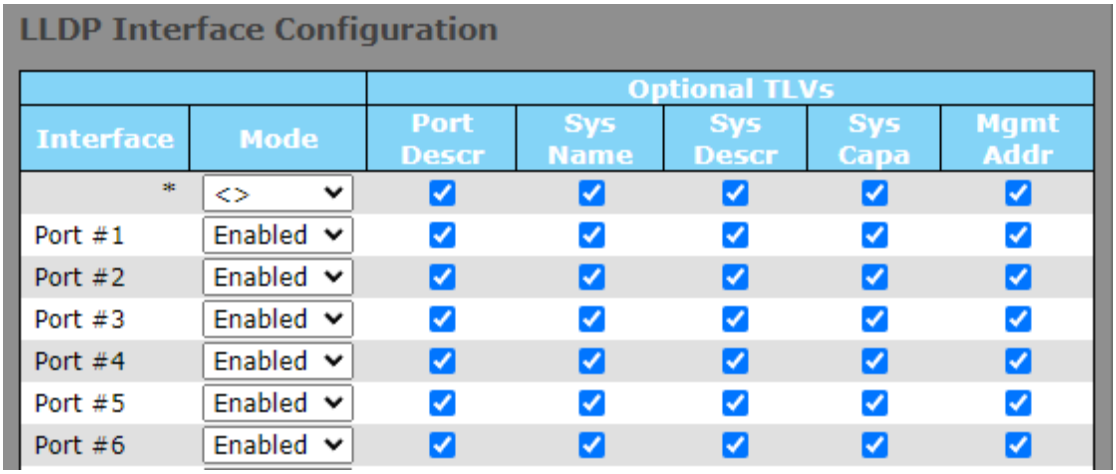
LLDP Configurations

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.

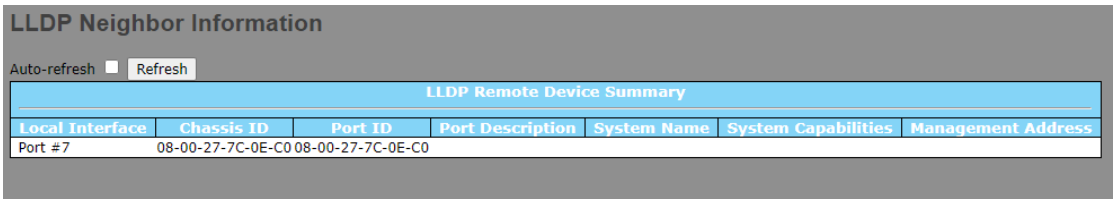


Label	Description
Interface	The switch interface name of the logical LLDP interface.
Mode	Select a LLDP mode from the drop down list. **Rx only**: The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. **Tx only**: The switch will drop LLDP information received from neighbors, but will send out LLDP information. **Disabled**: The switch will not send out LLDP information, and will drop LLDP information received from neighbors. **Enabled**: The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

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.

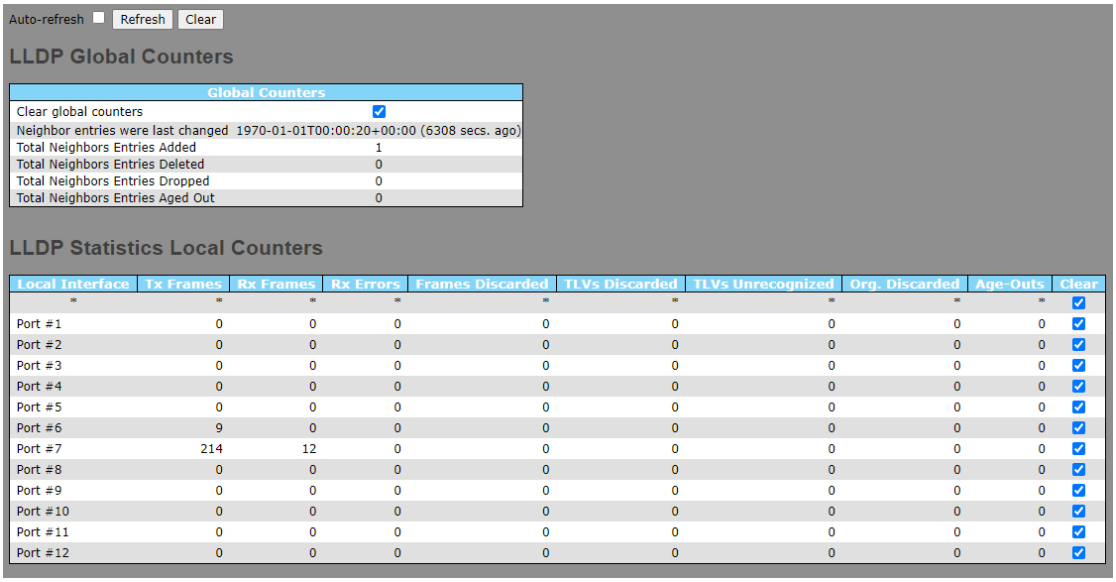


Label	Description
Local Port	The port that you use to transmits and receives LLDP frames.
Chassis ID	The identification number of the neighbor sending out the LLDP frames.
Remote Port ID	The identification of the neighbor port
System Name	The name advertised by the neighbor.
Port Description	The description of the port advertised by the neighbor.
System Capabilities	Description of the neighbor's capabilities. The capabilities include: 1. **Other** 2. **Repeater** 3. **Bridge** 4. **WLAN Access Point** 5. **Router** 6. **Telephone** 7. **DOCSIS Cable Device** 8. **Station Only** 9. **Reserved** When a capability is enabled, 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	Shows the number of entries deleted due to expired time-to-live

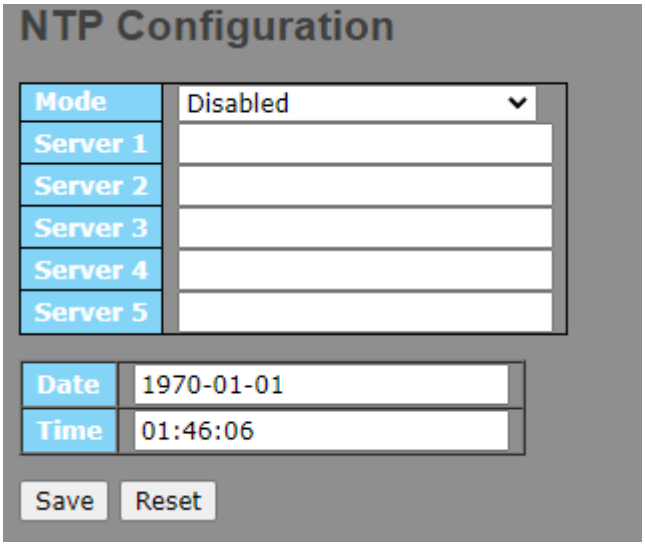
Entries Aged Out	

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.

1.1.15 NTP

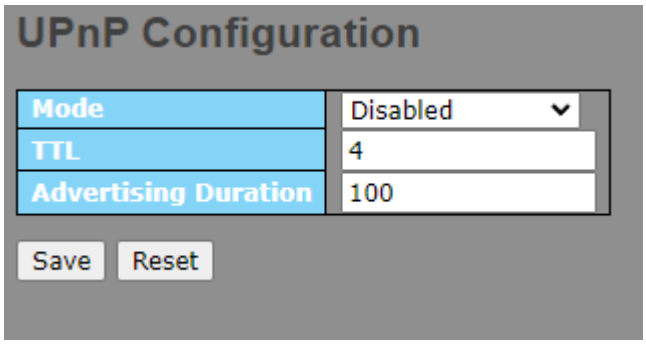
The function allows you to specify the Network Time Protocol (NTP) servers to query for the current time to maintain an accurate time on the switch, ensuring the system log record meaningful dates and times for event entries. With NTP, the switch can set its internal clock periodically according to an 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.

1.1.16 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

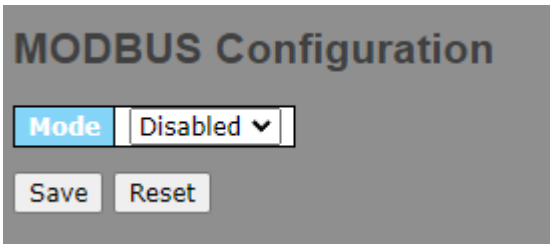


Label	Description
Mode	Indicates the UPnP operation mode. Possible modes are:

	Enabled: Enable UPnP mode operation. Disabled: Disable UPnP mode operation. When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.
TTL	The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.
Advertising Duration	The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

1.1.17 Modus TCP

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

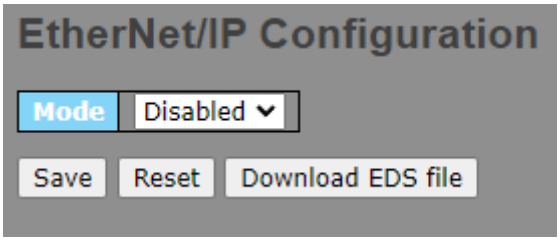


The following table describes the labels in this screen.

Label	Description
Mode	Enable or Disalble Modbus TCP function

1.1.18 Ethernet/IP

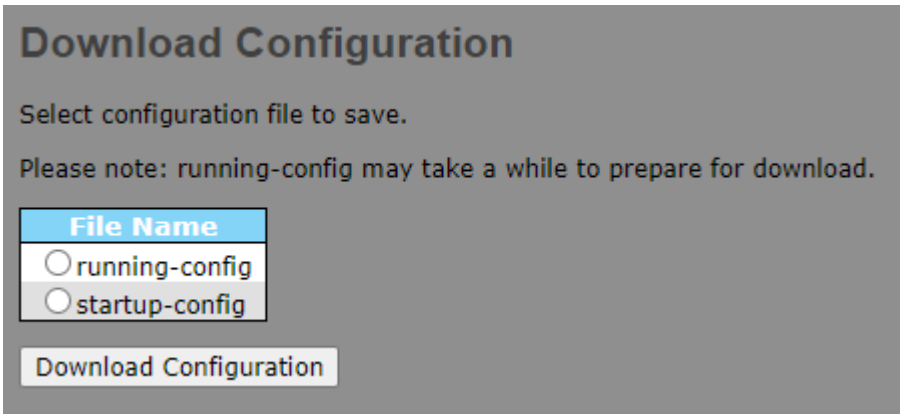
EtherNet/IP is an industrial network protocol that adapts the Common Industrial Protocol to standard Ethernet.[1] EtherNet/IP is one of the leading industrial protocols in the United States and is widely used in a range of industries including factory, hybrid and process.

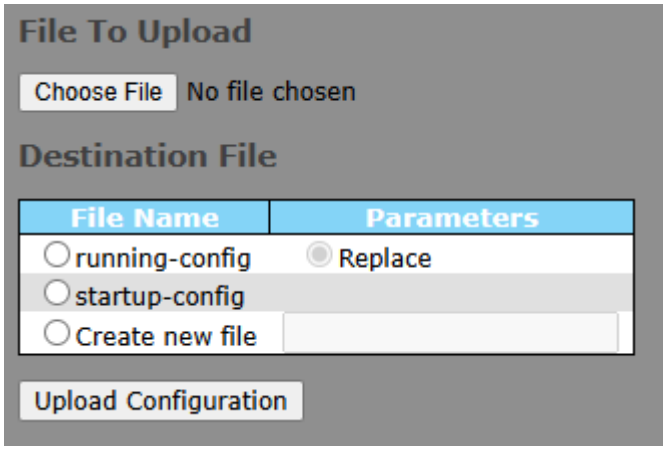


Label	Description
Mode	Indicates the EtherNet/IP mode operation. Possible modes are: Enabled: Enable EtherNet/IP mode operation. Disabled: Disable EtherNet/IP mode operation.

1.1.19 Backup/Restore Configurations

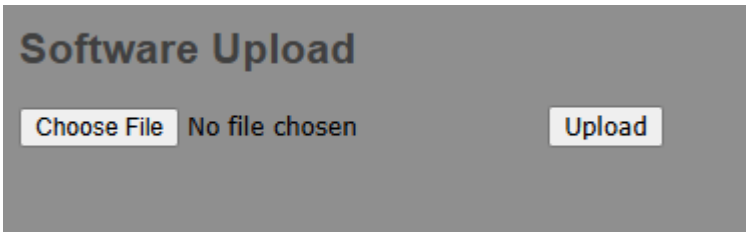
You can save/view or load switch configurations.





1.1.20 Firmware Update

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

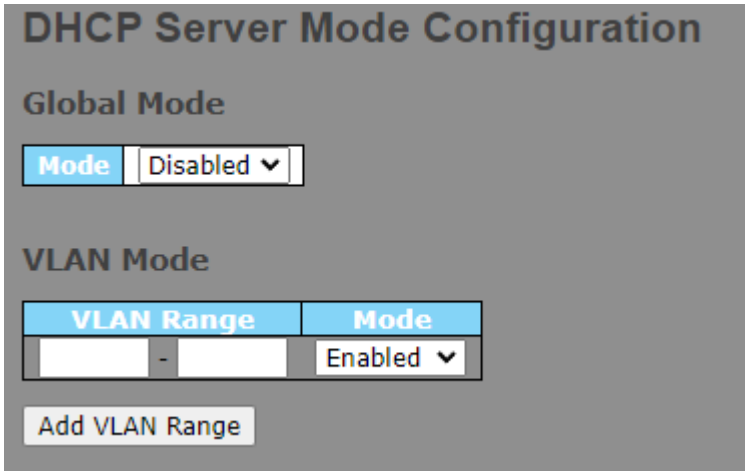


1.2 DHCP

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.

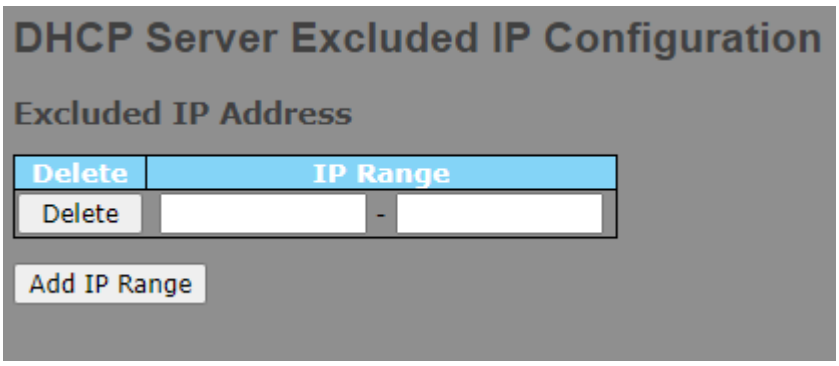
Mode



Label	Description
Global Mode	
Mode	Configure the operation mode per system. Possible modes are: **Enabled**: Enable DHCP server per system. **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. On the other hand, if you want to disable existed VLAN range, then you can follow the steps. 1. Press **Add VLAN Range** to add a new VLAN range. 2. input the VLAN range that you want to disable. 3. choose Mode to be **Disabled**. 4. press Save to apply the change. Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.
Mode	Indicate the operation mode per VLAN. Possible modes are: **Enabled:** Enable DHCP server per VLAN. **Disabled**: Disable DHCP server pre VLAN.

Excluded IP

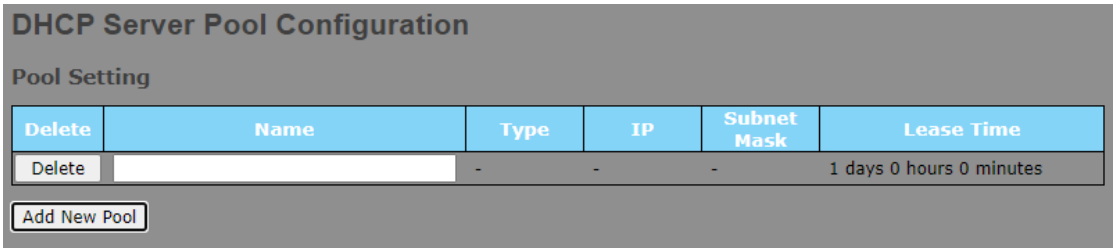
This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client



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

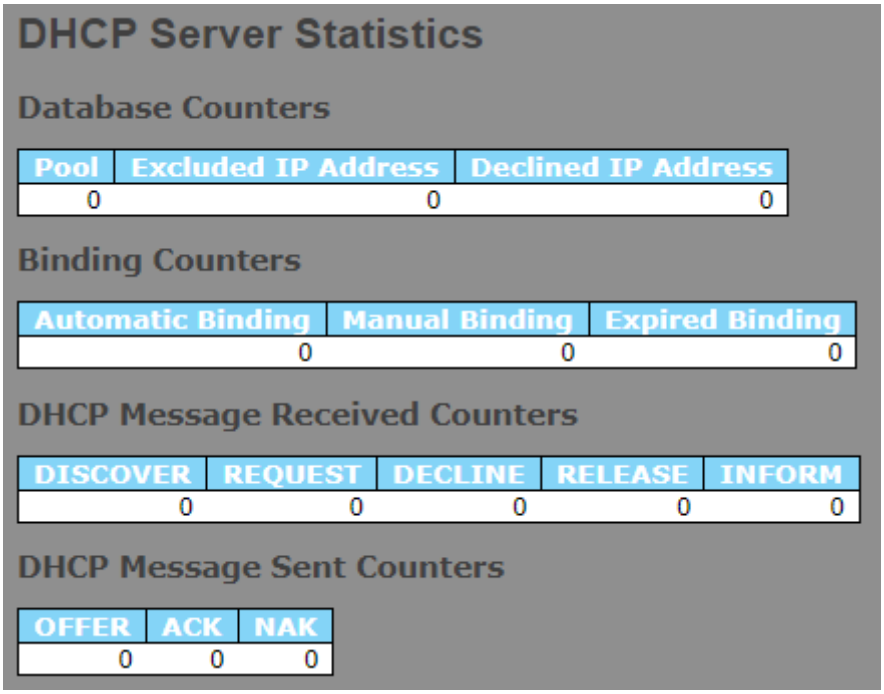
This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.



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. **Network**: the pool defines a pool of IP addresses to service more than one DHCP client. **Host**: the pool services for a specific DHCP client identified by client identifier or hardware address. If "-" is displayed, it means not defined.
IP	Display network number of the DHCP address pool. If "-" is displayed, it means not defined.
Subnet Mask	Display subnet mask of the DHCP address pool. If "-" is displayed, it means not defined.
Lease Time	Display lease time of the pool.

Statistics

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

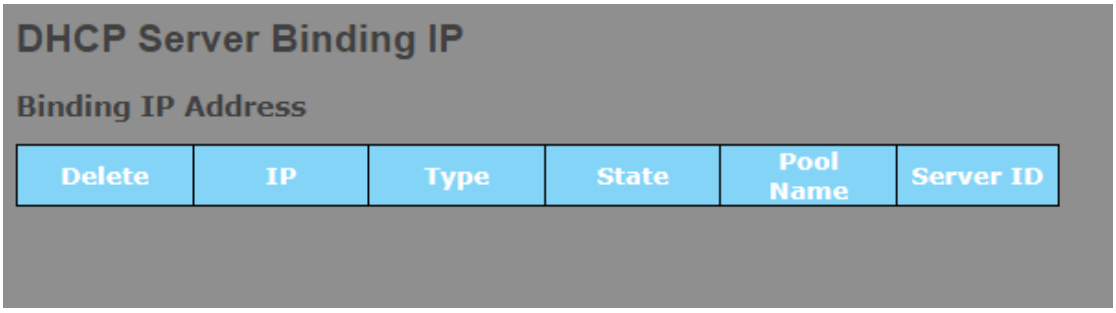


Label	Description
Database Counters	
Pool	Number of pools.
Excluded IP Address	Number of excluded IP address ranges.
Declined IP Address	Number of declined IP addresses.
Binding Counters	
Automatic Binding	Number of bindings with network-type pools.
Manual Binding	Number of bindings that administrator 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

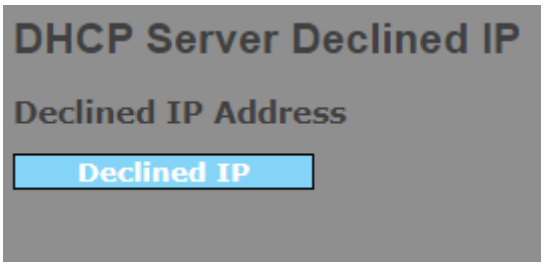
This page displays bindings generated for DHCP clients.



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

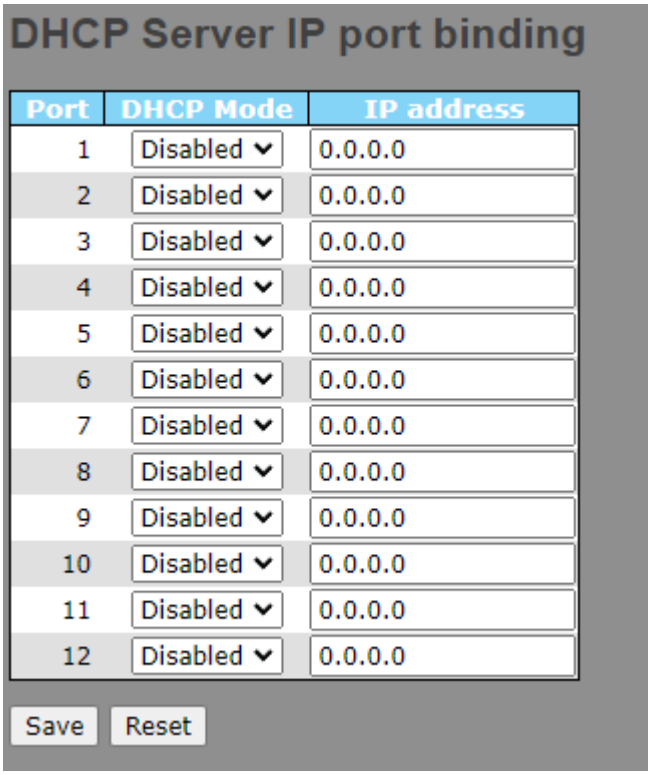
Display IP addresses declined by DHCP clients.



Label	Description
Declined IP	List of IP addresses declined.

IP and Port Binding

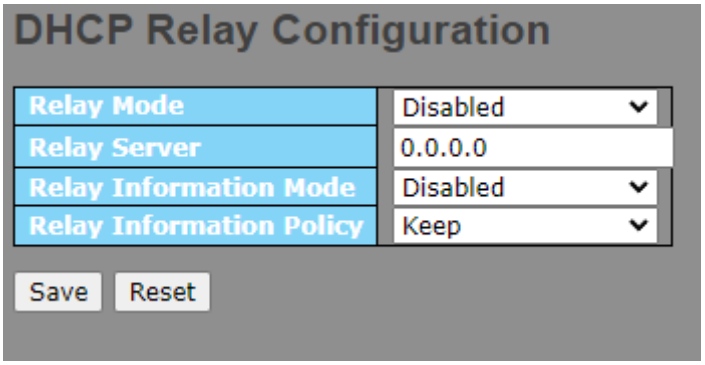
This page can be configured to allow users to allocate IP addresses based on SWITCH ports.



Label	Description
DHCP Mode	Enable or Disable DHCP Server .
IP Address	The user defined IP in this field will be assigned to the device

1.2.2 DHCP Relay

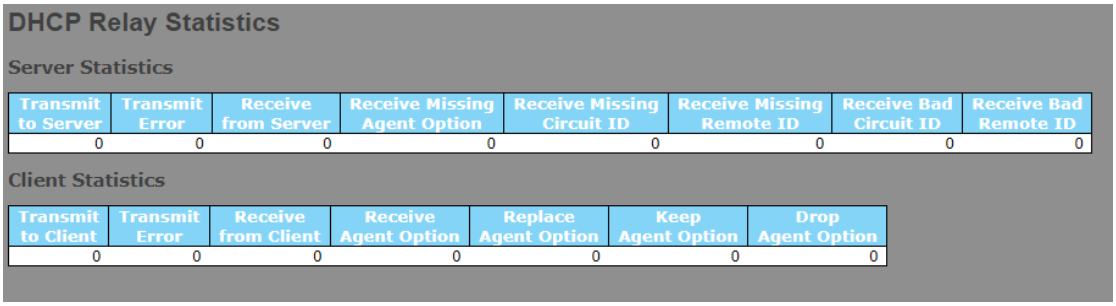
DHCP relay is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain. You can configure the function in this page.



Label	Description
Relay Mode	Indicates the existing DHCP relay mode. The modes include:

	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. **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. The modes include: **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. **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: **Replace**: replace the original relay information when a DHCP message containing the information is received. **Keep**: keep the original relay information when a DHCP message containing the information is received. **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.

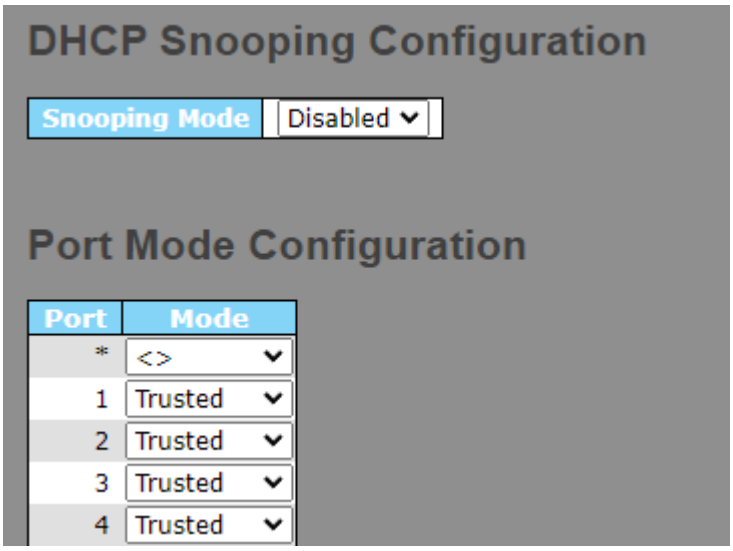


Label	Description
Transmit to Sever	The number of packets relayed from the client to the server
Transmit Error	The number of packets with errors when being sent to clients
Receive from Server	The number of packets received from the server
Receive Missing Agent Option	The number of packets received without 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

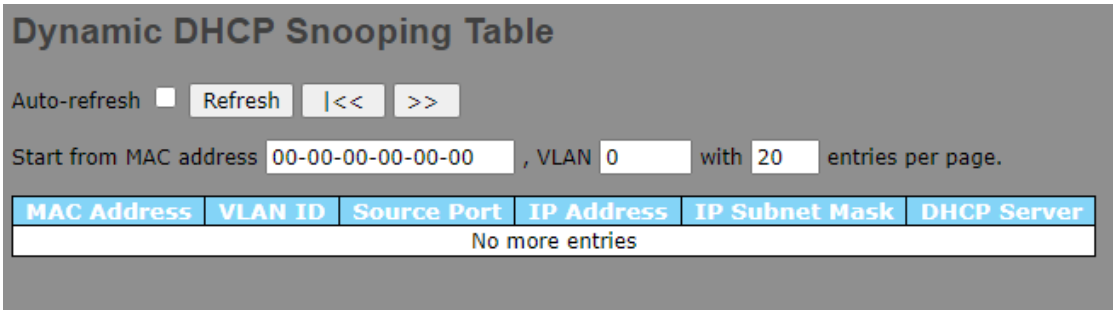
Configure DHCP Snooping on this page.



Label	Description
Snooping Mode	Indicates the DHCP snooping mode operation. Possible modes are: **Enabled**: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports. **Disabled**: Disable DHCP snooping mode operation.
Port Mode Configuration	Indicates the DHCP snooping port mode. Possible port modes are: **Trusted**: Configures the port as trusted source of the DHCP messages. **Untrusted**: Configures the port as untrusted source of the DHCP messages.

Snooping Table

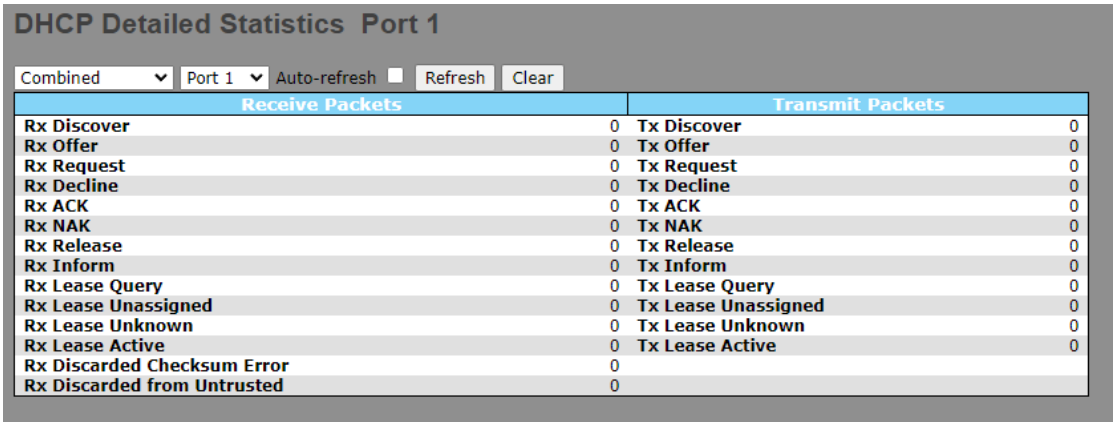
This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.



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.

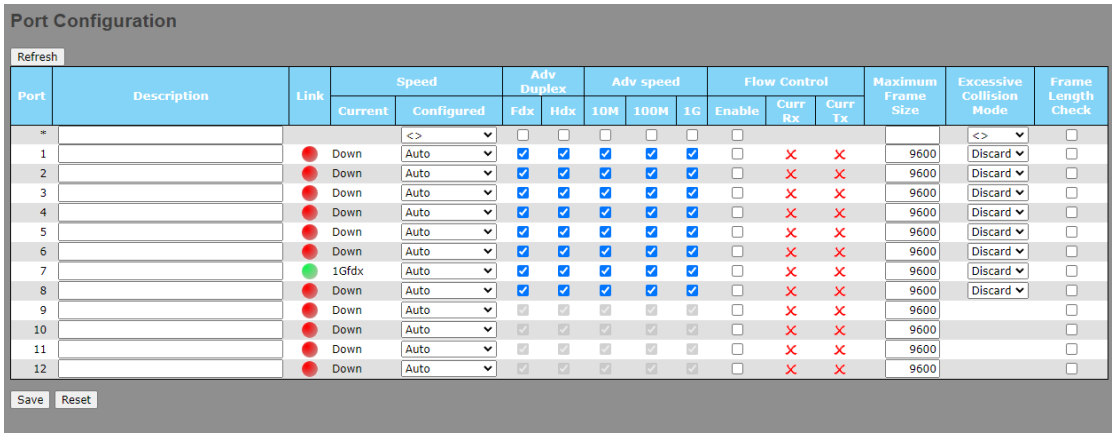
Rx and Tx Request	The number of request (option 53 with value 3) packets received and transmitted.
Rx and Tx Decline	The number of decline (option 53 with value 4) packets received and transmitted.
Rx and Tx ACK	The number of ACK (option 53 with value 5) packets received and transmitted.
Rx and Tx NAK	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 Unknown	The number of lease unknown (option 53 with value 12) packets received and transmitted.
Rx and Tx Lease Active	The number of lease active (option 53 with value 13) packets received and transmitted.
Rx Discarded checksum error	The number of discard packet that IP/UDP checksum is error.
Rx Discarded from Untrusted	The number of discarded packet that are coming from untrusted port.

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: **Disabled** - Disables the switch port operation. **Auto** - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner. **10Mbps HDX** - Forces the cu port in 10Mbps half duplex mode. **10Mbps FDX** - Forces the cu port in 10Mbps full duplex mode. **100Mbps HDX** - Forces the cu port in 100Mbps half duplex mode.

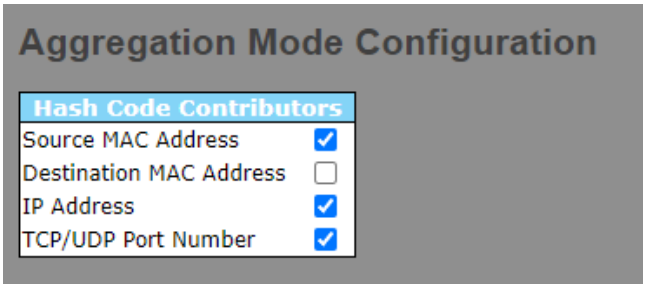
	100Mbps FDX - Forces the cu port in 100Mbps full duplex mode. **1Gbps FDX** - Forces the port in 1Gbps full duplex **2.5Gbps FDX** - Forces the Serdes port in 2.5Gbps full duplex mode. **SFP_Auto_AMS** - Automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto 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. **100-FX** - SFP port in 100-FX speed. Cu port disabled. **1000-X** - SFP port in 1000-X speed. Cu port disabled. Ports in AMS mode with 1000-X speed have Cu port preferred. Ports in AMS mode with 1000-X speed have fiber port preferred. 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. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port

	are transmitted. The Rx and Tx settings are determined by the result of the last Auto Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed. NOTICE: The 100FX standard 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. **Discard**: Discard frame after 16 collisions (default). **Restart**: Restart backoff algorithm after 16 collisions.
Frame Length Check	Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field 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

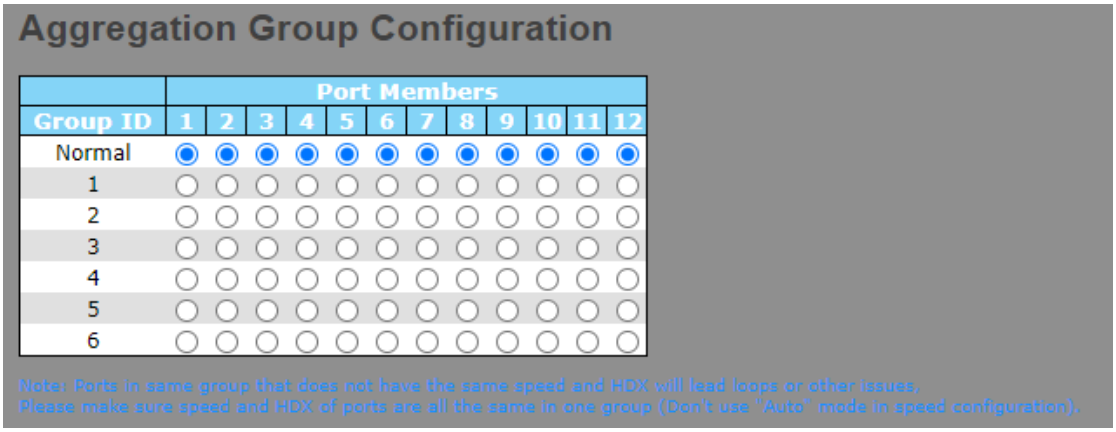
1.3.2 Port Trunk

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



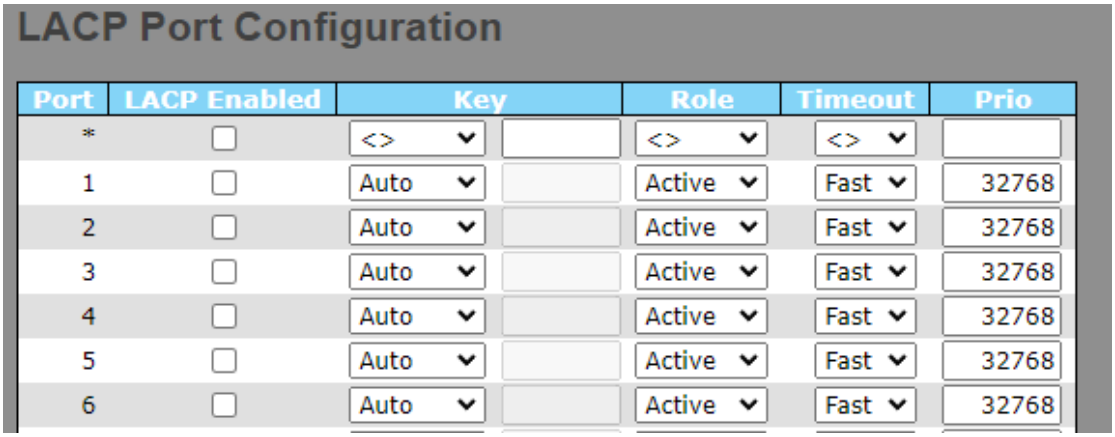
Label	Description
Source MAC Address	Calculates the destination port of the frame. You can check this box to enable the source MAC address, or uncheck to disable. By default, **Source MAC Address** is enabled.
Destination MAC Address	Calculates the destination port of the frame. You can check this box 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

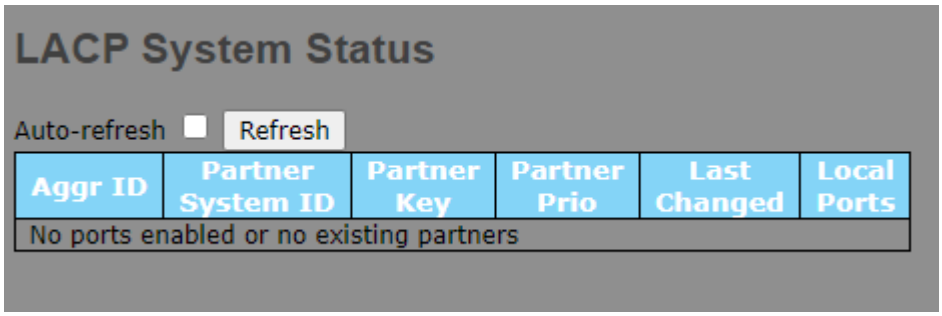
LACP (Link Aggregation Control Protocol) trunks are similar to static port trunks, but they are more flexible because LACP is compliant with the IEEE 802.3ad standard. Hence, it is interoperable with equipment from other vendors that also comply with the standard. This page allows you to enable LACP 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

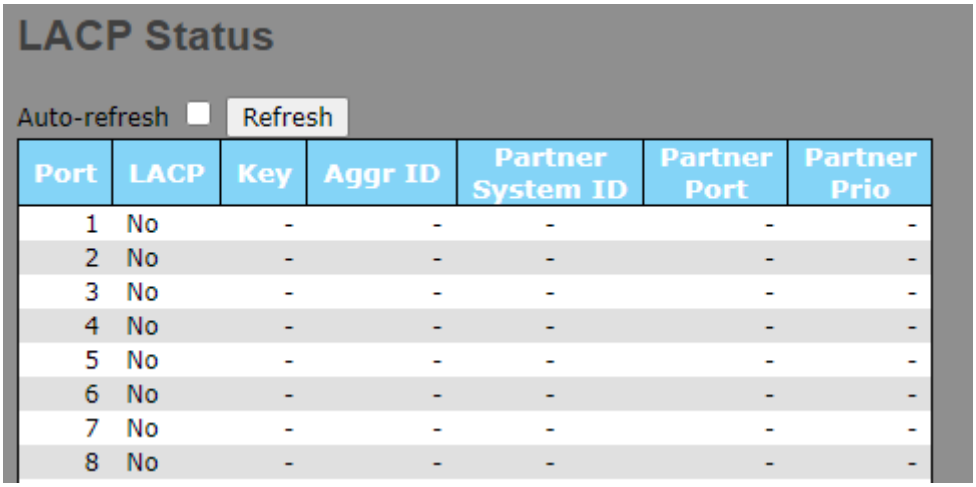
This page provides a status overview for all LACP instances.



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

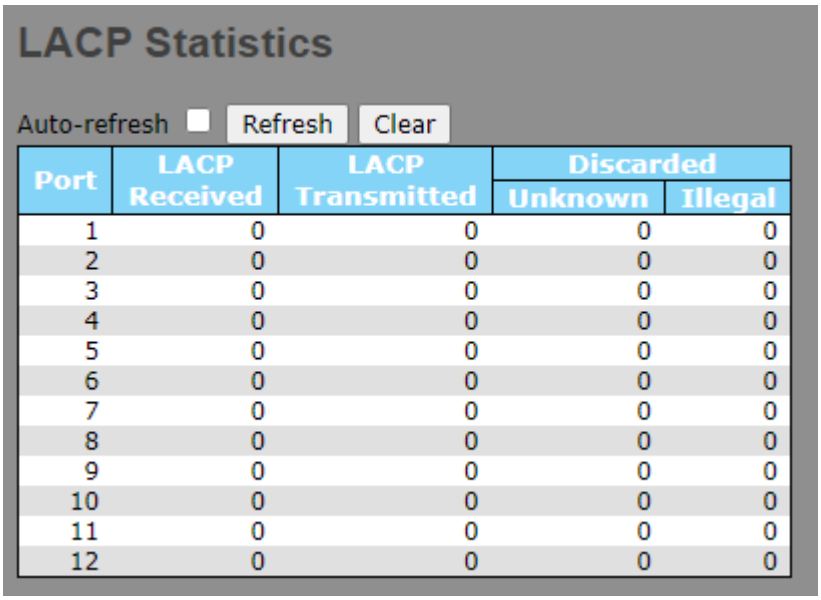
This page provides an overview of the LACP status for all ports.



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.

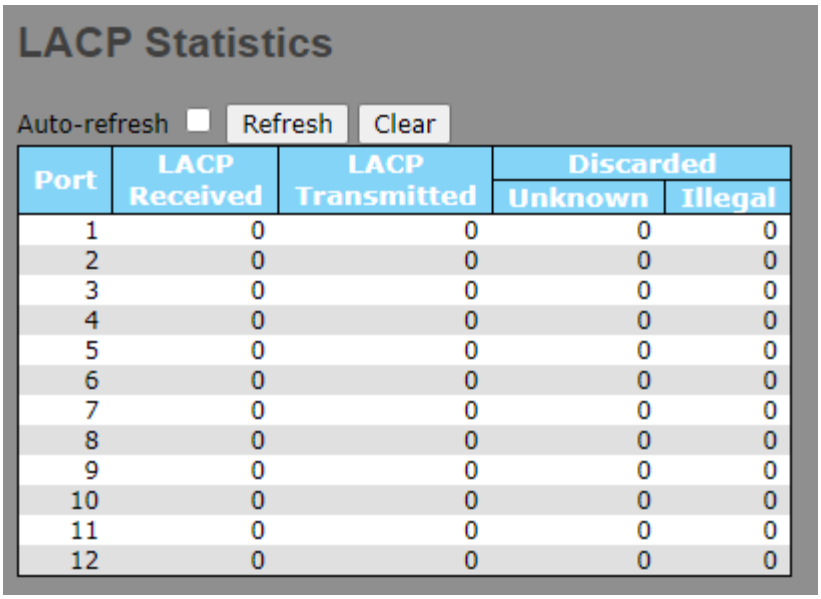


Label	Description
Port	Switch port number
LACP Transmitted	The number of LACP frames sent from each port
LACP Received	The number of LACP frames received at each port
Discarded	The number of unknown or illegal LACP frames discarded at each

	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

Static

This page is used to see the staus of ports in Aggregation group.

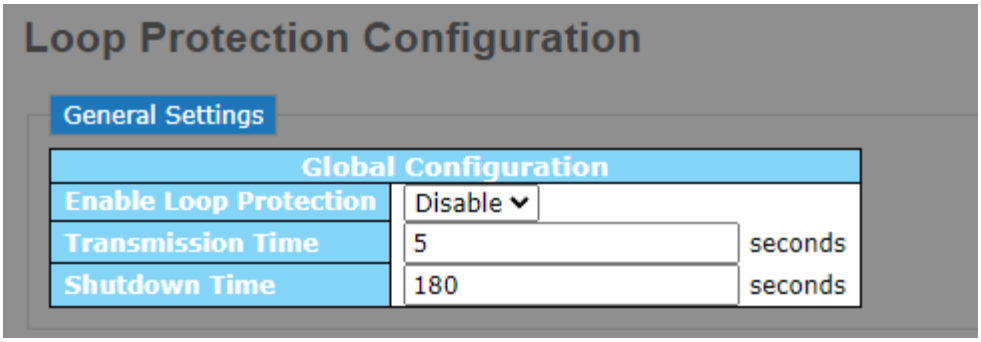


Label	Description
Aggr ID	The Aggregation ID associated with this aggregation instance.
Name	Name of the Aggregation group ID.
Type	Type of the Aggregation group(Static or LACP).
Speed	Speed of the Aggregation group.
Configured ports	Click to refresh the page immediately
Aggregated ports	Aggregated member ports of the Aggregation group.

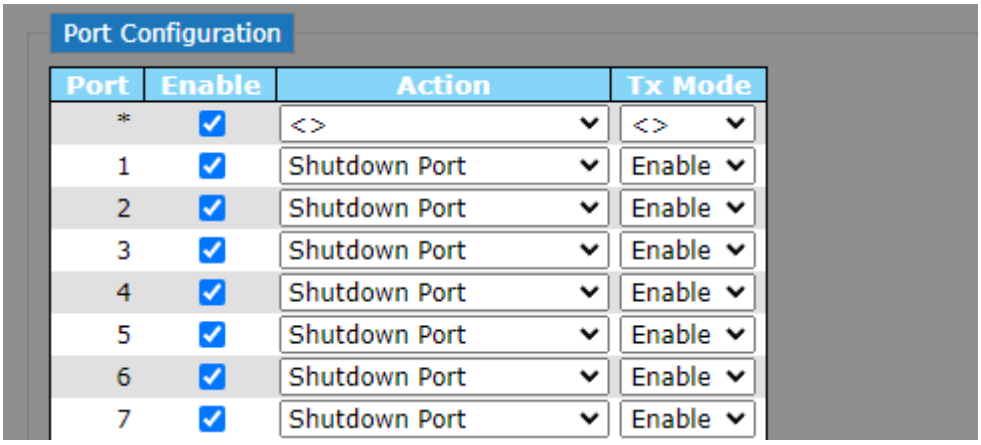
1.3.3 Loop Protection

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).

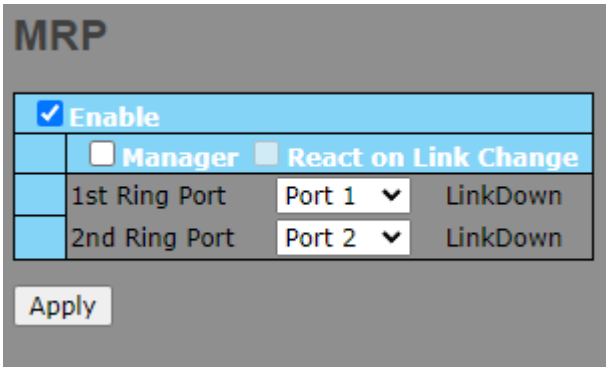


Label	Description
Port	Switch port number
Enable	Activate loop protection functions (as a whole)
Action	Configures the action to take when a loop is detected. Valid values include **Shutdown Port**, **Shutdown Port**, and **Log or Log Only**.
Tx Mode	Controls whether the port is actively generating loop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

1.4 Redundancy

1.4.1.1 MRP

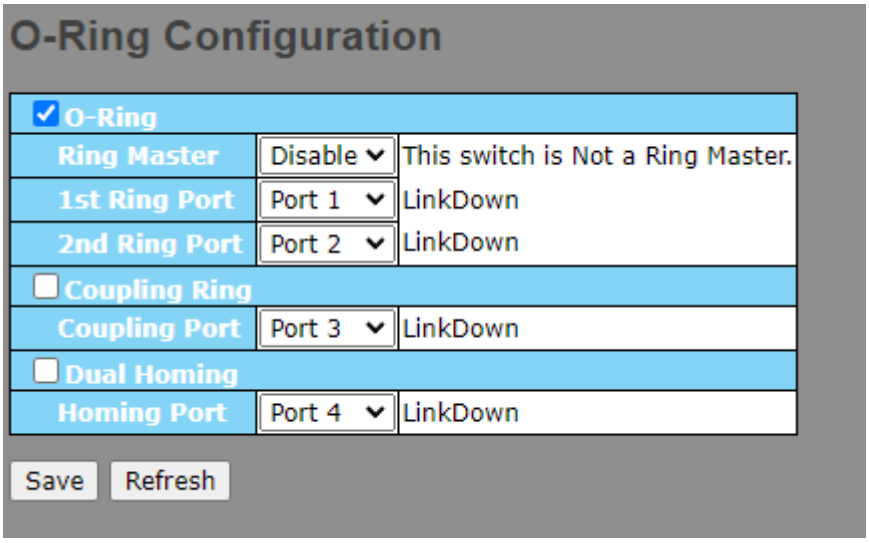
MRP (Media Redundancy Protocol) is an industry standard for high-availability Ethernet networks. MRP allowing Ethernet switches in ring configuration to recover from failure rapidly to ensure seamless data transmission. A MRP ring (IEC 62439) can support up to 50 devices and will enable a back-up link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



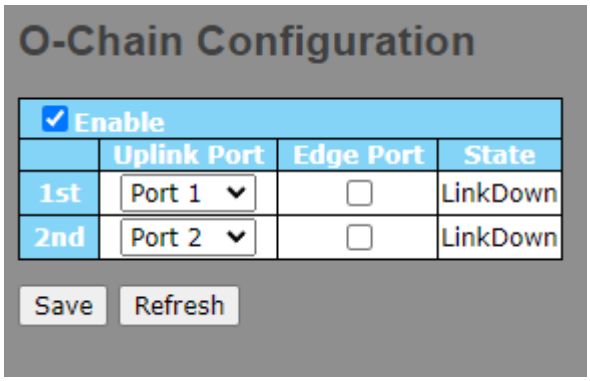
The following table describes the labels in this screen.

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.

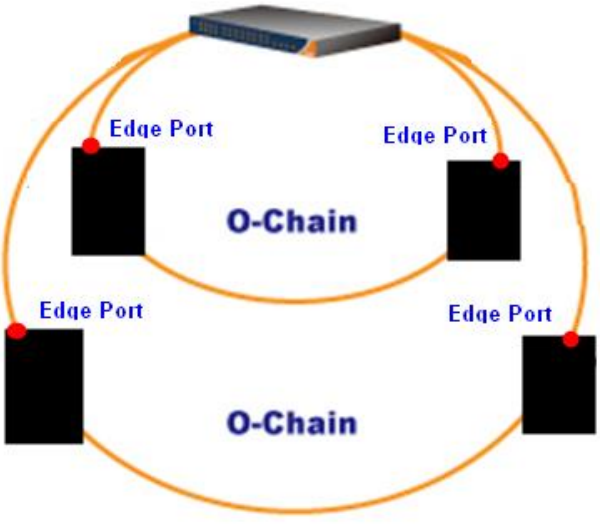
Note: We don't suggest you to set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load.

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.



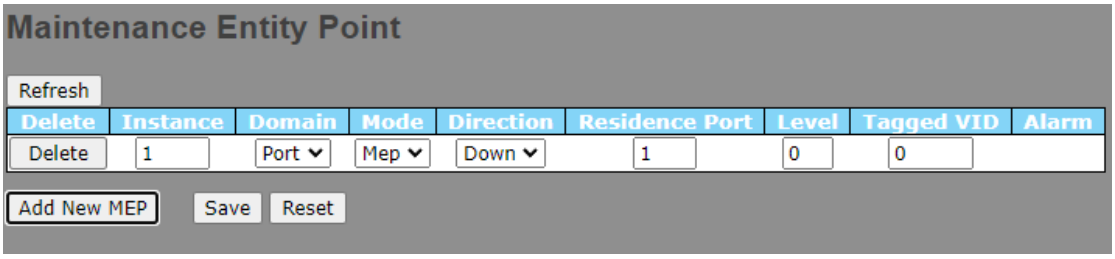
Label	Description
Enable	Enabling the O-Chain function
1st Ring Port	Choosing the port which connect to the ring
2nd Ring Port	Choosing the port which connect to the ring
Edge Port	In the O-Chain application, the head and tail of two Switch Port, must start the Edge,MAC smaller Switch, Edge port will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



1.4.1.4 G.8032

1.4.1.4.1 MEP

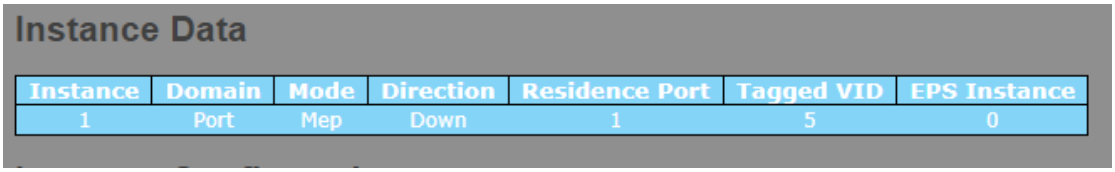
The Maintenance Entity Point instances are configured here.



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. **Esp:** Future use **Evc:** This is a MEP in the EVC Domain. 'Flow Instance' is a EVC **Mpls:** Future use
Mode	**MEP:** This is a Maintenance Entity End Point. **MIP:** This is a Maintenance Entity Intermediate Point.
Direction	**Ingress:** This is a Ingress (down) MEP - monitoring ingress traffic on 'Residence Port'. **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.
Tagged VID	**Port MEP:** An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.
Alarm	There is an active alarm on the MEP.

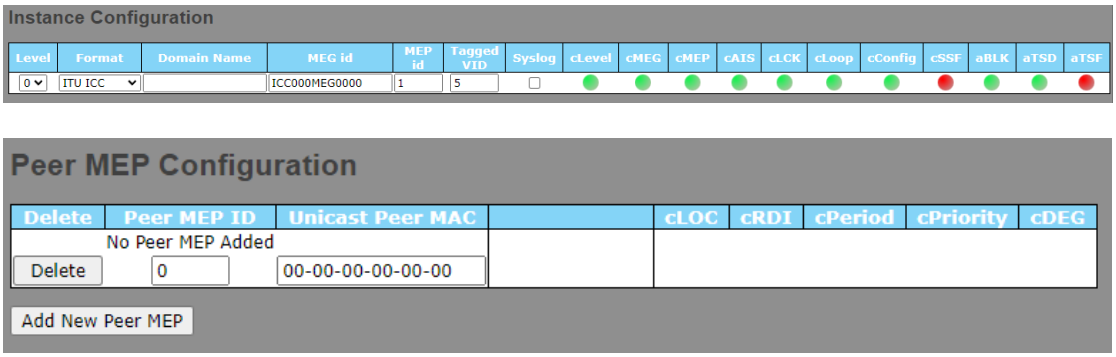
MEP Configuration –Instance Data

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



Label	Description
MEP Instance	MEP Instance
Domain	Show domain info .
Mode	Show mode info
Direction	Show direction info .
Residence Port	Show residence port info
Tagged VID	Show the MEP Tagged VID Value .

MEP Configuration –Instance Data

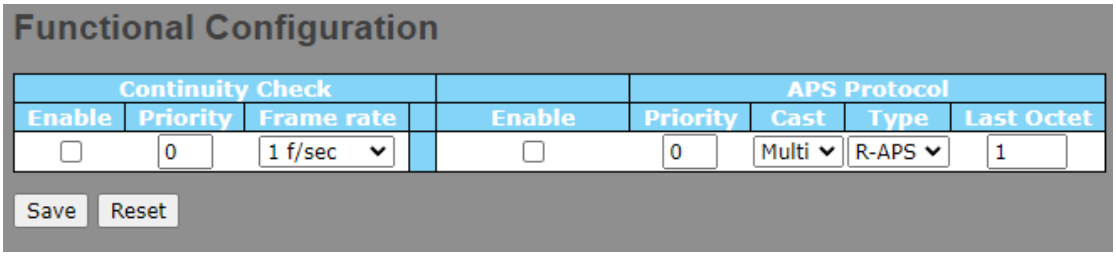


Label	Description
Level	See help on MEP create WEB.
Format	This is the configuration of the two possible Maintenance Association Identifier formats. **ITU ICC:** This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char. **IEEE String:** This is defined by IEEE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

	Name' is not used. 'MEG id' must be max. 15 char.
Domain Name	This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char.
MEG Id	This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be max 16 char.
MEP Id	This value will become the transmitted two byte CCM MEP ID.
Tagged VID	This value will be the VID of a TAG added to the OAM PDU.
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

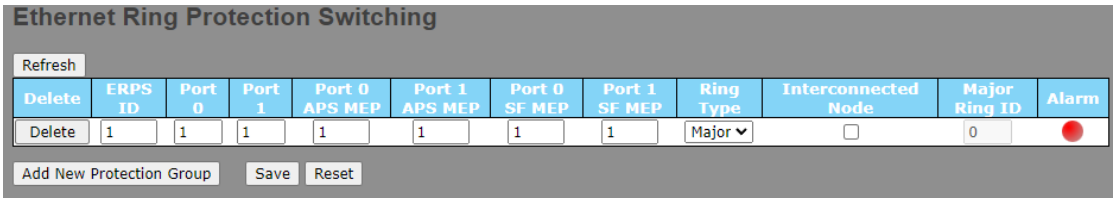


Label	Description
	Continuity Check
Enable	Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.
Priority	The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement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

	CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.
APS Protocol	
Enable	Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.
Priority	The priority to be inserted as PCP bits in TAG (if any).
Cast	Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.
Type	R-APS: APS PDU is transmitted as R-APS - this is for ERPS. L-APS: APS PDU is transmitted as L-APS - this is for ELPS.
Last Octet	This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) 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.

1.4.1.4.2 ERPS

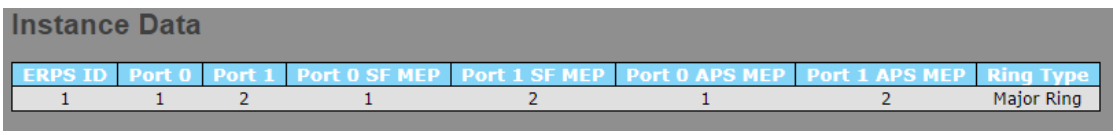
The Ethernet Ring Protection Switch instances are configured here.



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

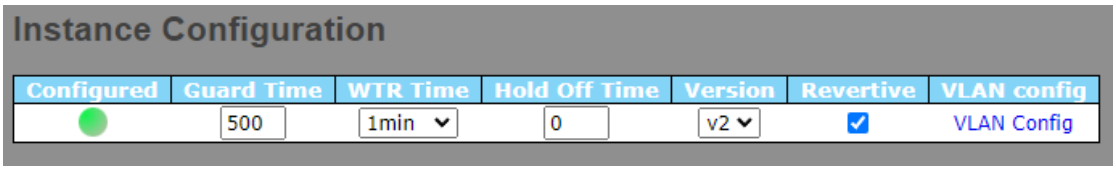
Port 0	This will create a Port 0 of the switch in the ring.
Port 1	This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this 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.

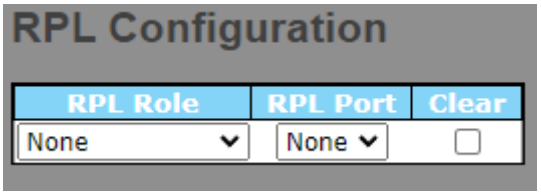
ERPS Configuration-Instance Configuration



Label	Description
Configured	Red: This ERPS is only created and has not yet been configured - is not active. 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. 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. The range of the hold off timer is 0 to 10 seconds in steps of 100 ms
Version	ERPS Protocol Version - v1 or v2

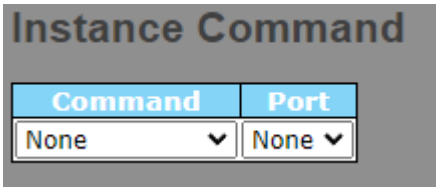
Revertive	In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL. In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.
VLAN config	VLAN configuration of the Protection Group. Click on the "VLAN Config" link to 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.

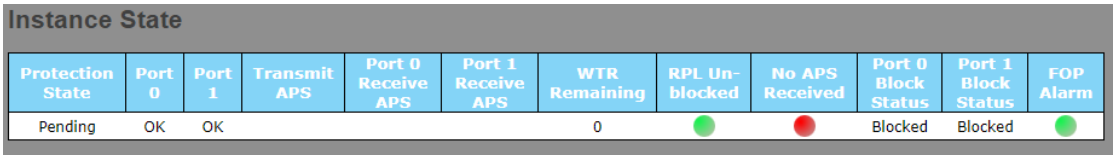
ERPS Configuration- Instance Command



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

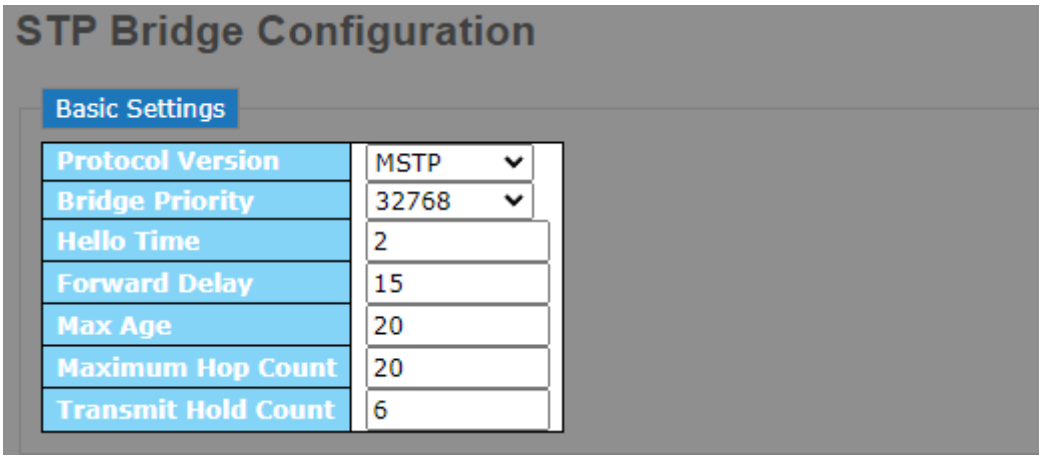


Label	Description
Protection State	ERPS state according to State Transition Tables in G.8032.
Port 0	OK: State of East port is ok SF: State of East port is Signal Fail
Port 1	OK: State of West port is ok SF: State of West port is Signal Fail
Transmit APS	The transmitted APS according to State Transition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

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.



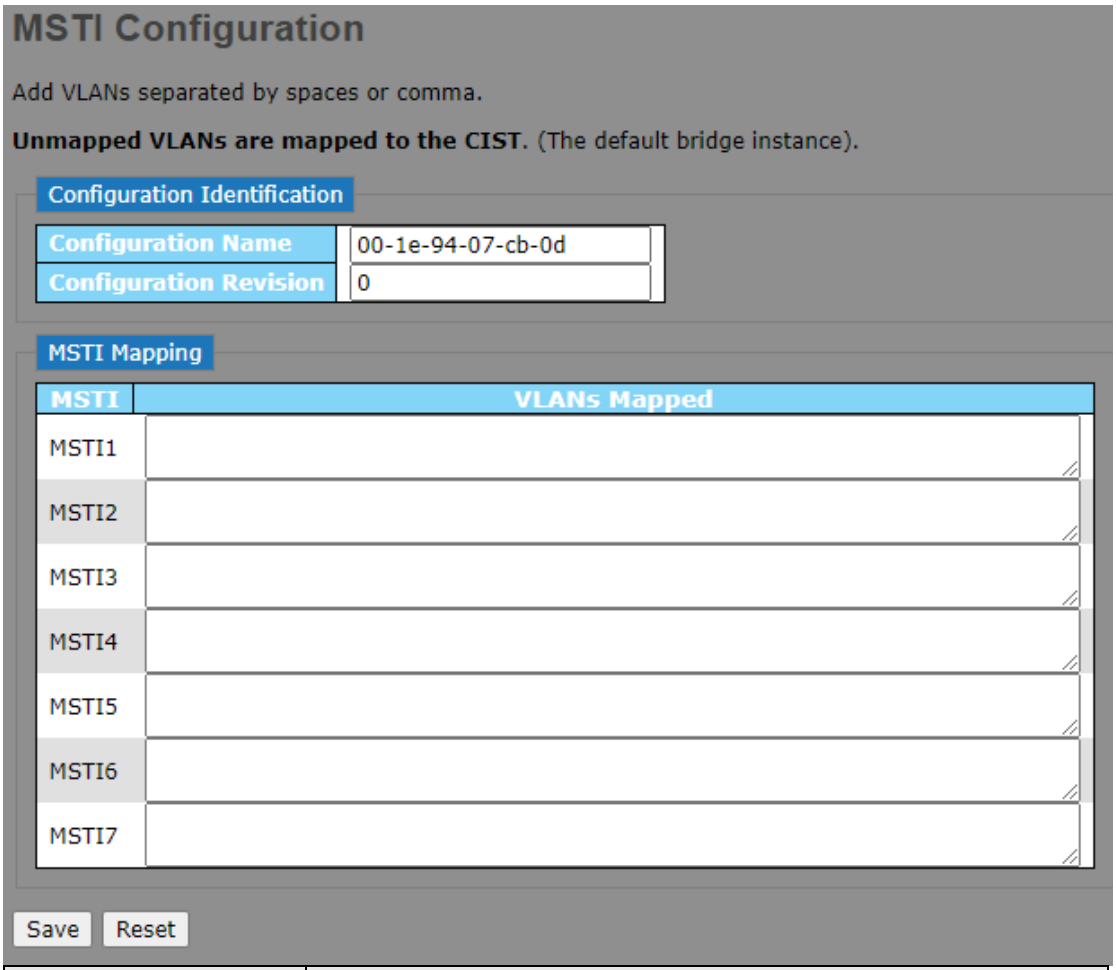
Label	Description
Protocol Version	The STP protocol version setting. Valid values are STP, RSTP and MSTP.
Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
Max Age	The maximum 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.

Advanced Settings

Label	Description
Edge Port BPDU Filtering	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
Edge Port BPDU Guard	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
Port Error Recovery	Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
Port Error Recovery Timeout	The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

MSTI Mapping

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

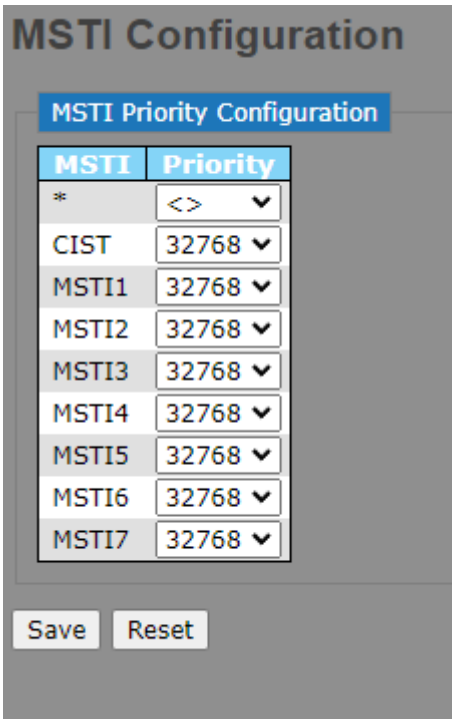


Label	Description
Configuration Name	The name identifiying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters.
Configuration Revision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

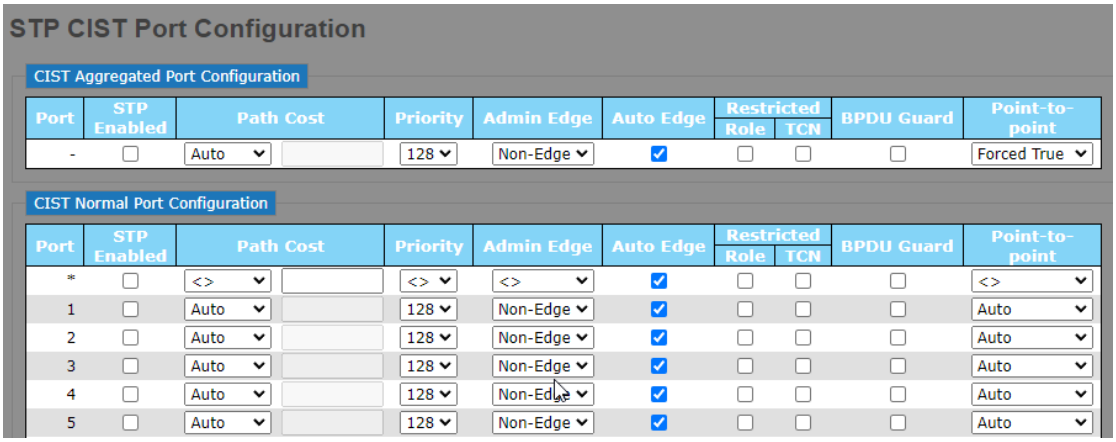
This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



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.

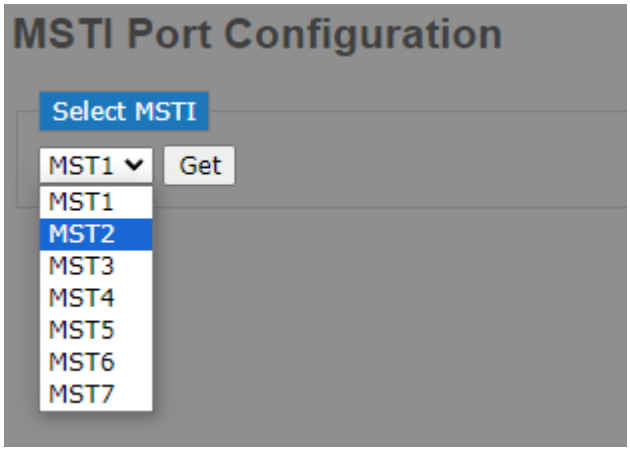


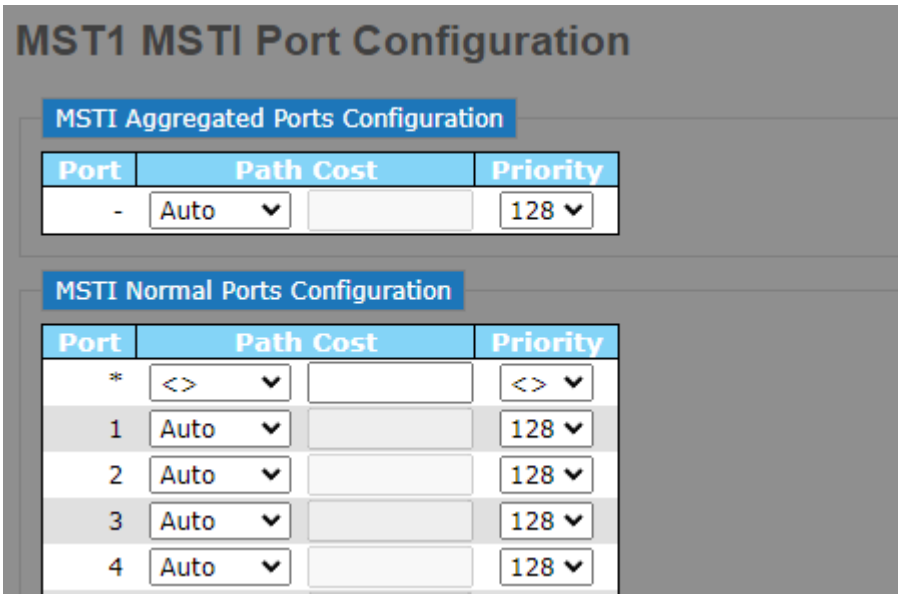
Label	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended 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.





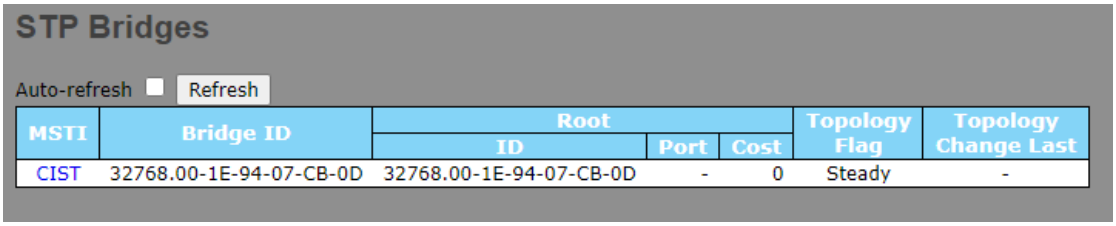
Label	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined 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.

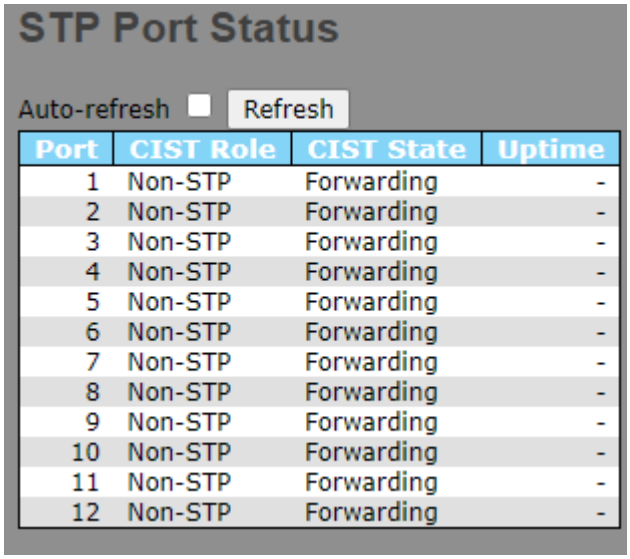
The displayed table contains a row for each STP bridge instance, where the column displays the following information:



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

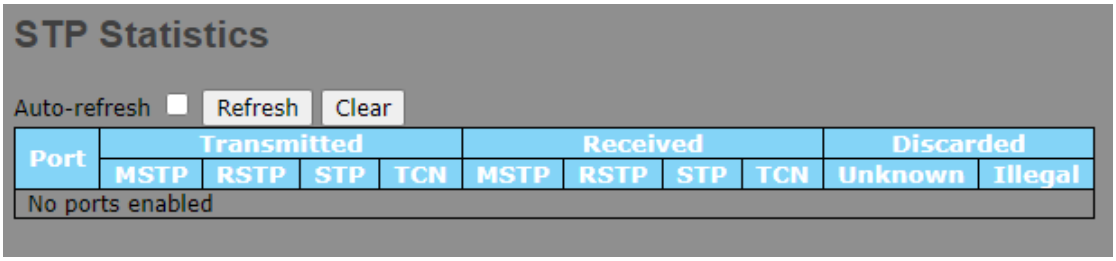
This page displays the STP CIST port status for port physical ports in the currently selected switch.



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

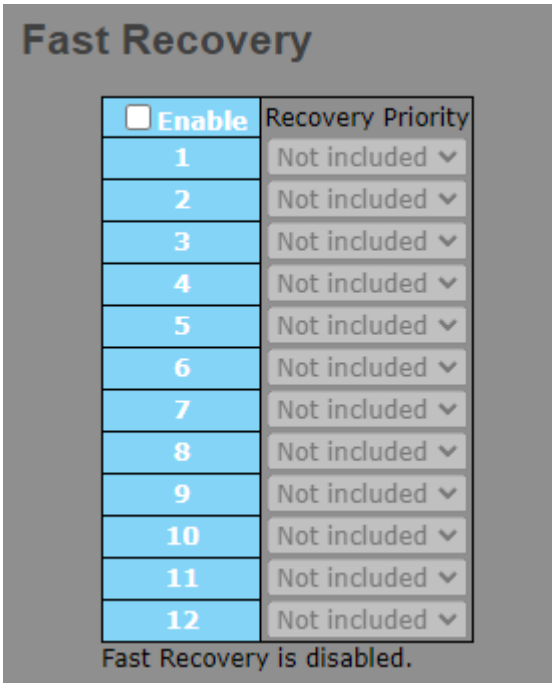
This page displays the RSTP port statistics counters for bridge ports in the currently selected switch.



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.

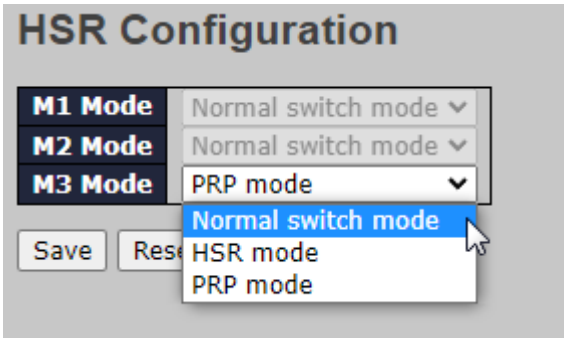
Label	Description
Active	Activate the fast recovery mode.
port	Port can be configured as 12 priorities. Only the port with highest priority will be the active port. 1st Priority is the highest.
Apply	Click "**Apply**" to activate the configurations.

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 .

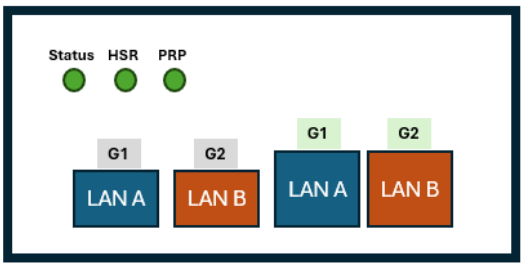
Will can select the module work mode

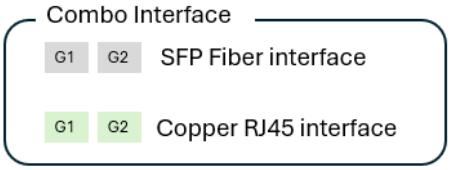


Label	Description
Normal Switch Mode	The module G1/G2 Port = Normal Switch port .
PRP Mode	The module G1/G2 Port will run PRP .
HSR Mode	The module G1/G2 Port will run HSR

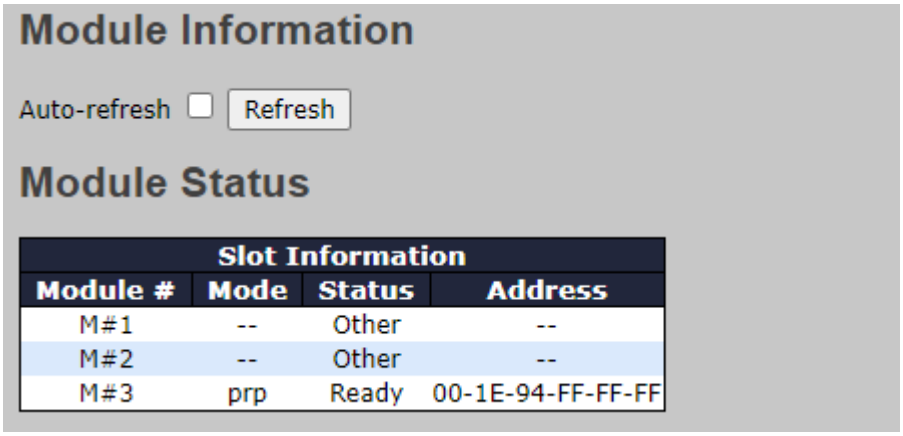
Module Information

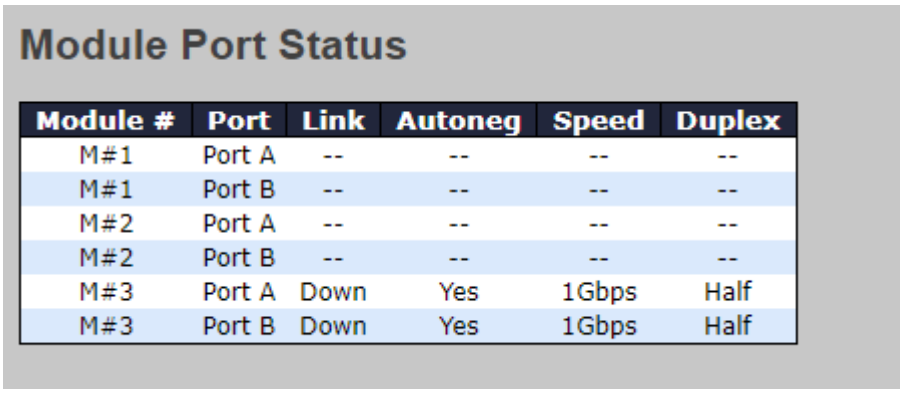
Users can choose between FIBER interface and COPPER interface.





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





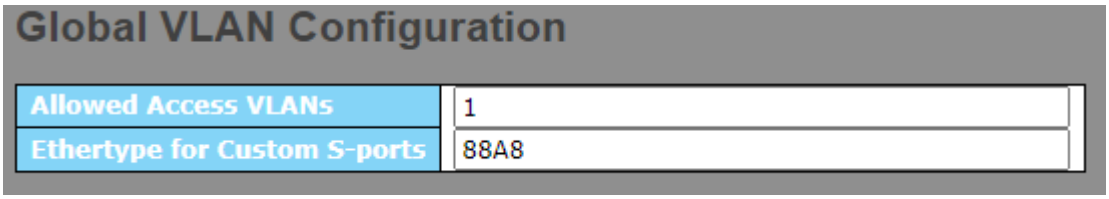
Label	Description
Module Status	
Mode	Show Module status (None / PRP / HSR)
Status	Other = no module connected Ready = Module connect and ready .
Address	Show HSR(PRP) Module MAC Address (not is switch MAC)
Module Port Status	
Link	Show Link status (Up / Down)
Autonego	Show Auto-negotiation status
Speed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

1.5 VLAN

1.5.1 VLAN Membership

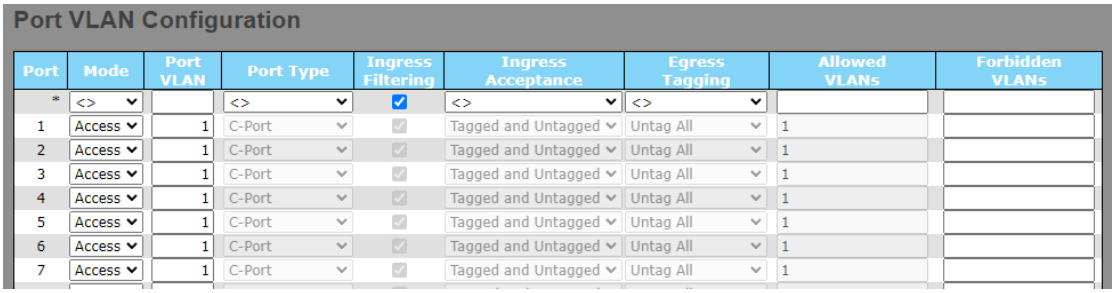
A VLAN is a group of end devices with a common set of requirements, independent of physical location. With the same attributes as a physical LAN, VLANs enable you to group end devices even if they are not located physically on the same LAN segment. By splitting up a network into sets of VLANs, assigning 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. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: **1,10-13,200,300**. Spaces are allowed in between the delimiters.
Ethertype for Custom S-ports	This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration



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. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied. **Access:** Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics: • Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1 • Accepts untagged and C-tagged frames • Discards all frames not classified to the Access VLAN • On egress all frames are transmitted untagged **Trunk:** Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics: • By default, a trunk port is member of all VLANs (1-4095)

	• The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs • Frames classified to a VLAN that the port is not a member of are discarded • By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress • Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress **Hybrid:** Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities: • Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware • Ingress filtering can be controlled • Ingress acceptance of frames and configuration of egress tagging can be configured independently
Port VLAN	Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1. On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.
Port Type	Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts

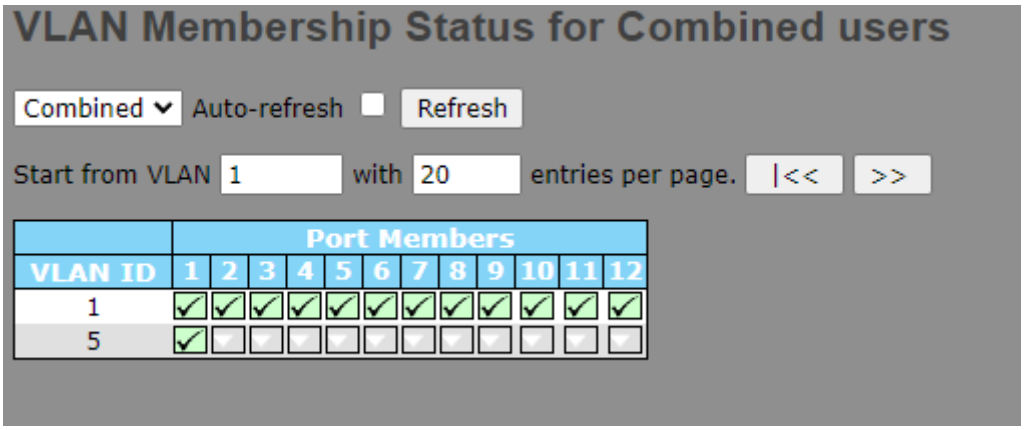
	on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required. **Unaware:** On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress. **C-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. **S-Port:** On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. If frames must be tagged on egress, they will be tagged with an S-tag. **S-Custom-Port:** On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. If frames must be tagged on egress, they will be tagged with the custom S-tag.
Ingress Filtering	Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.

	If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.
Ingress Acceptance	Hybrid ports allow for changing the type of frames that are accepted on ingress. **Tagged and Untagged** Both tagged and untagged frames are accepted. See Port Type for a description of when a frame is considered tagged. **Tagged Only** Only frames tagged with the corresponding Port Type tag are accepted on ingress. **Untagged Only** Only untagged frames are accepted on ingress. See Port 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. **Untag Port VLAN** Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. **Tag All** All frames, whether classified to the Port VLAN or not, are transmitted with a tag. **Untag All** All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.
Allowed VLANs	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to **1-4095**. The field may be left empty, which means that the port will not become member of any VLANs
Forbidden VLANs	A port may be configured to never become member of one or more VLANs. This is particularly useful when dynamic VLAN

	protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.

1.5.2 Membership Status

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

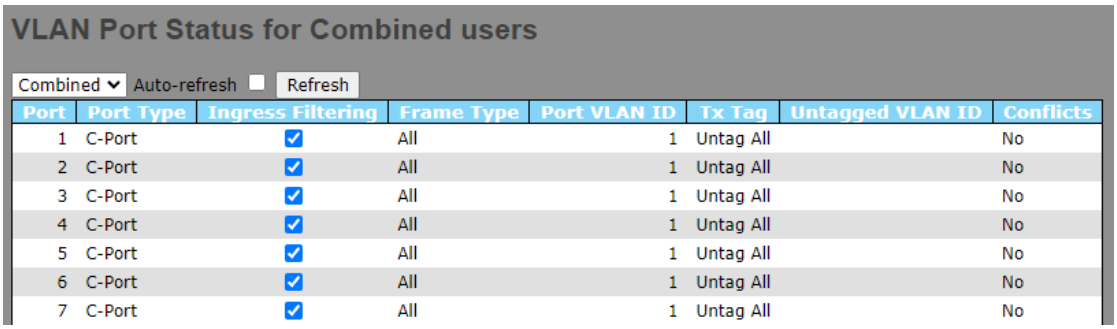


Label	Description
VLAN User	Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware
VLAN ID	VLAN ID for which the Port members are displayed.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. If a port is included in a VLAN, the following image will be displayed: ✓. If a port is in the forbidden port list, the following image will be displayed: ✕. If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed: ✕. The

	port will not be a member of the VLAN in this case.

1.5.3 Port Status

This page provides VLAN Port Status



Label	Description
VLAN User	Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware. 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. The field is empty if not overridden by the selected user.
Ingress Filtering	Shows whether a given user wants ingress filtering enabled or not. 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.

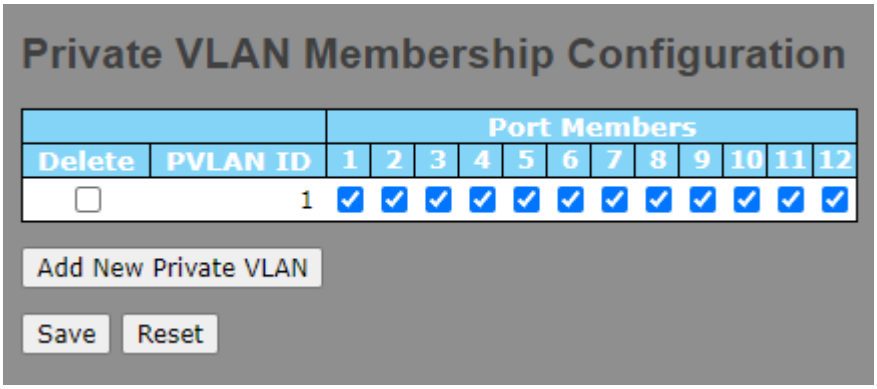
	The field is empty if not overridden by the selected user.
Port VLAN ID	Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user.
Tx Tag	Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port. 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. 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. 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. If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module. The "Combined" user reflects what is actually configured in hardware.

1.5.4 Private VLAN

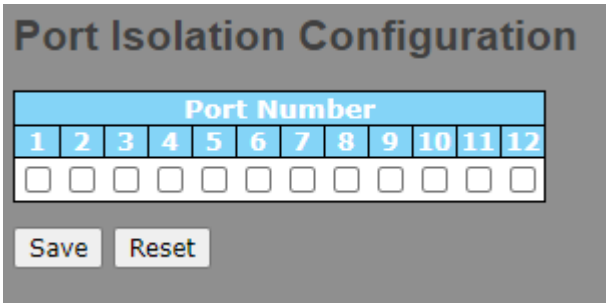
The private VLAN membership configuration for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that 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. The private VLAN is enabled when you click Save. The **Delete** button can be used to undo the addition of new private VLANs.



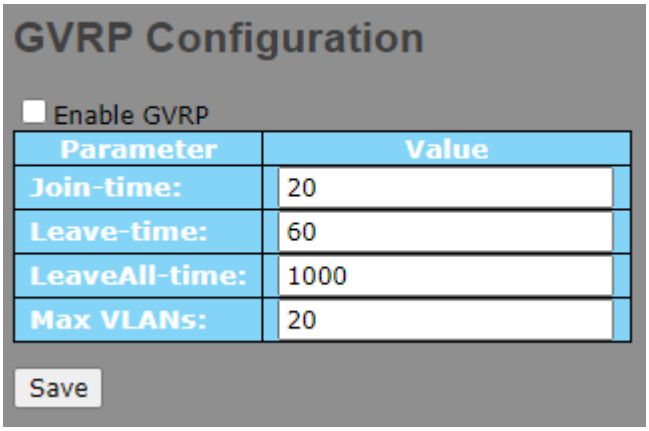
Label	Description
Port Members	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. By default, port isolation is disabled for all ports.

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.

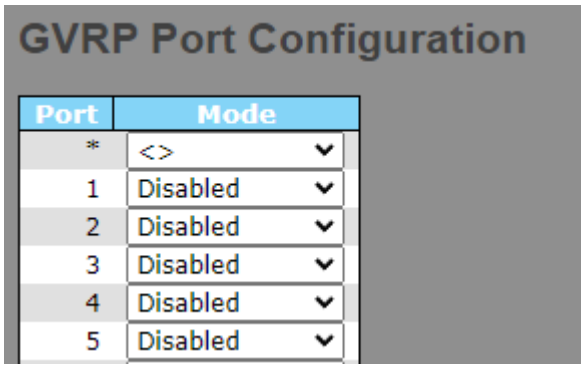


Label	Description
Enable GVRP globally	The GVRP feature is globally enabled by setting the check mark in the checkbox named Enable GVRP and pressing the Save button.

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. 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. 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

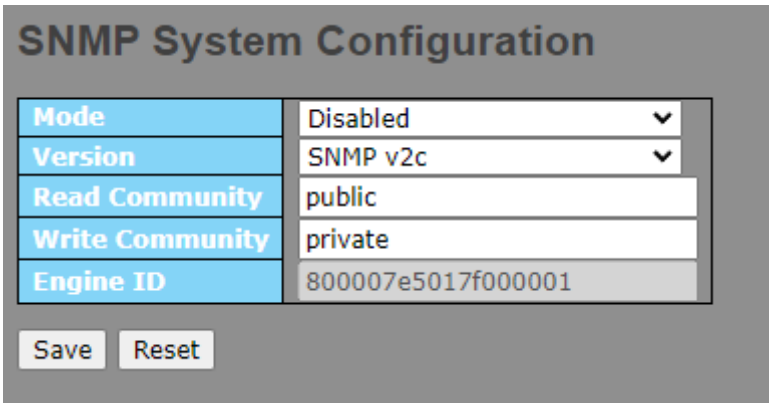
This page allows you to enable or disable a port for GVRP operation. This configuration can be performed either before or after GVRP is configured globally - the protocol operation will be the same.



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

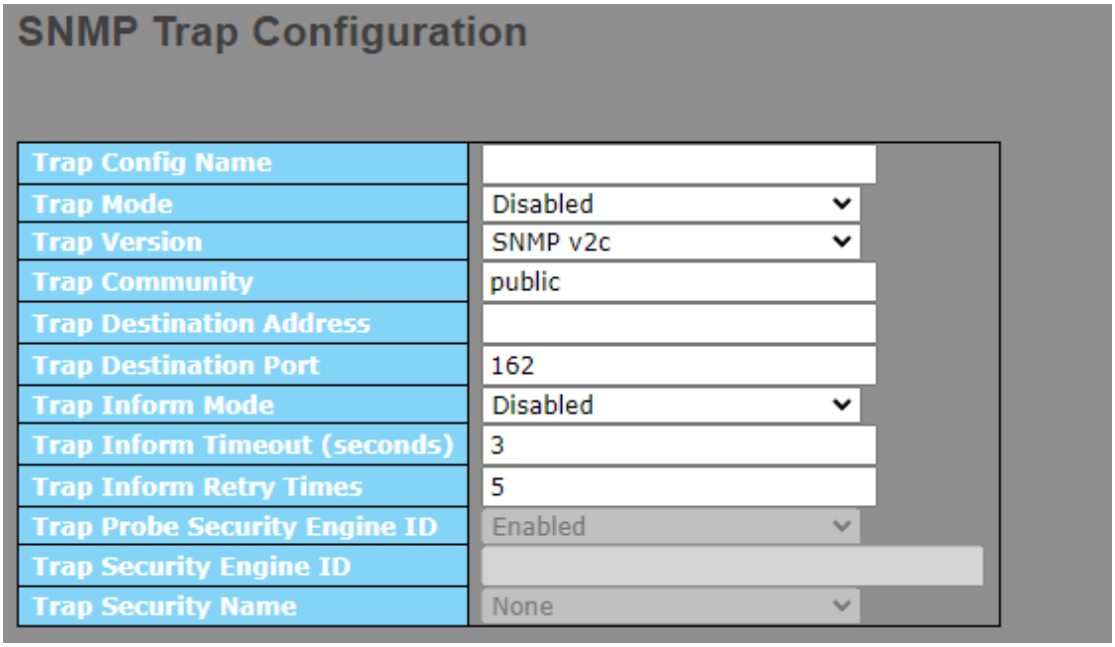
1.6.1 SNMP System Configurations



Label	Description
Mode	Indicates existing SNMP mode. Possible modes include: **Enabled**: enable SNMP mode **Disabled**: disable SNMP mode
Version	Indicates the supported SNMP version. Possible versions include: **SNMP v1**: supports SNMP version 1. **SNMP v2c**: supports SNMP version 2c. **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. 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. 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

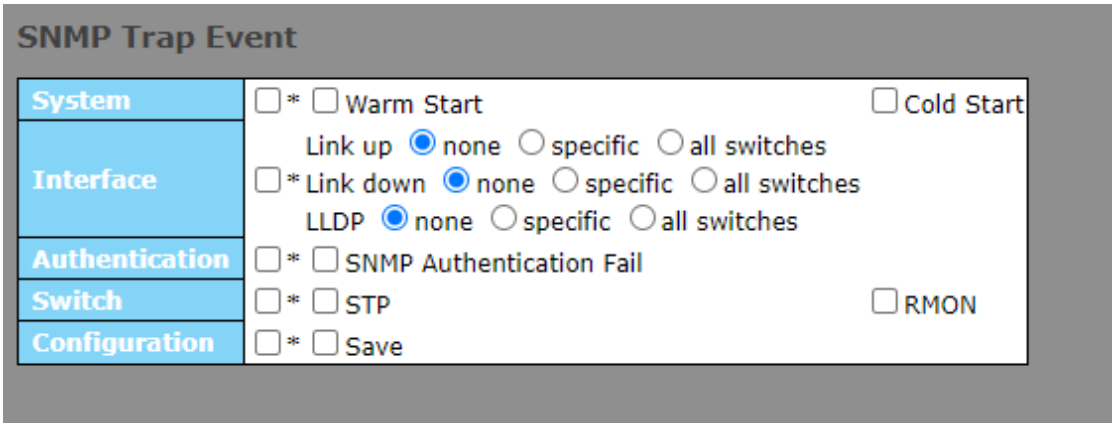
SNMP Trap Detailed Configuration



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: **Enabled**: enable SNMP trap mode **Disabled**: disable SNMP trap mode
Trap Version	Indicates the supported SNMP trap version. Possible versions include: **SNMP v1**: supports SNMP trap version 1 **SNMP v2c**: supports SNMP trap version 2c **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'). 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. 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: **Enabled**: enable SNMP trap inform mode **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: **Enabled**: Enable SNMP trap probe security engine ID mode of operation. **Disabled**: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

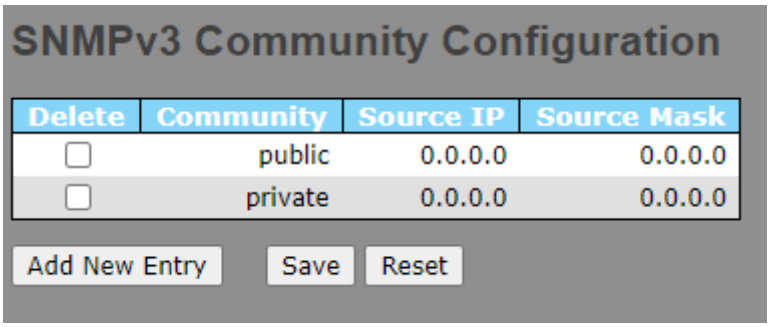
SNMP Trap Event



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

1.6.3 SNMP Community Configurations

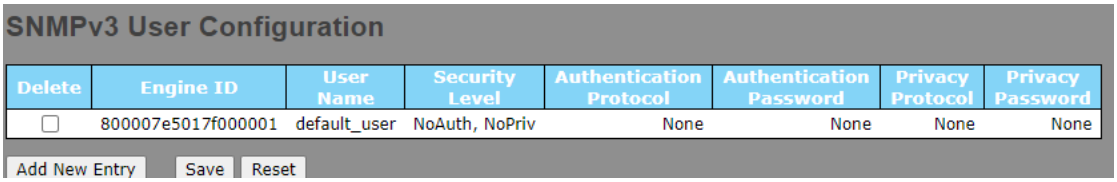
This page allows you to configure SNMPv3 community table. The entry index key is **Community**.



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**.



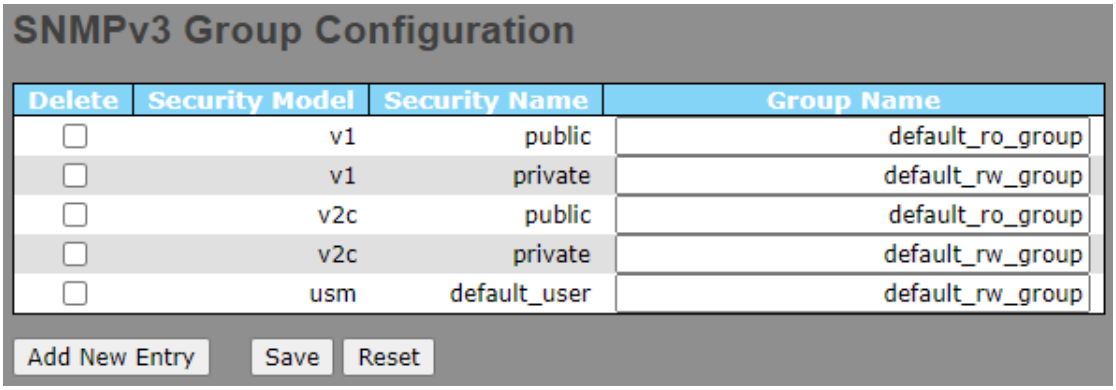
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The 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: **NoAuth, NoPriv**: no authentication and none privacy **Auth, NoPriv**: Authentication and no privacy **Auth, Priv**: Authentication and privacy 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: **None**: no authentication protocol **MD5**: an optional flag to indicate that this user is using MD5 authentication protocol **SHA**: an optional flag to indicate that this user is using SHA authentication protocol 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: **None**: no privacy protocol **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

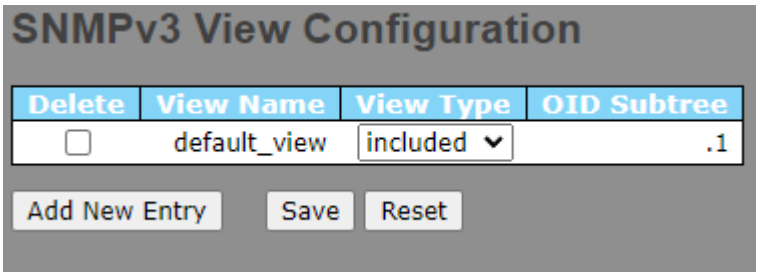
This page allows you to configure SNMPv3 group table. The entry index keys are **Security Model** and **Security Name**.



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: **v1**: Reserved for SNMPv1. **v2c**: Reserved for SNMPv2c. **usm**: User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and 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

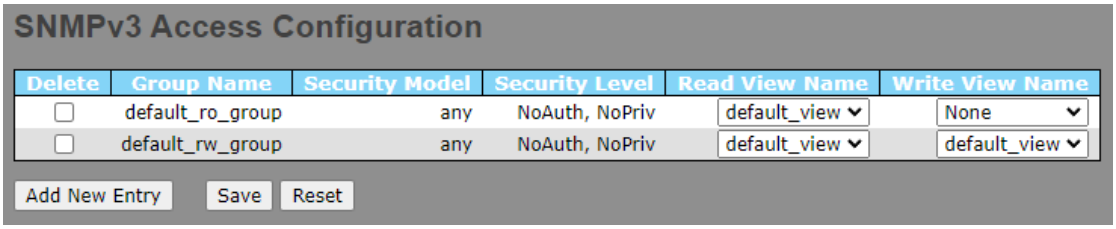
This page allows you to configure SNMPv3 view table. The entry index keys are **View Name** and **OID Subtree**.



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: **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. 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

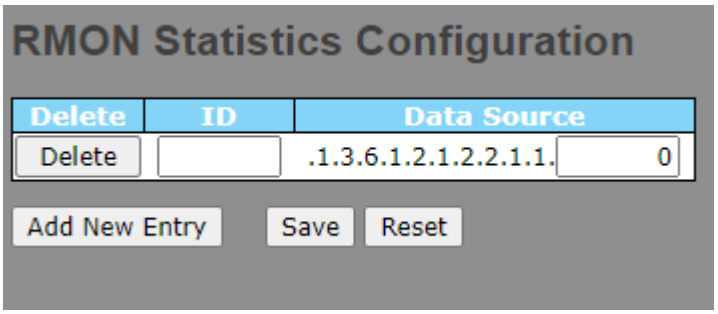
This page allows you to configure SNMPv3 access table. The entry index keys are **Group Name**, **Security Model**, and **Security Level**.



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: **any**: Accepted any security model (v1|v2c|usm).

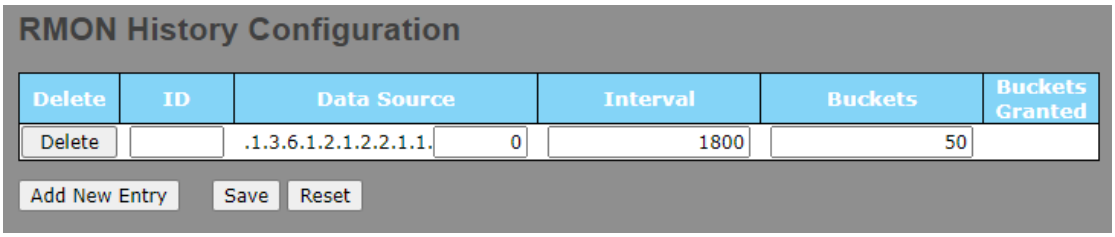
	v1: Reserved for SNMPv1. **v2c**: Reserved for SNMPv2c. **usm**: User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models include: **NoAuth, NoPriv**: no authentication and no privacy **Auth, NoPriv**: Authentication and no privacy **Auth, Priv**: Authentication and privacy
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and 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



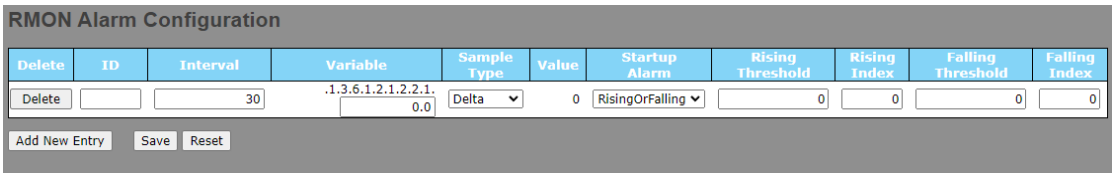
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example,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

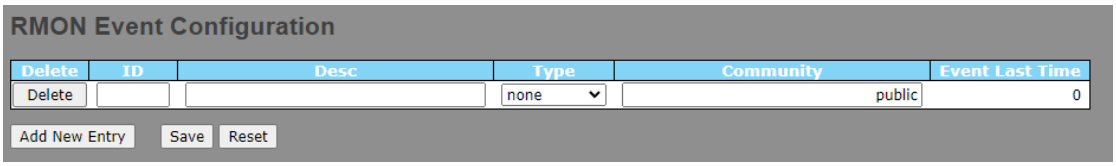


Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
Variable	Indicates the particular variable to be sampled, the possible variables are: **InOctets**: The total number of octets received on the interface, including framing characters. **InUcastPkts:** The number of uni-cast packets delivered to a higher-layer protocol.

	InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. **InDiscards**: The number of inbound packets that are discarded even the packets are normal. **InErrors**: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. **InUnknownProtos**: the number of the inbound packets that were discarded because of the unknown or un-support protocol. **OutOctets**: The number of octets transmitted out of the interface , including framing characters. **OutUcastPkts**: The number of uni-cast packets that request to transmit. **OutNUcastPkts**: The number of broad-cast and multi-cast packets that request to transmit. **OutDiscards**: The number of outbound packets that are discarded even the packets are normal. **OutErrors**: The number of outbound packets that could not be transmitted because of errors. **OutQLen**: The length of the output packet queue (in packets).
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: **Absolute**: Get the sample directly. **Delta**: Calculate the difference between samples (default).
Value	The value of the statistic during the last sampling period.
Startup Alarm	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: **Rising**Trigger alarm when the first value is larger than the rising threshold. **Falling**Trigger alarm when the first value is less than the falling threshold. **RisingOrFalling**Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
Rising Threshold	Rising threshold value (-2147483648-2147483647).
Rising Index	Rising event index (1-65535).
Falling Threshold	Falling threshold value (-2147483648-2147483647)

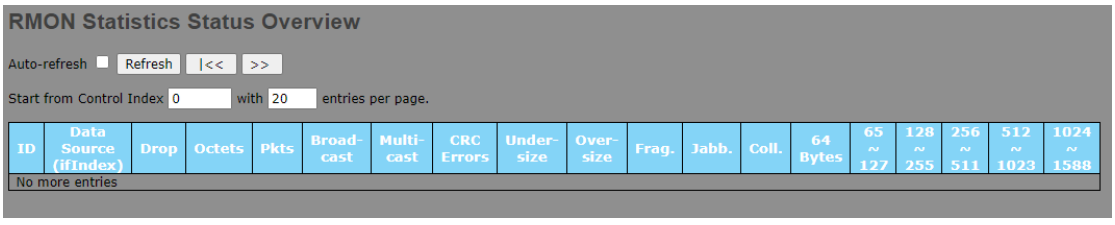
Falling Index	Falling event index (1-65535).

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: **none**: No SNMP log is created, no SNMP trap is sent. **log**: Create SNMP log entry when the event is triggered. **snmptrap**: Send SNMP trap when the event is triggered. **logandtrap**: Create SNMP log entry and sent SNMP trap when the event is triggered.
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.

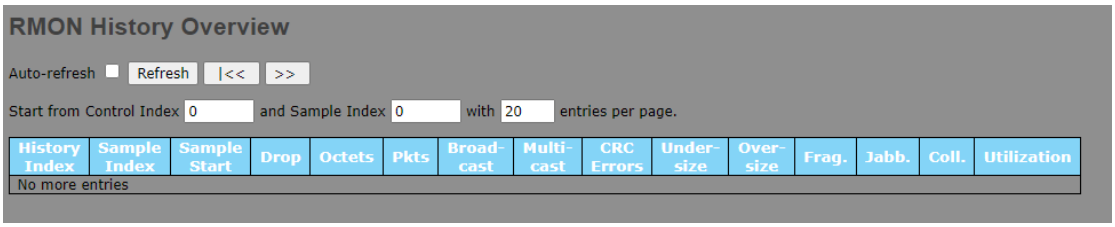
Statistics Stauts



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.

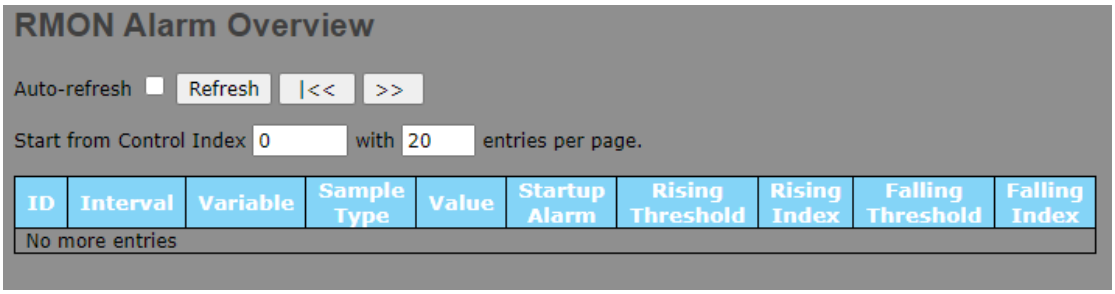
History Status



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

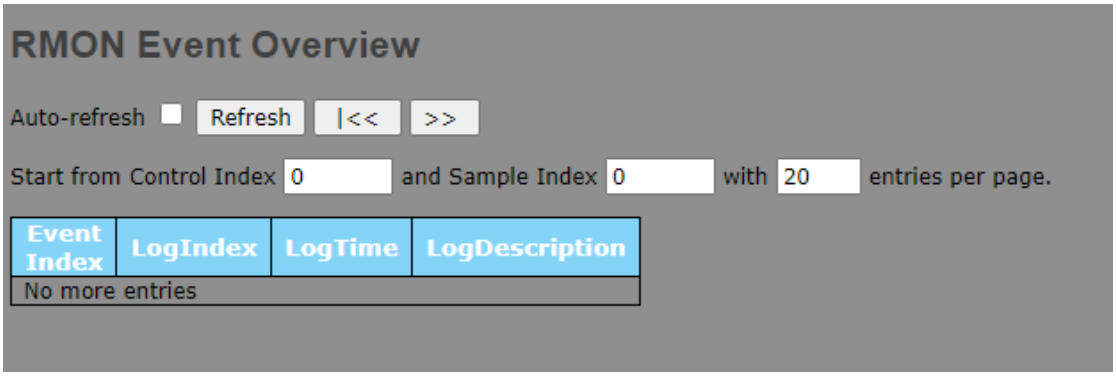
	this interface during this sampling interval, in hundredths of a percent.

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.

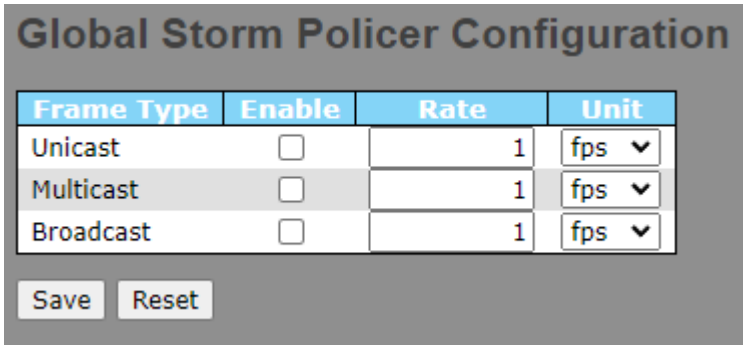
1.7 Traffic Prioritization

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.

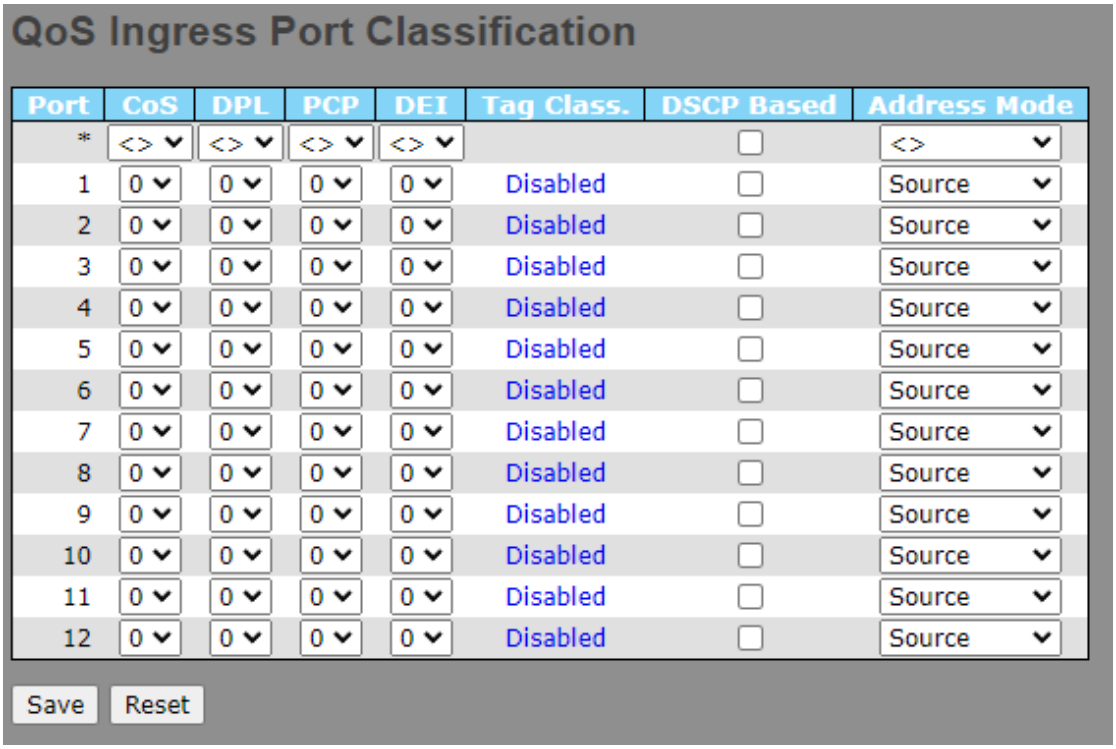
Note: frames sent to the CPU of the switch are always limited to approximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.



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. 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 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. 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. PCP value: 0 1 2 3 4 5 6 7 QoS class: 1 0 2 3 4 5 6 7 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.

	The classified QoS class can be overruled by a QCL entry. 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 All frames are classified to a DP level. 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. 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. The classified DP level can be overruled by a QCL entry.
PCP	Controls the default PCP value All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	Controls the default DEI value All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Tag Class	Shows the classification mode for tagged frames on this port **Disabled**: Use default QoS class and DP level for tagged frames **Enabled**: Use mapped versions of PCP and DEI for tagged frames Click on the mode to configure the mode and/or mapping Note: this setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN-unaware ports are always classified to the default QoS class and DP level.
DSCP Based	Click to enable DSCP Based QoS Ingress Port Classification

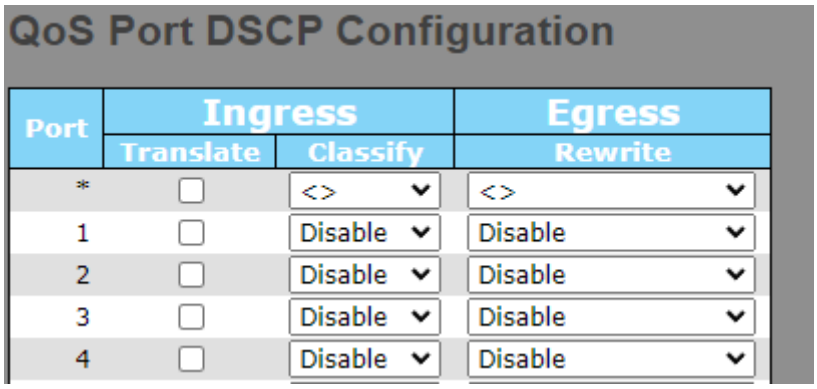
1.7.3 Port Tag Remaking

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 **Classified**: use classified PCP/DEI values **Default**: use default PCP/DEI values **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.

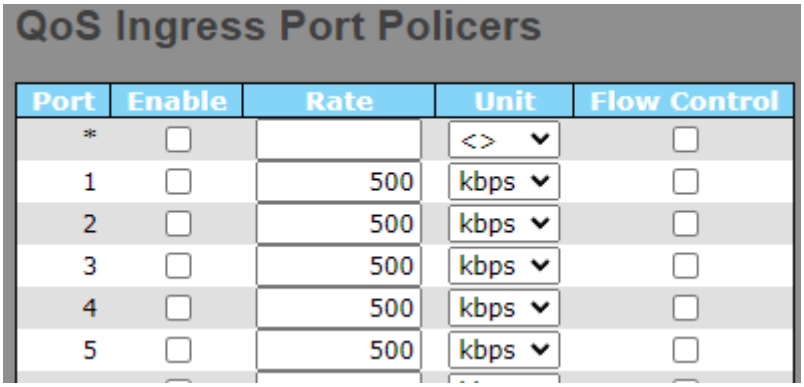


Label	Description
Port	Shows the list of ports for which you can configure DSCP Ingress and Egress settings.
Ingress	In **Ingress** settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: 1. **Translate**

	2. **Classify**
1. Translate	Check to enable ingress translation
2. Classify	Classification has 4 different values. Disable: no Ingress DSCP classification DSCP=0: classify if incoming (or translated if enabled) DSCP is 0. Selected: classify only selected DSCP whose classification is enabled as specified in **DSCP Translation** window for the specific DSCP. All: classify all DSCP
Egress	Port egress rewriting can be one of the following options: **Disable**: no Egress rewrite **Enable**: rewrite enabled without remapping **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. **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.

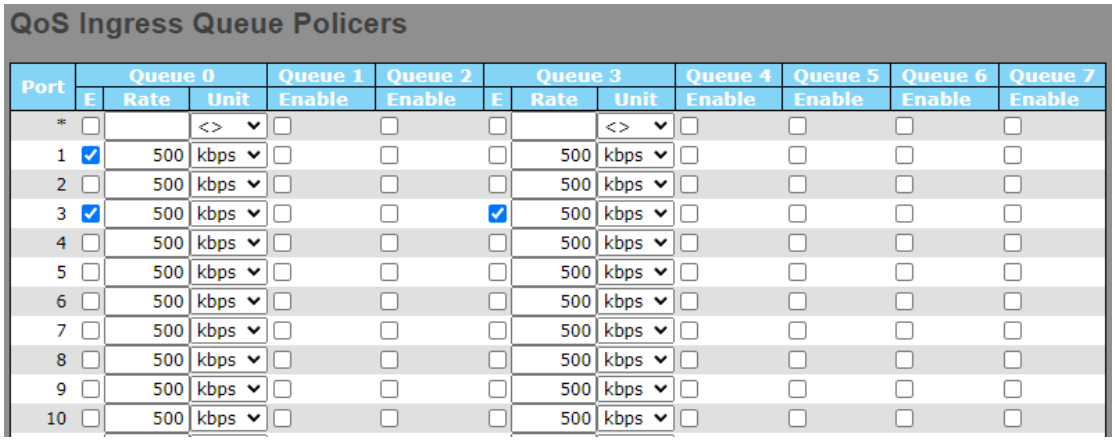


Label	Description

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.

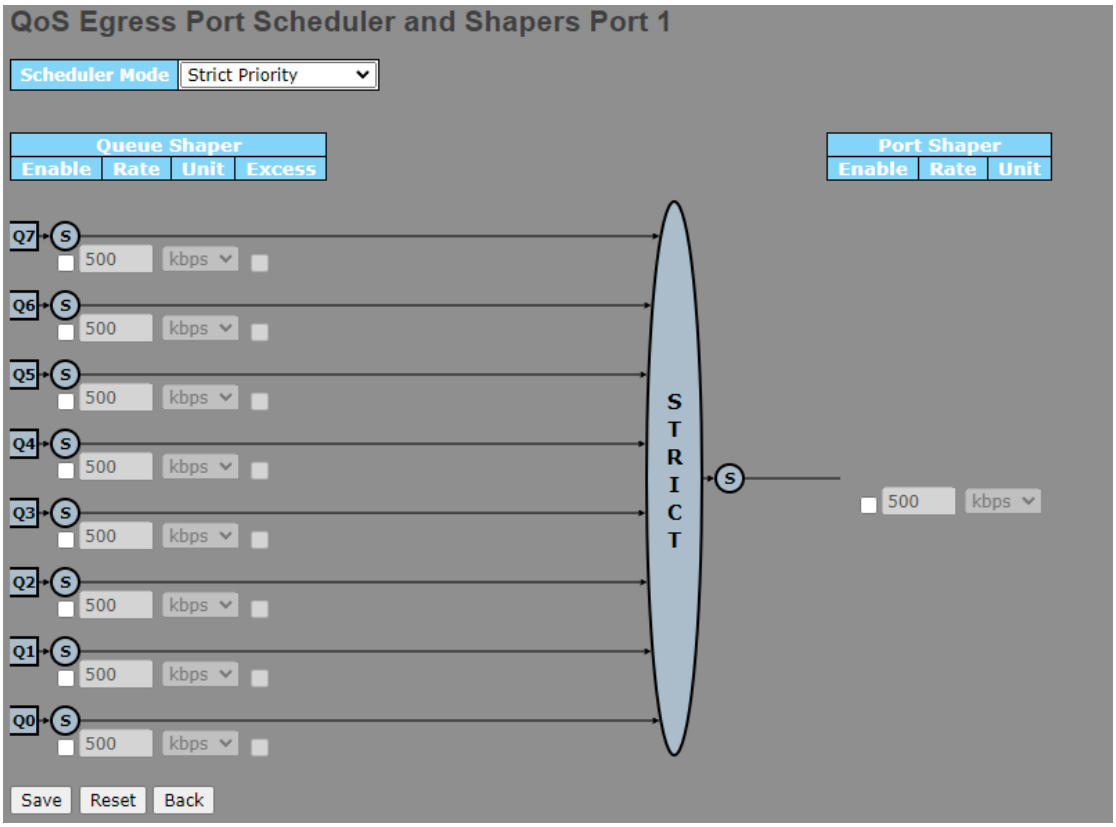


Label	Description
Port	The port number for which the configuration below applies.
Enable(E)	Check to enable queue policer for individual switch ports
Rate	Configures the rate of each queue policer. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and is restricted to 1 to 3300 when the **Unit** is **Mbps**. 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**. 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.

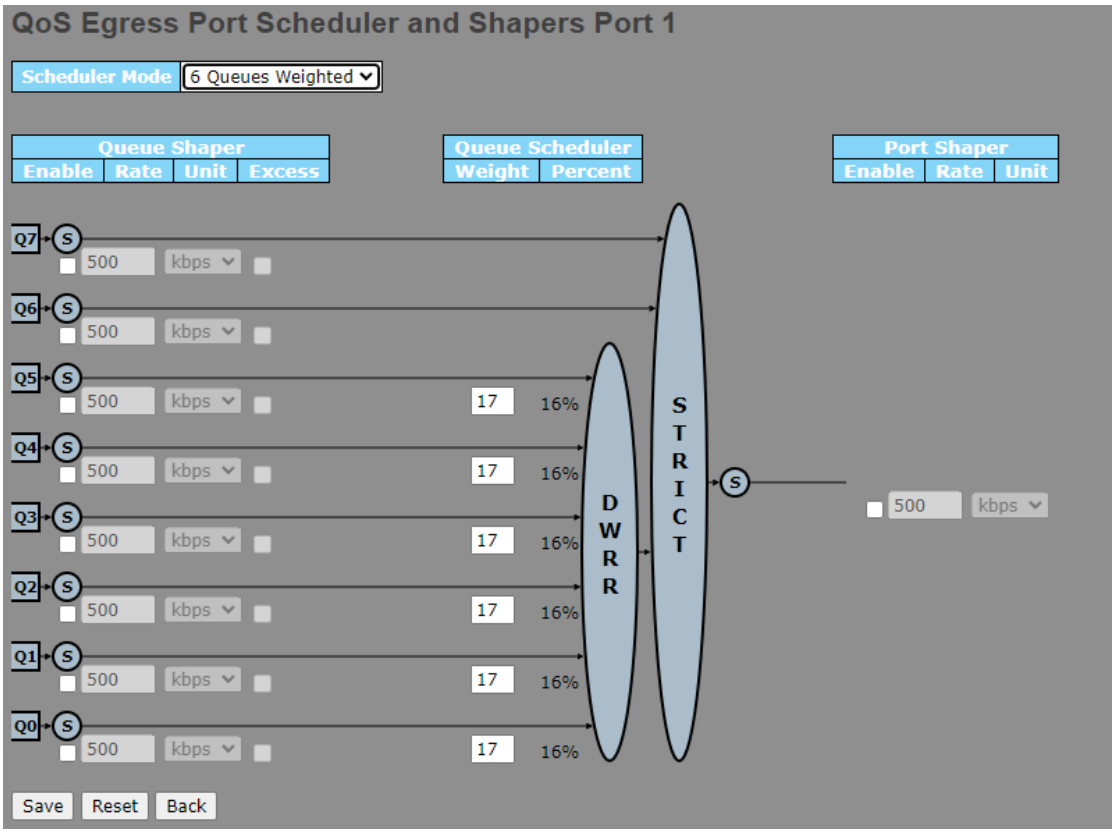
Strict Priority



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

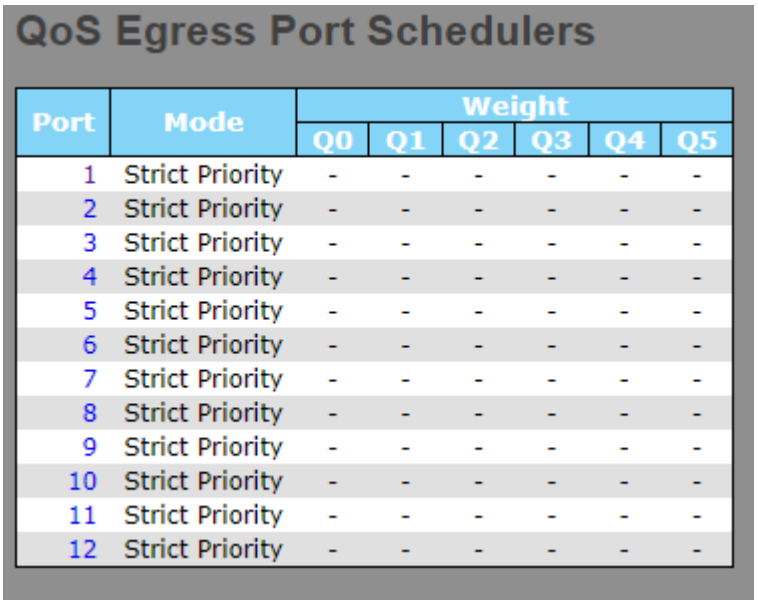


Label	Description
Scheduler Mode	Controls whether the scheduler mode is **Strict Priority** or **Weighted** on this switch port
Queue Shaper Enable	Check to enable queue shaper for individual switch ports
Queue Shaper Rate	Configures the rate of each queue shaper. The default value is **500**. This value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

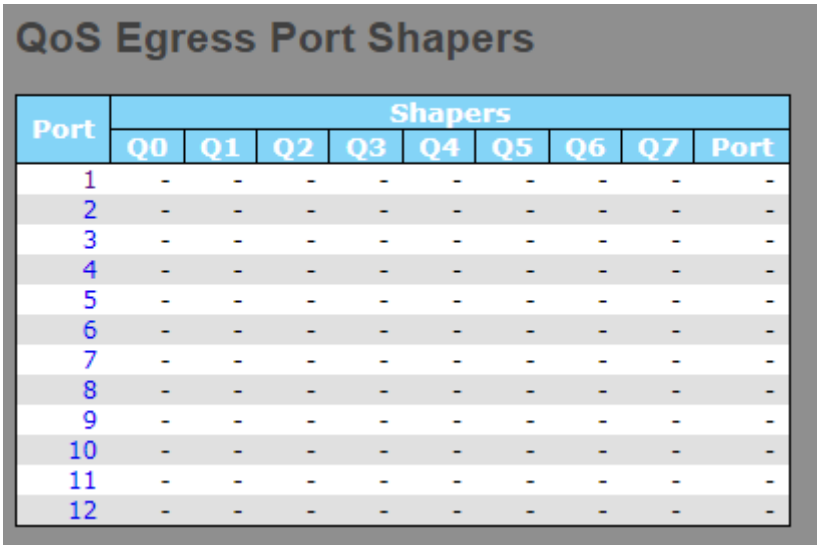


Label	Description
Port	The switch port number to which the following settings will be applied. Click on the port number to configure the schedulers
Mode	Shows the scheduling mode for this port

Qn	Shows the weight for this queue and port

1.7.9 Port Shaping

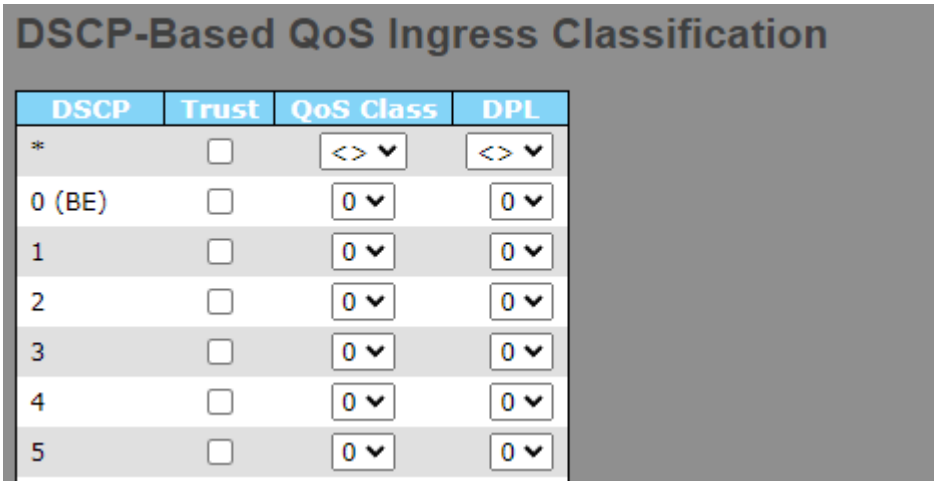
This page provides an overview of QoS Egress Port Shapers for all switch ports.



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

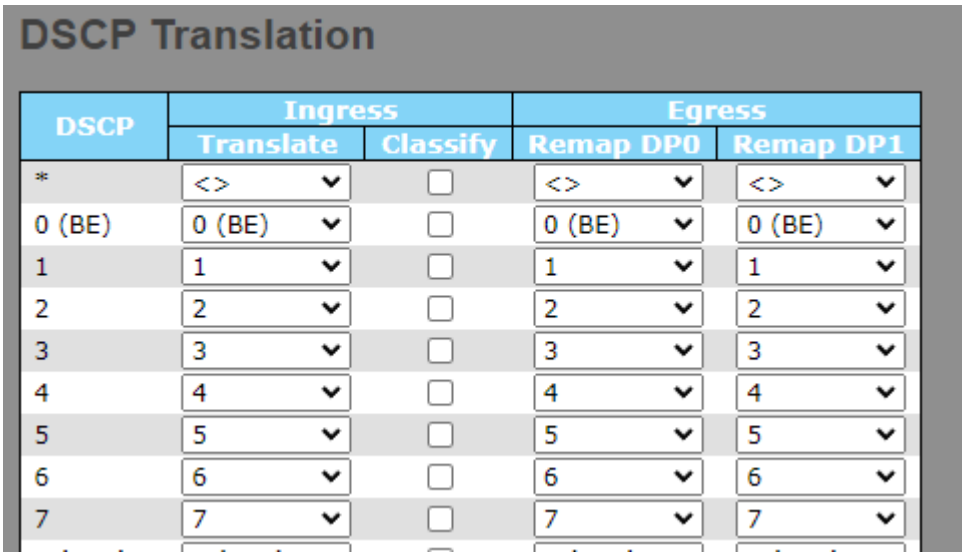
This page allows you to configure basic QoS DSCP-based QoS Ingress Classification settings for all switches.



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**.

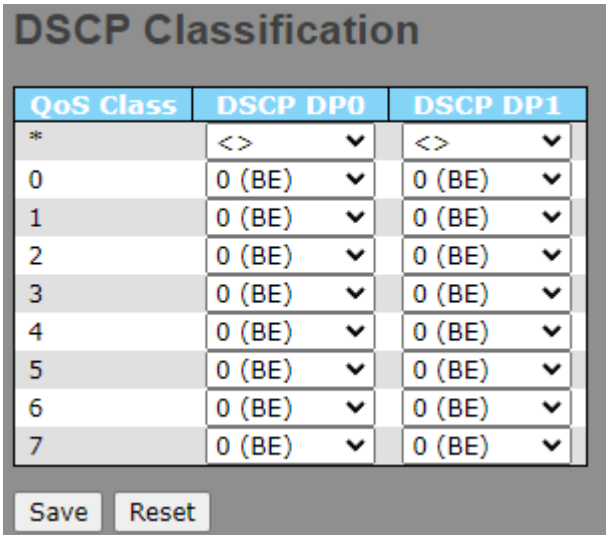


Label	Description
DSCP	Maximum number of supported DSCP values is 64 and valid DSCP value ranges from 0 to 63.
Ingress	Ingress DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation - 1. **Translate:** DSCP can be translated to any of (0-63) DSCP values. 2. **Classify:** check to enable ingress classification
Egress	Configurable engress parameters include;

	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. **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

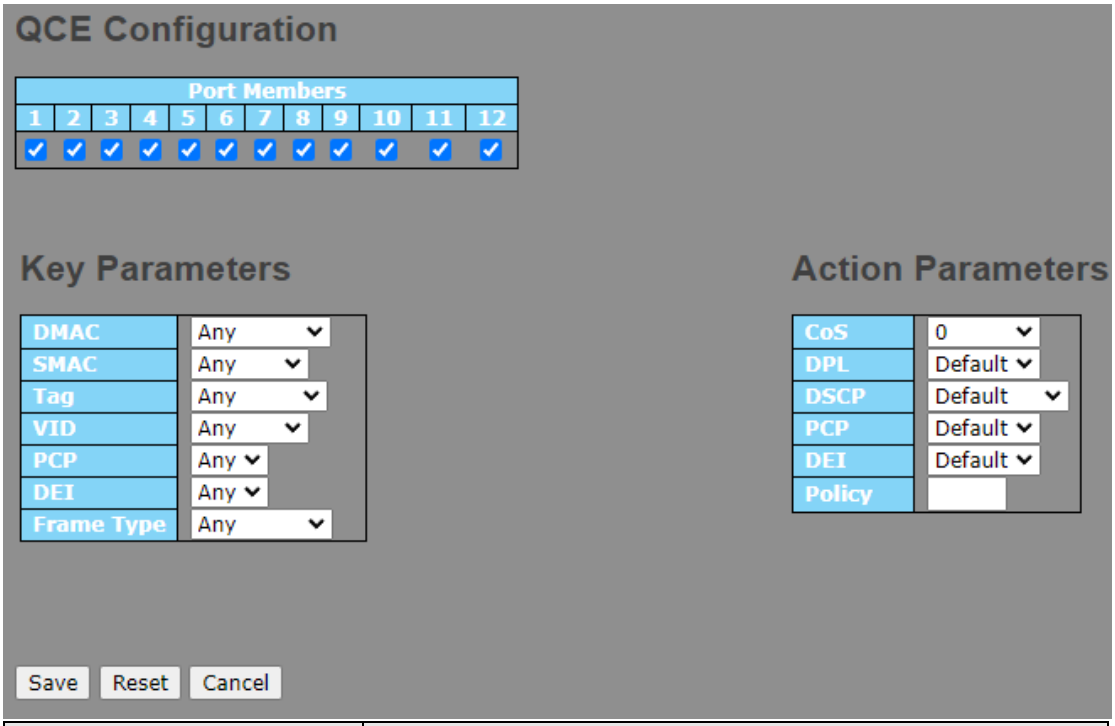
This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.



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



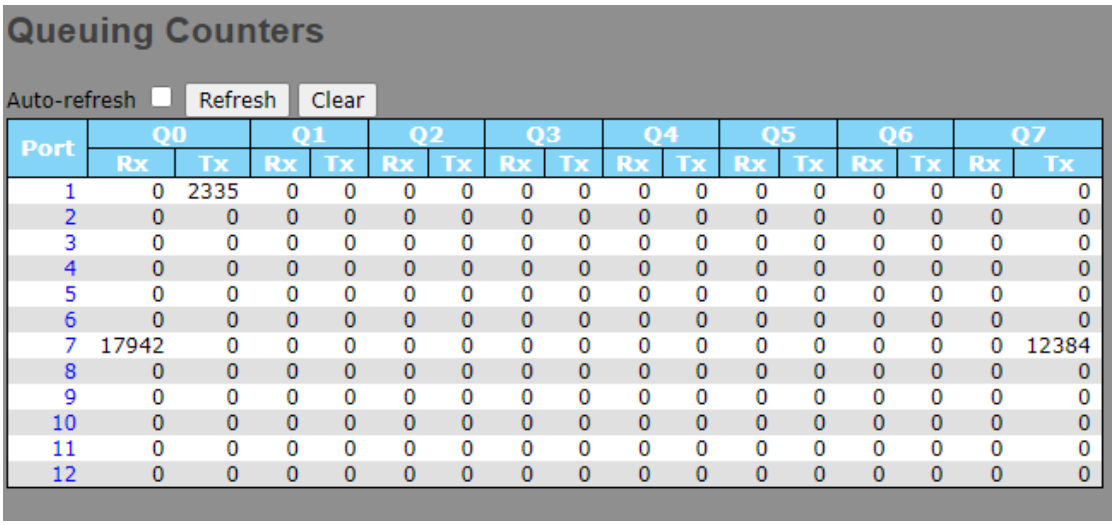
Label	Description
Port Members	Check to include the port in the QCL entry. By default, all ports are included.
Key Parameters	Key configurations include: **Tag**: value of tag, can be **Any**, **Untag** or **Tag**. **VID**: valid value of VLAN ID, can be any value from 1 to 4095 **Any**: user can enter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

	IPv6 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**. DSAP Address: valid DSAP (Destination Service Access Point) values can range from 0x00 to 0xFF or **Any**. The default value is **Any**. 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** 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. 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. IP Fragment: Ipv4 frame fragmented options include **'yes'**, **'no'**, and **'any'**. Sport Source TCP/UDP Port: (0-65535) or **Any**, specific value or port range applicable for IP protocol UDP/TCP 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** Source IP IPv6 source address: (a.b.c.d) or **Any**, 32 LS bits 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. Sport Source TCP/UDP port: (0-65535) or **Any**, specific

	value or port range applicable for IP protocol UDP/TCP 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** Valid Drop Precedence Level value can be (0-1) or **Default**. Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or **Default**. Default means that the default classified value is not modified by this QCE.

1.7.14 QoS Statistics

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

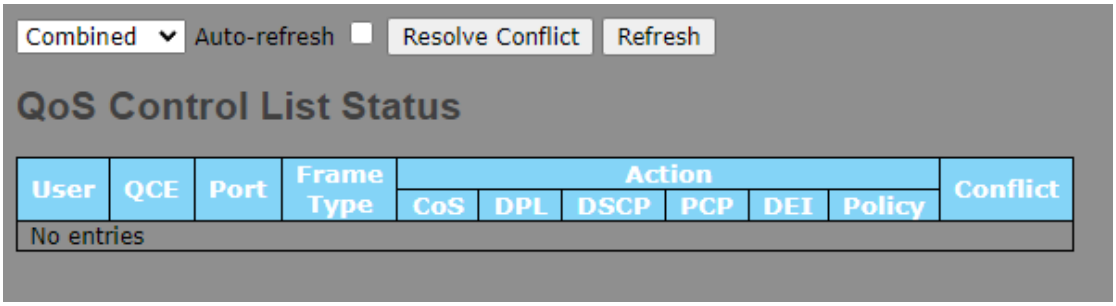


Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	2335	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	17942	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12384
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

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.

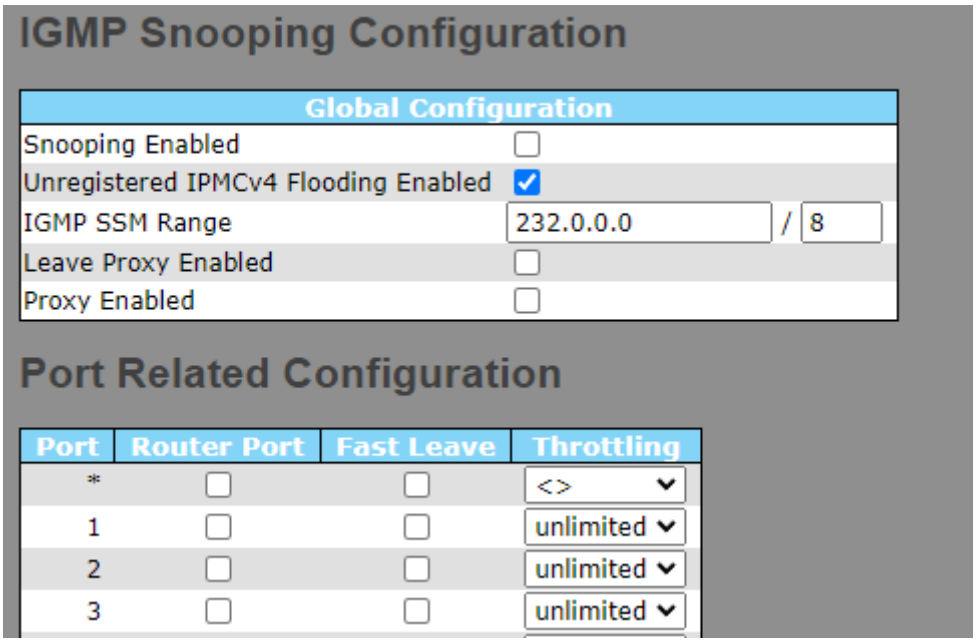


Label	Description
User	Indicates the QCL user
QCE#	Indicates the index of QCE
Frame Type	Indicates the type of frame to look for incoming frames. Possible frame types are: **Any**: the QCE will match all frame type. **Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. **LLC**: Only (LLC) frames are allowed. **SNAP**: Only (SNAP) frames are allowed. **IPv4**: the QCE will match only IPV4 frames. **IPv6**: the QCE will match only IPV6 frames.
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. There are three action fields: **Class**, **DPL**, and **DSCP**. **Class**: Classified QoS; if a frame matches the QCE, it will be put in the queue. **DPL**: Drop Precedence Level; if a frame matches the QCE, then DP level will set to a value displayed under DPL column. **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. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.
IGMP SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range.
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. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

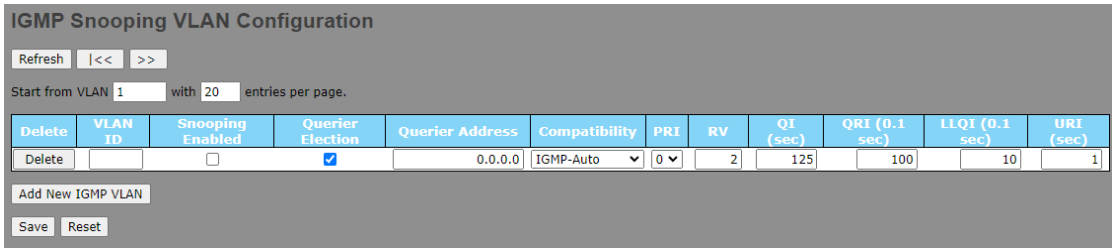
Fast Leave	Check to enable fast leave on the port
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

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.

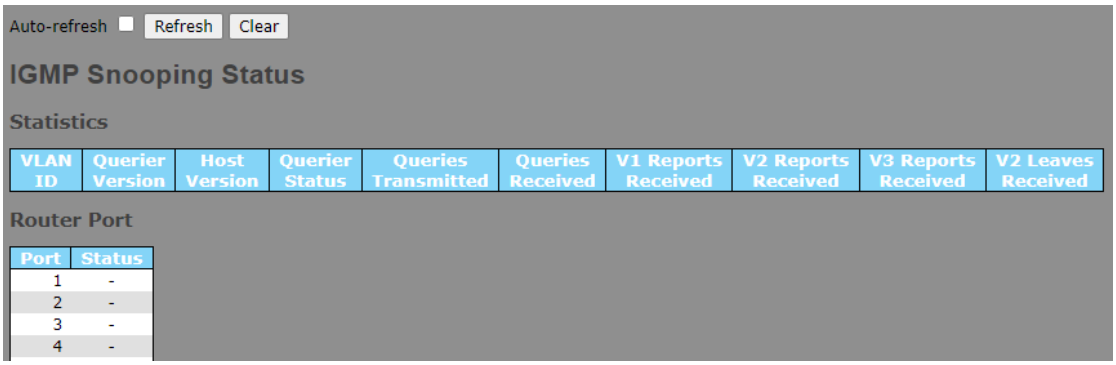


Label	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry
IGMP Snooping Enable	Check to enable IGMP snooping for individual VLAN. Up to 32 VLANs can be selected.
Querier Election	Enable to join IGMP Querier election 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. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address.

Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is **IGMP-Auto**, **Forced IGMPv1**,**Forced IGMPv2**, **Forced IGMPv3**, default compatibility value is IGMP-Auto.
PRI	Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is **0** (best effort) to **7** (highest), default interface priority value is 0.
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is **1** to **255**, default robustness variable value is 2.
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is **1** to **31744** seconds, default query interval is 125 seconds.
QRI	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is **0** to **31744** in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
LLQI(LMQI for IGMP)	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is **0** to **31744** in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).
URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is **0** to **31744** seconds, default unsolicited report interval is 1 second.

IGMP Snooping Status

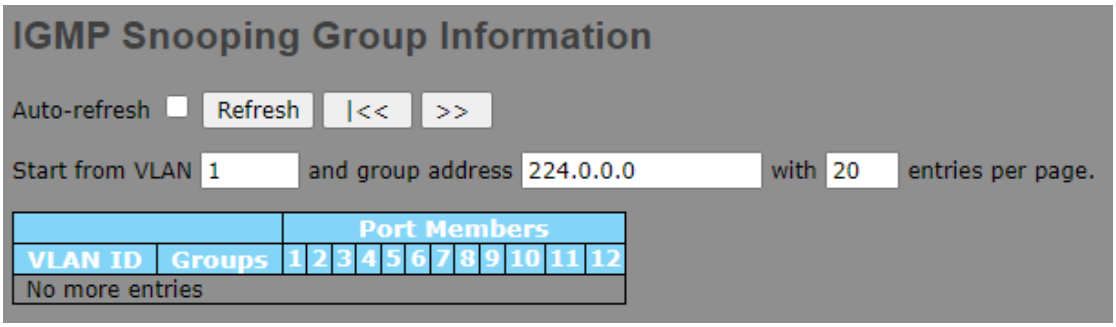
This page provides IGMP snooping status.



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

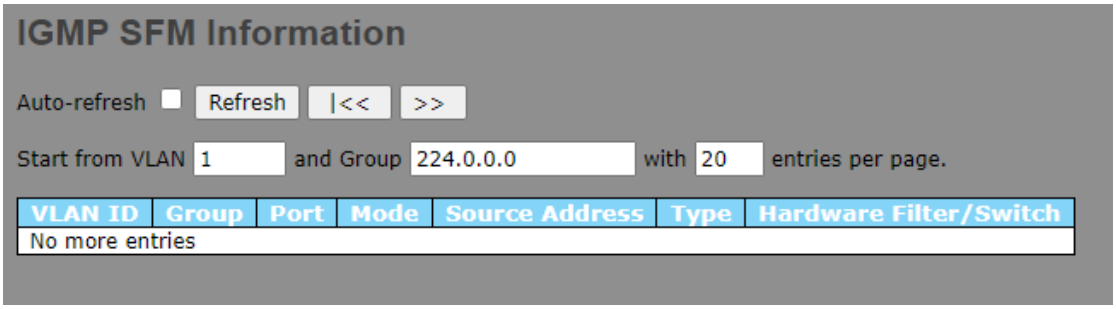
Entries in the **IGMP Group Table** are shown on this page. The **IGMP Group Table** is sorted first by VLAN ID, and then by group.



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

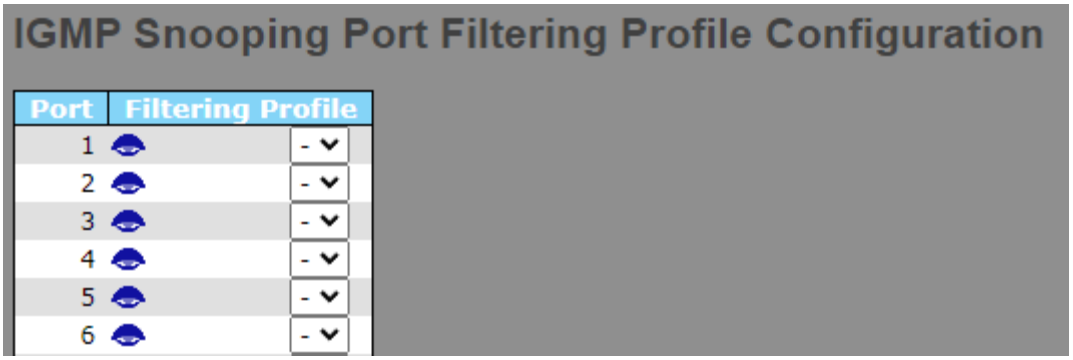
Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the 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. Currently, the maximum number of IPv4 source address for filtering (per group) is 8. When there is no any source filtering address, the text "None" is shown in the Source Address field.

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

Port Group Filtering



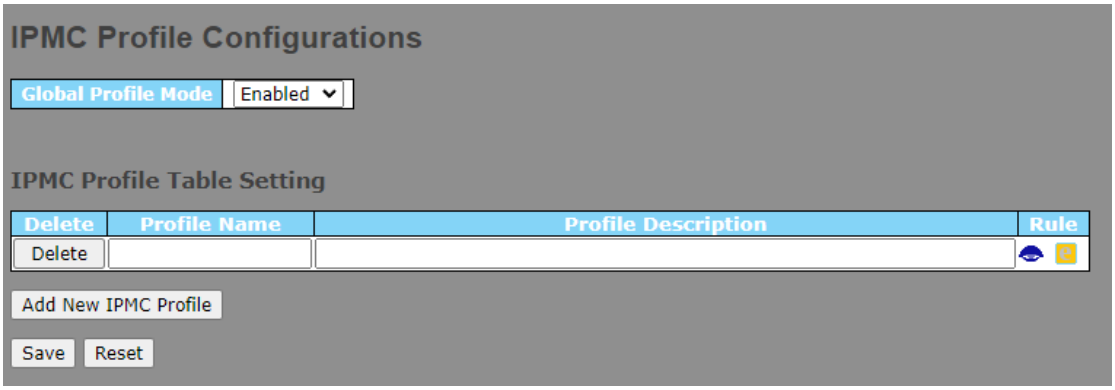
Label	Description
Port	The logical port for the settings.
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.
Profile Management Button	You can inspect the rules of the designated profile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

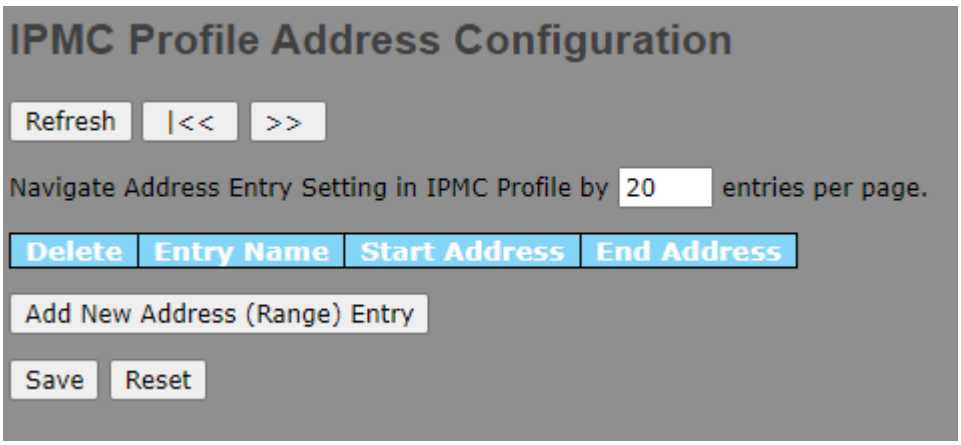


Label	Description
Global Profile Mode	Enable/Disable the Global IPMC Profile. System starts to do filtering based on profile settings only when the global profile mode is enabled.
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
Profile Name	The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.
Profile Description	Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.
Rule	When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons: : List the rules associated with the designated profile. : Adjust the rules associated with the designated profile.

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.

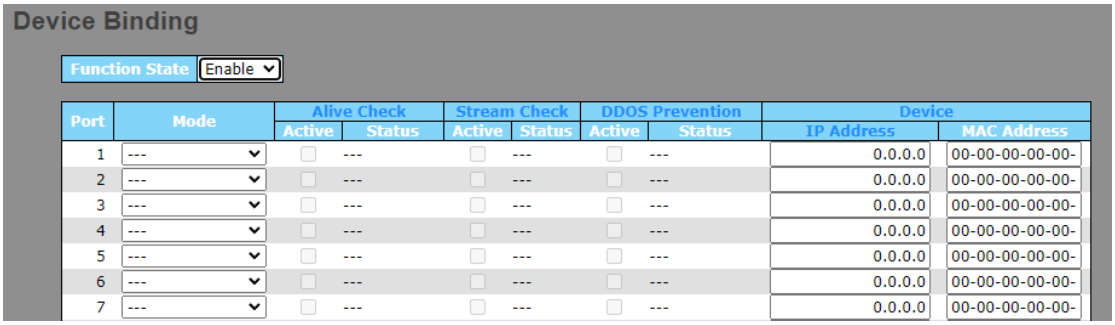


Label	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
Entry Name	The name used for indexing the address entry table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.
Start Address	The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.
End Address	The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

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.



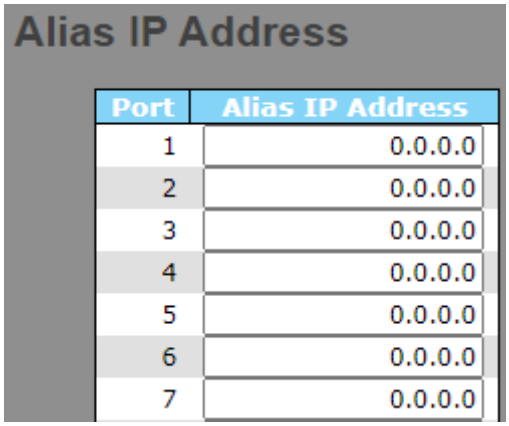
Label	Description
Mode	Indicates the device binding operation for each port. Possible modes are: **---**: disable **Scan**: scans IP/MAC automatically, but no binding function **Binding**: enables binding. Under this mode, any IP/MAC that does not match the entry will not be allowed to access the network. **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: **---**: disable **Got Reply**: receive ping reply from device, meaning the device is still alive **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: **---**: disable **Normal**: the stream is normal. **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: **---**: disable **Analyzing**: analyzes packet throughput for initialization **Running**: analysis completes and ready for next move **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

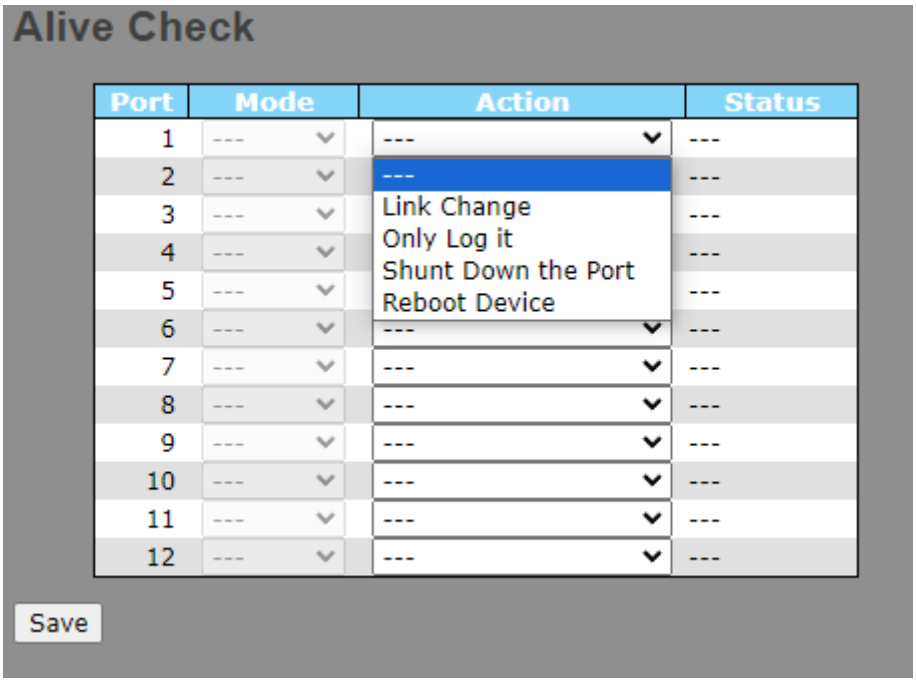
This page provides Alias IP Address configuration. Some devices might have more than one IP addresses. You could specify the other IP address here.



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

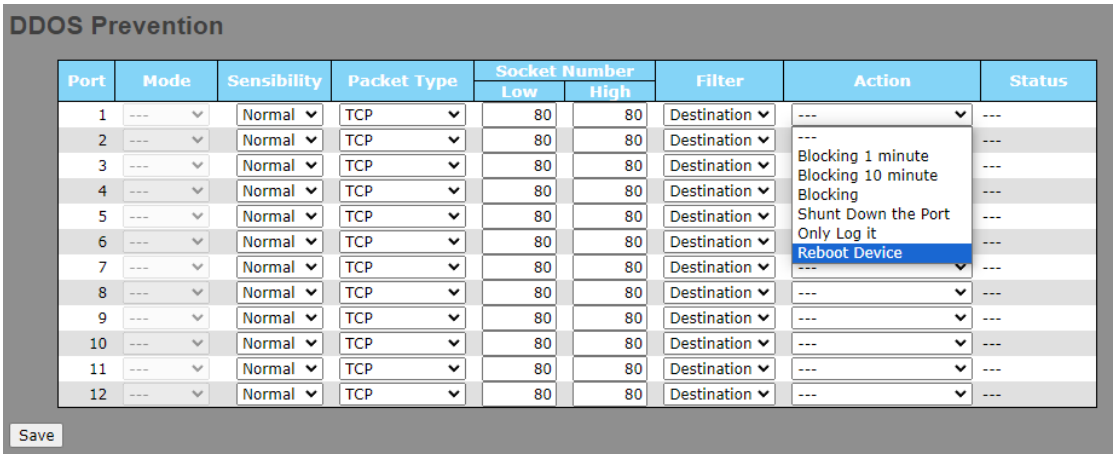
You can use ping commands to check port link status. If port link fails, you can set actions from the drop-down list.



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.

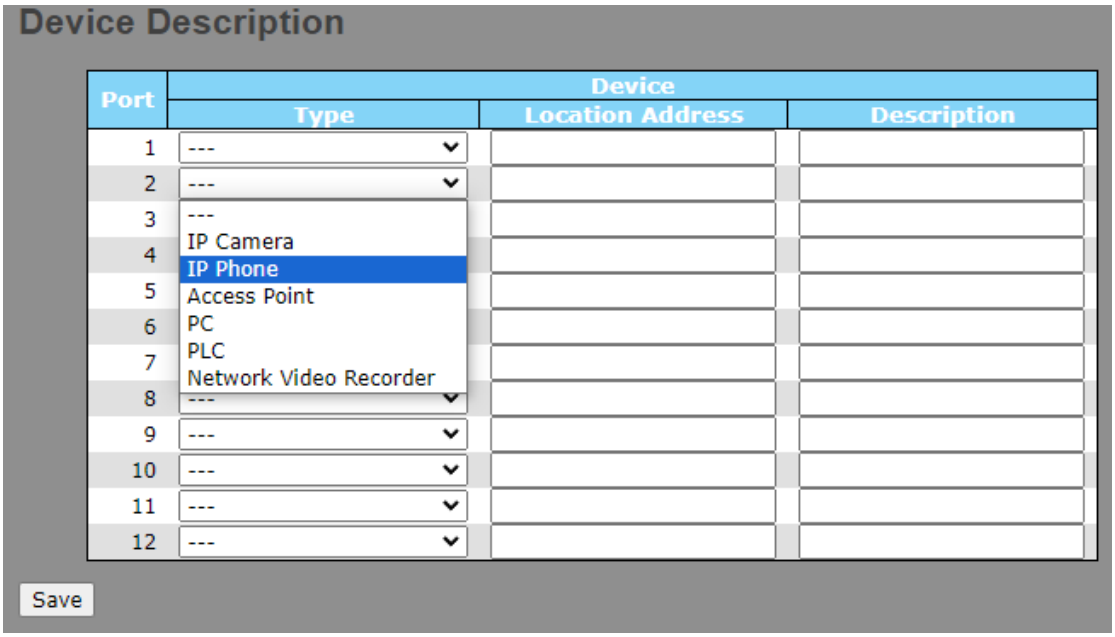


Label	Description
Mode	Enables or disables DDOS prevention of the port
Sensibility	Indicates the level of DDOS detection. Possible levels are: **Low**: low sensibility **Normal**: normal sensibility **Medium**: medium sensibility **High**: high sensibility
Packet Type	Indicates the types of DDoS attack packets to be monitored. Possible types are: **RX Total**: all ingress packets **RX Unicast**: unicast ingress packets **RX Multicast**: multicast ingress packets **RX Broadcast**: broadcast ingress packets **TCP**: TCP ingress packets **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: **---**: no action **Blocking 1 minute**: blocks the forwarding for 1 minute and log the event

	Blocking 10 minute: blocks the forwarding for 10 minutes and log the event **Blocking**: blocks and logs the event **Shunt Down the Port**: shuts down the port (No Link) and logs the event **Only Log it**: simply logs the event **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: **---**: disables DDOS prevention **Analyzing**: analyzes packet throughput for initialization **Running**: analysis completes and ready for next move **Attacked**: DDOS attacks occur

Device Description

This page allows you to configure device description settings.

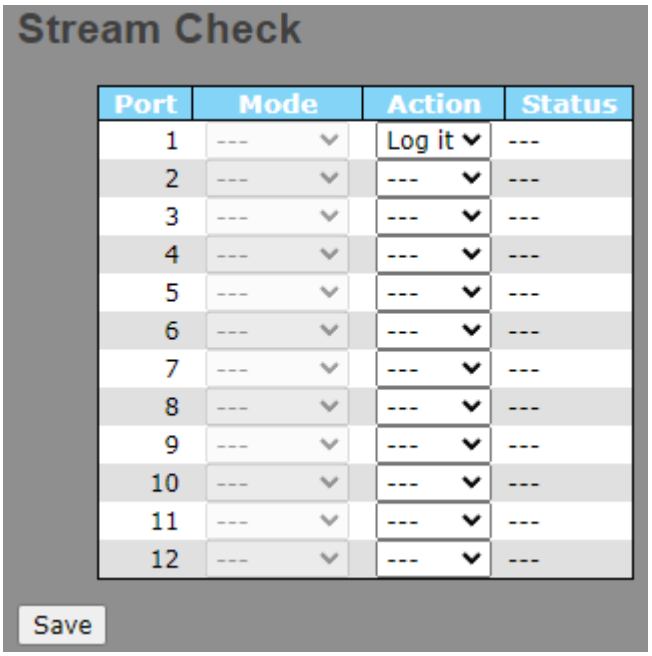


Label	Description
Type	Indicates device types. Possible types are: **---** (no specification), **IP Camera**, **IP Phone**, **Access Point**, **PC**, **PLC**, and **Network Video Recorder**
Location Address	Indicates location information of the device. The information can be used for Google Mapping.

Description	Device descriptions

Stream Check

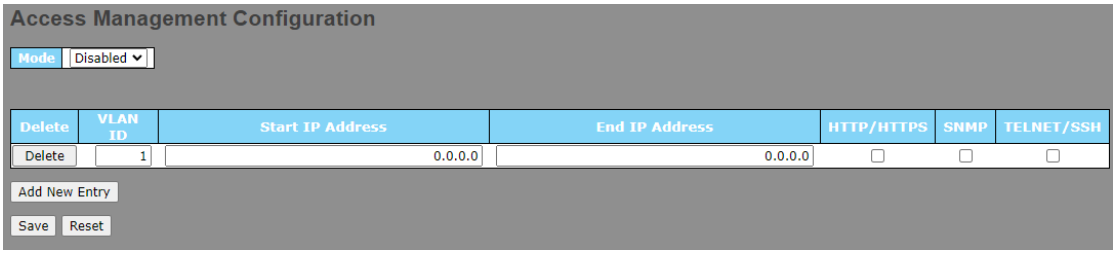
This page allows you to configure stream check settings.



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: **---**: no action **Log it**: simply logs the event

1.9.2 Access Management Configuration

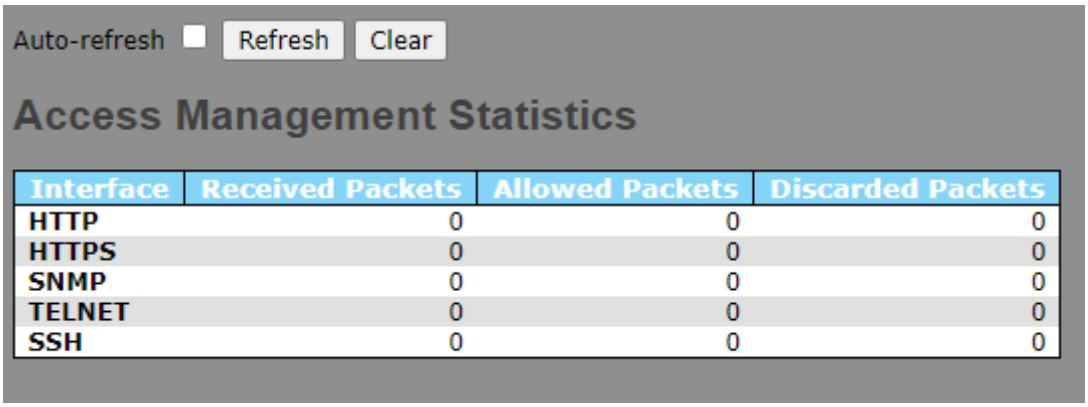
You can configure access management table on this page. If the application's type match any one of the access management entries, it will allow access to the switch.



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

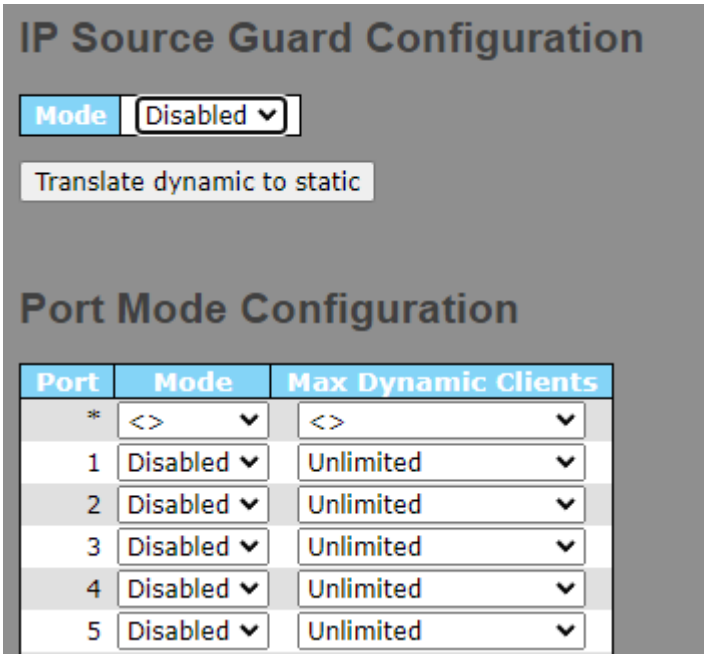
This page provides an overview of access management configurations.



1.9.3 IP Source Guard

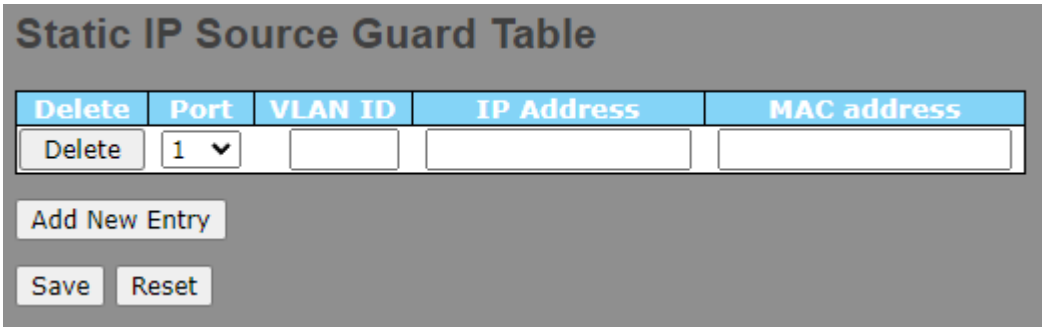
IP source guard can prevent traffic attacks if a host tries to use the IP address of its neighbor. You can enable IP source guard when DHCP snooping is enabled on an untrusted interface. With this function enabled, the switch blocks all IP traffic received on the interface except for DHCP packets allowed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

Configuration



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

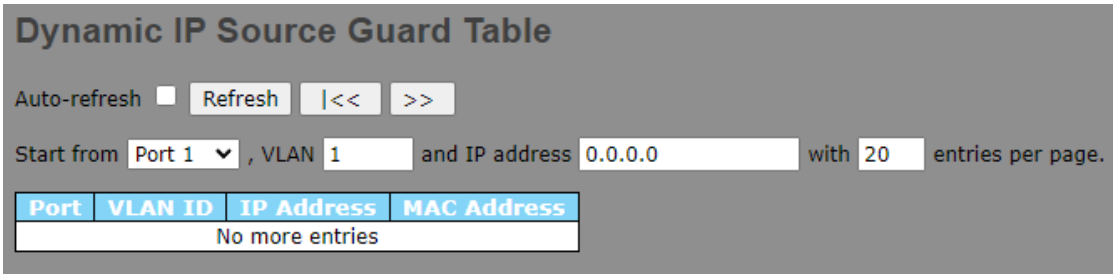
Static Table



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.

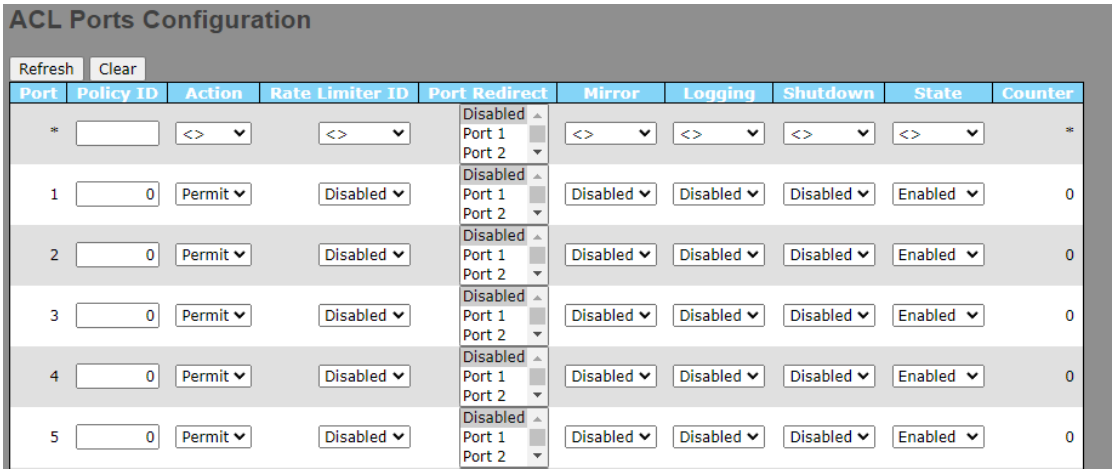


Label	Description
Port	The logical port for the settings.
VLAN ID	The vlan id for the settings.
IP Address	Allowed source IP address.
MAC Address	Allowed source MAC address.

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.

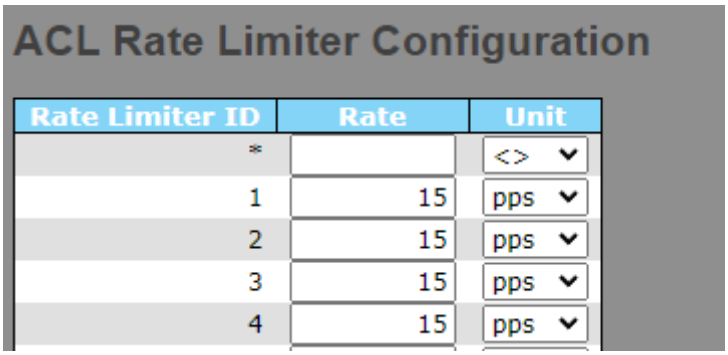


Label	Description
Port	The switch port number to which the following settings will be applied
Policy ID	Select to apply a policy to the port. The allowed values are 1 to 8. The default value is **1**.
Action	Select to **Permit** to permit or **Deny** to deny forwarding. The default

	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: **Enabled**: frames received on the port are stored in the system log **Disabled**: frames received on the port are not logged The default value is **Disabled**. Please note that system log memory capacity and logging rate is limited.
Shutdown	Specifies the shutdown operation of this port. The allowed values are: **Enabled**: if a frame is received on the port, the port will be disabled. **Disabled**: port shut down is disabled. The default value is **Disabled**.
Counter	Counts the number of frames that match this ACE.

Rate Limiters

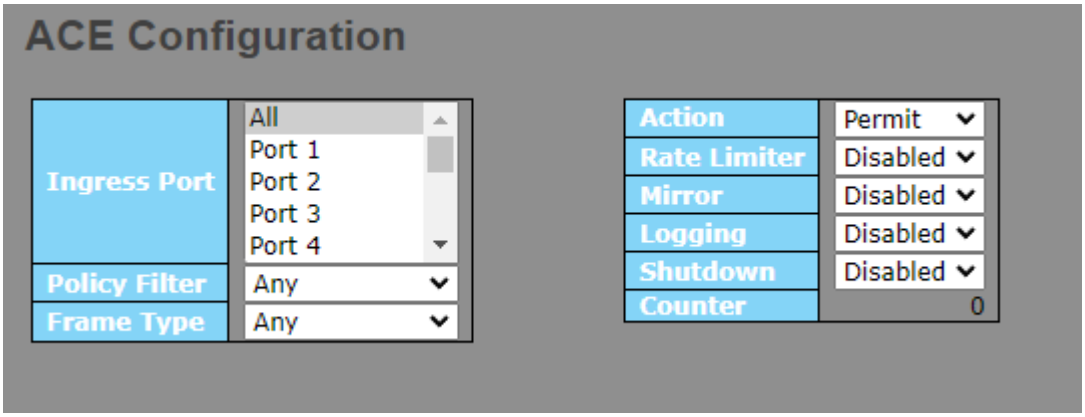
This page allows you to configure the rate limiter for the ACL of the switch.



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. The 1 kpps is actually 1002.1 pps.
Unit	Specify the unit for the rate.

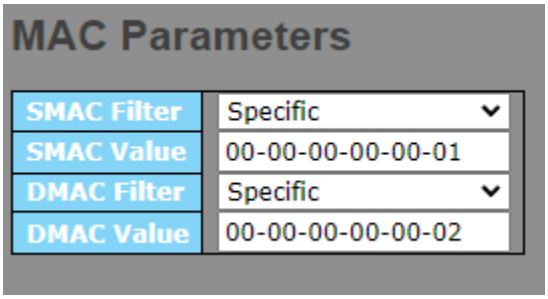
ACL Control List

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.



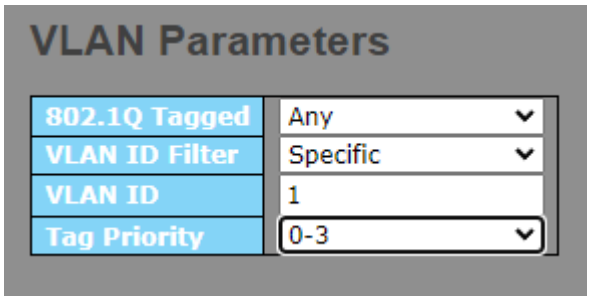
Label	Description
Ingress Port	Indicates the ingress port to which the ACE will apply. **Any**: the ACE applies to any port **Port n**: the ACE applies to this port number, where n is the number of the switch port. **Policy n**: the ACE applies to this policy number, where n can range from 1 to 8.
Frame Type	Indicates the frame type of the ACE. These frame types are mutually exclusive. **Any**: any frame can match the ACE. **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). **ARP**: only ARP frames can match the ACE. Notice the ARP frames will not match the ACE with Ethernet type. **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. Permit: takes action when the frame matches the ACE. 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: **Enabled**: frames matching the ACE are stored in the system log. **Disabled**: frames matching the ACE are not logged. Please note that system log memory capacity and logging rate is limited.
Shutdown	Specifies the shutdown operation of the ACE. The allowed values are: **Enabled**: if a frame matches the ACE, the ingress port will be disabled. **Disabled**: port shutdown is disabled for the ACE.
Counter	Indicates the number of times the ACE matched by a frame.

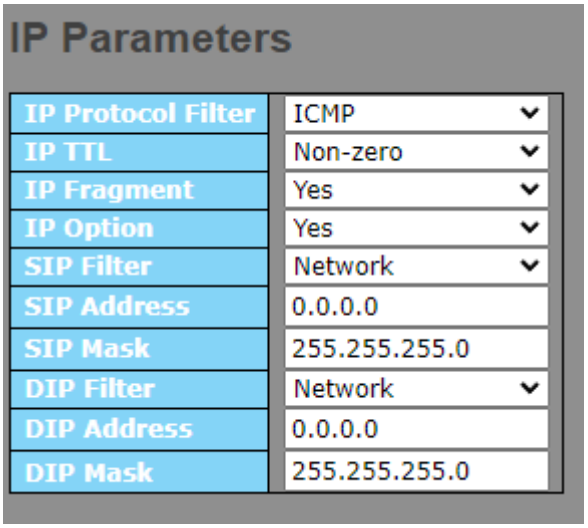


Label	Description
SMAC Filter	(Only displayed when the frame type is Ethernet Type or ARP.) Specifies the source MAC filter for the ACE. **Any**: no SMAC filter is specified (SMAC filter status is "**don't-care**"). **Specific**: if you want to filter a specific source MAC address with the ACE, choose 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 **Any**: no DMAC filter is specified (DMAC filter status is "**don't-care**"). **MC**: frame must be multicast.

	BC: frame must be broadcast. **UC**: frame must be unicast. **Specific**: If you want to filter a specific destination MAC address with 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.

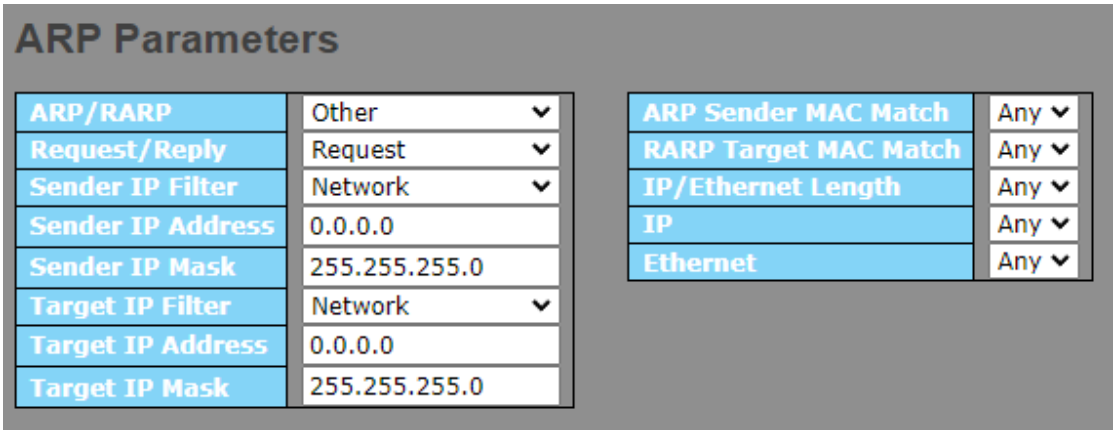


Label	Description
VLAN ID Filter	Specifies the VLAN ID filter for the ACE **Any**: no VLAN ID filter is specified (VLAN ID filter status is "**don't-care**"). **Specific**: if you want to filter a specific VLAN ID with the ACE, choose this value. A field for entering a VLAN ID number appears.
VLAN ID	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 **Any**: no IP protocol filter is specified ("**don't-care**"). **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. 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. **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. **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 **Zero**: IPv4 frames with a time-to-live value greater than zero must not be able to match this entry. **Non-zero**: IPv4 frames with a time-to-live field greater than zero must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
IP Fragment	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.

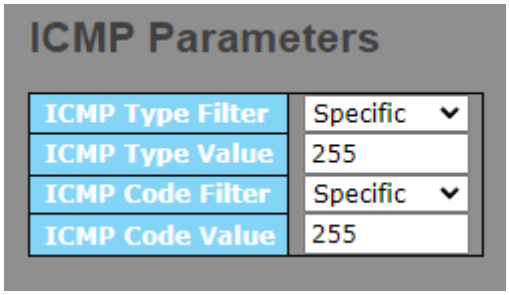
	No: IPv4 frames whose MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. **Yes**: IPv4 frames whose MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
IP Option	Specifies the options flag settings for the ACE **No**: IPv4 frames whose options flag is set must not be able to match this entry. **Yes**: IPv4 frames whose options flag is set must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
SIP Filter	Specifies the source IP filter for this ACE **Any**: no source IP filter is specified (Source IP filter is "**don't-care**"). **Host**: source IP filter is set to **Host**. Specify the source IP address in the **SIP Address** field that appears. **Network**: source IP filter is set to **Network**. Specify the source IP address and source IP mask in the **SIP Address** and **SIP Mask** fields that appear.
SIP Address	When **Host** or **Network** is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.
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 **Any**: no destination IP filter is specified (destination IP filter is "**don't-care**"). **Host**: destination IP filter is set to **Host**. Specify the destination IP address in the **DIP Address** field that appears. **Network**: destination IP filter is set to **Network**. Specify the destination IP address and destination IP mask in the **DIP Address** and **DIP Mask** fields that appear.
DIP Address	When **Host** or **Network** is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.
DIP Mask	When **Network** is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.



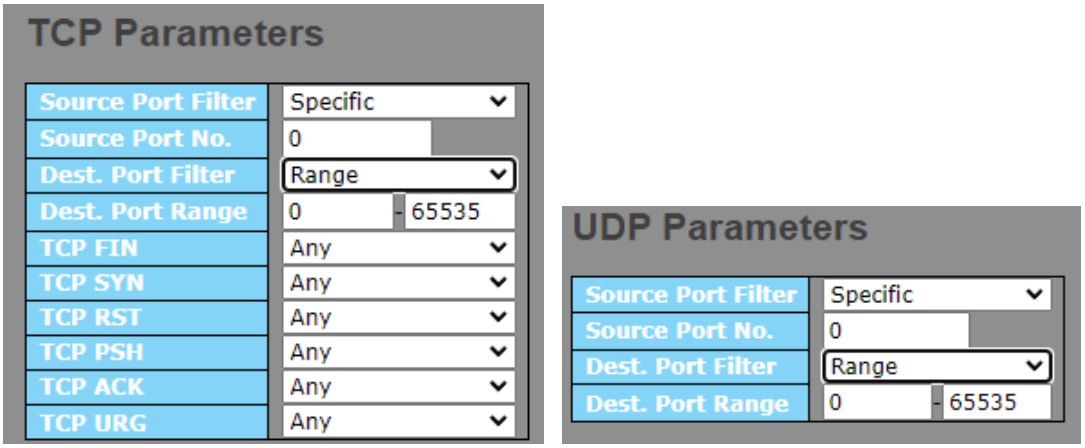
Label	Description
ARP/RARP	Specifies the available ARP/RARP opcode (OP) flag for the ACE **Any**: no ARP/RARP OP flag is specified (OP is "**don't-care**"). **ARP**: frame must have ARP/RARP opcode set to ARP **RARP**: frame must have ARP/RARP opcode set to RARP. **Other**: frame has unknown ARP/RARP Opcode flag.
Request/Reply	Specifies the available ARP/RARP opcode (OP) flag for the ACE **Any**: no ARP/RARP OP flag is specified (OP is "**don't-care**"). **Request**: frame must have ARP Request or RARP Request OP flag set. **Reply**: frame must have ARP Reply or RARP Reply OP flag.
Sender IP Filter	Specifies the sender IP filter for the ACE **Any**: no sender IP filter is specified (sender IP filter is "**don't-care**"). **Host**: sender IP filter is set to **Host**. Specify the sender IP address in the **SIP Address** field that appears. **Network**: sender IP filter is set to **Network**. Specify the sender IP address and sender IP mask in the **SIP Address** and **SIP Mask** fields that appear.
Sender IP Address	When Host or Network is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
Sender IP Mask	When Network is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
Target IP Filter	Specifies the target IP filter for the specific ACE

	Any: no target IP filter is specified (target IP filter is "**don't-care**"). **Host**: target IP filter is set to **Host**. Specify the target IP address in the **Target IP Address** field that appears. **Network**: target IP filter is set to **Network**. Specify the target IP address and target IP mask in the **Target IP Address** and **Target IP Mask** fields that appear.
Target IP Address	When **Host** or **Network** is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
Target IP Mask	When **Network** is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
ARP SMAC Match	Specifies whether frames will meet the action according to their sender hardware address field (SHA) settings. **0**: ARP frames where SHA is not equal to the SMAC address **1**: ARP frames where SHA is equal to the SMAC address **Any**: any value is allowed ("**don't-care**").
RARP SMAC Match	Specifies whether frames will meet the action according to their target hardware address field (THA) settings. **0**: RARP frames where THA is not equal to the SMAC address **1**: RARP frames where THA is equal to the SMAC address **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. **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. **1**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must match this entry. **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. **0**: ARP/RARP frames where the HLD is equal to Ethernet (1) must not match this entry. **1**: ARP/RARP frames where the HLD is equal to Ethernet (1)

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



Label	Description
ICMP Type Filter	Specifies the ICMP filter for the ACE **Any**: no ICMP filter is specified (ICMP filter status is "**don't-care**"). **Specific**: if you want to filter a specific ICMP filter with 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 **Any**: no ICMP code filter is specified (ICMP code filter status is "**don't-care**"). **Specific**: if you want to filter a specific ICMP code filter with 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.



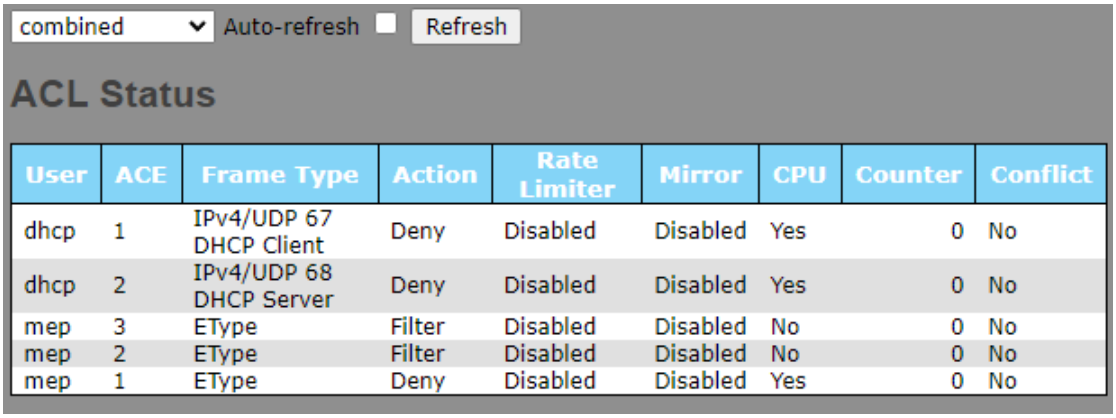
Label	Description
TCP/UDP Source Filter	Specifies the TCP/UDP source filter for the ACE **Any**: no TCP/UDP source filter is specified (TCP/UDP source filter status is "**don't-care**"). **Specific**: if you want to filter a specific TCP/UDP source filter with the ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears. **Range**: if you want to filter a specific TCP/UDP source range filter with 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 **Any**: no TCP/UDP destination filter is specified (TCP/UDP destination filter status is "**don't-care**"). **Specific**: if you want to filter a specific TCP/UDP destination filter with the ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears. **Range**: if you want to filter a specific range TCP/UDP destination filter with 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. **0**: TCP frames where the FIN field is set must not be able to match this entry. **1**: TCP frames where the FIN field is set must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
TCP SYN	Specifies the TCP SYN ("synchronize sequence numbers") value for the ACE **0**: TCP frames where the SYN field is set must not be able to match this entry. **1**: TCP frames where the SYN field is set must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
TCP PSH	Specifies the TCP PSH ("push function") value for the ACE **0**: TCP frames where the PSH field is set must not be able to match this entry. **1**: TCP frames where the PSH field is set must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
TCP ACK	Specifies the TCP ACK ("acknowledgment field significant") value for the ACE **0**: TCP frames where the ACK field is set must not be able to match this entry. **1**: TCP frames where the ACK field is set must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
TCP URG	Specifies the TCP URG ("urgent pointer field significant") value for

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

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.



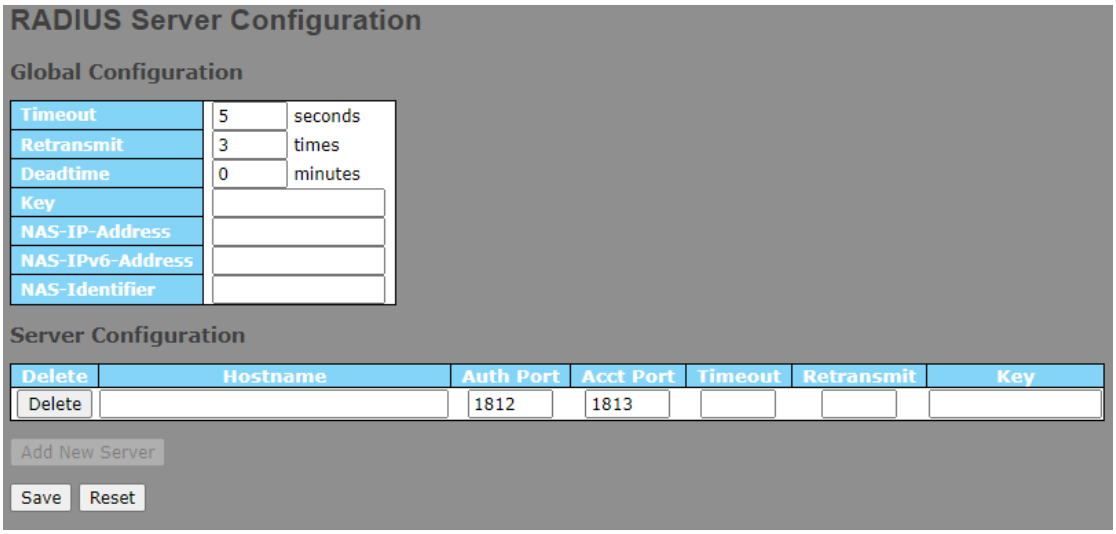
Label	Description
User	Indicates the ACL user.
ACE	Indicates the ACE ID on local switch.
Frame Type	Indicates the frame type of the ACE. Possible values are: **Any:** The ACE will match any frame type. **EType:** The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. **ARP:** The ACE will match ARP/RARP frames. **IPv4:** The ACE will match all IPv4 frames. **IPv4/ICMP:** The ACE will match IPv4 frames with ICMP protocol. **IPv4/UDP:** The ACE will match IPv4 frames with UDP protocol. **IPv4/TCP:** The ACE will match IPv4 frames with TCP protocol. **IPv4/Other:** The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. **IPv6:** The ACE will match all IPv6 standard frames.

Action	Indicates the forwarding action of the ACE. **Permit:** Frames matching the ACE may be forwarded and learned. **Deny:** Frames matching the ACE are dropped.
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

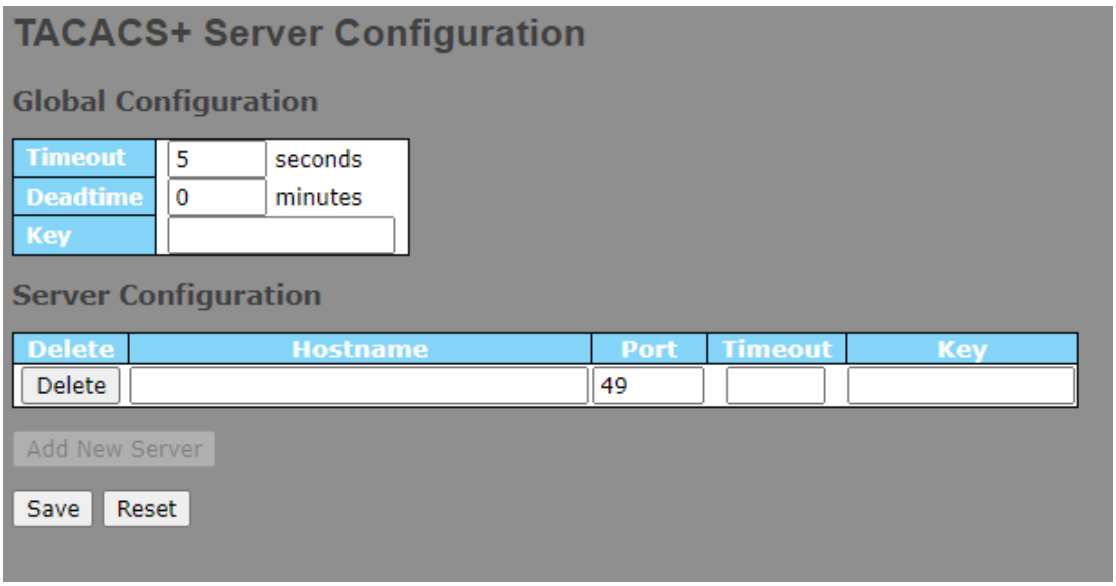
This page allows you to configure authentication servers.



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. 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). 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. 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+



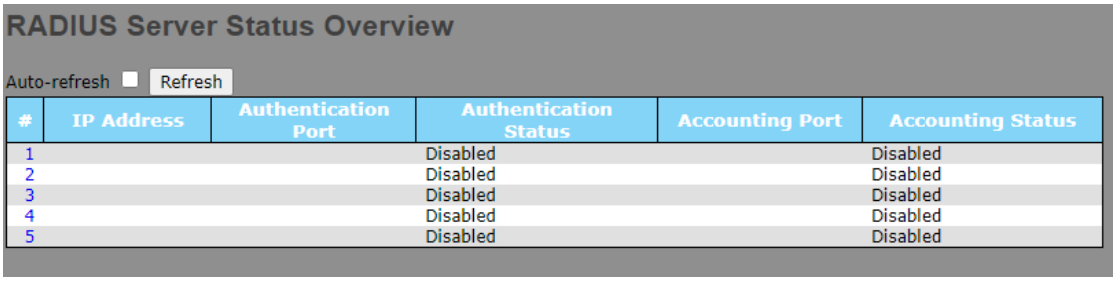
Label	Description
Timeout	The timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled server (if any). TACACS+ servers 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. 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

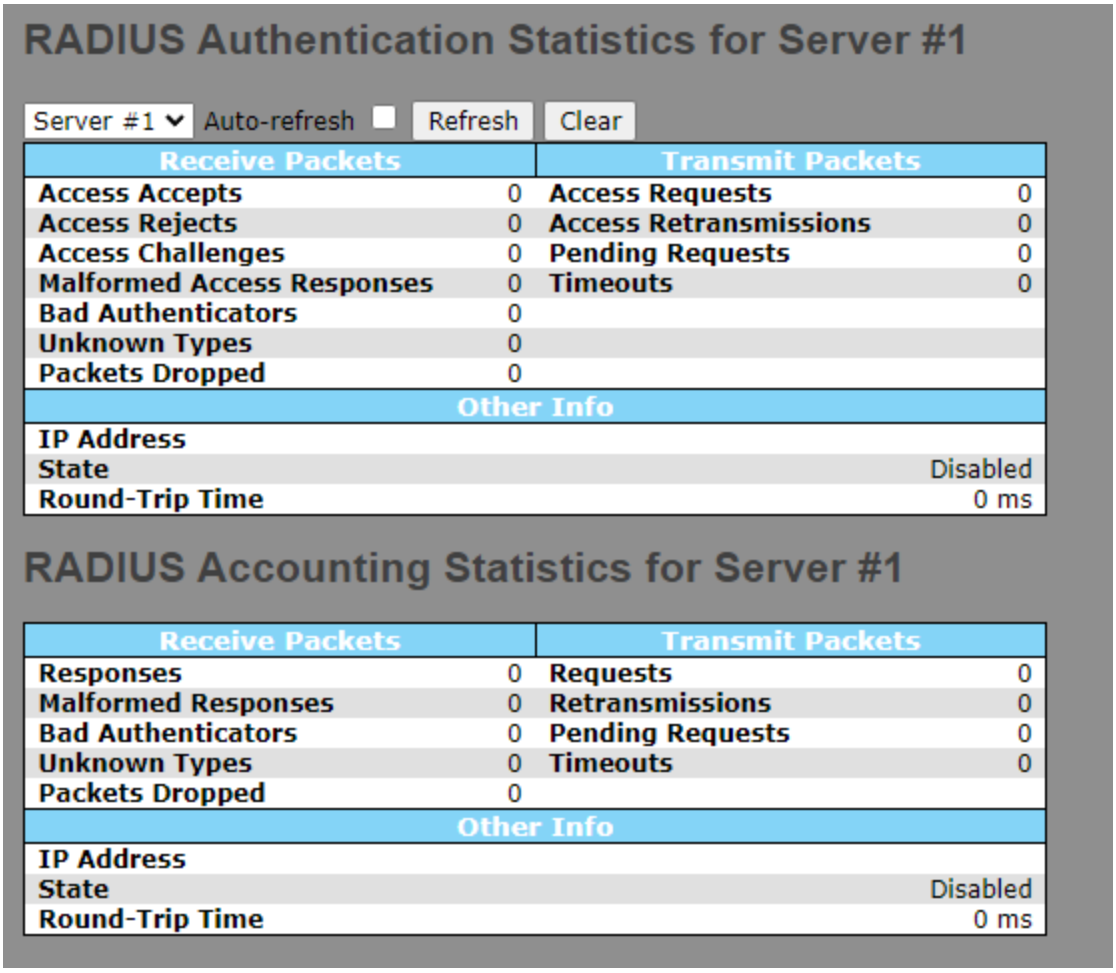
This page provides an overview of the status of the RADIUS servers configurable on the authentication configuration page.



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: **Disabled**: the server is disabled. **Not Ready**: the server is enabled, but IP communication is not yet up and running. **Ready**: the server is enabled, IP communications are built, and the RADIUS module is ready to accept access attempts. **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.



1.9.8 ARP Inspection (only for Layer 3 Model)

This page provides ARP Inspection related configuration.

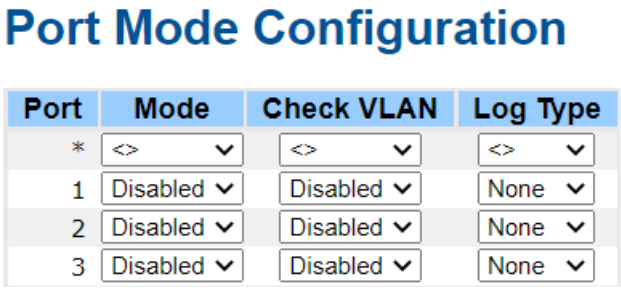
Configuration

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

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.

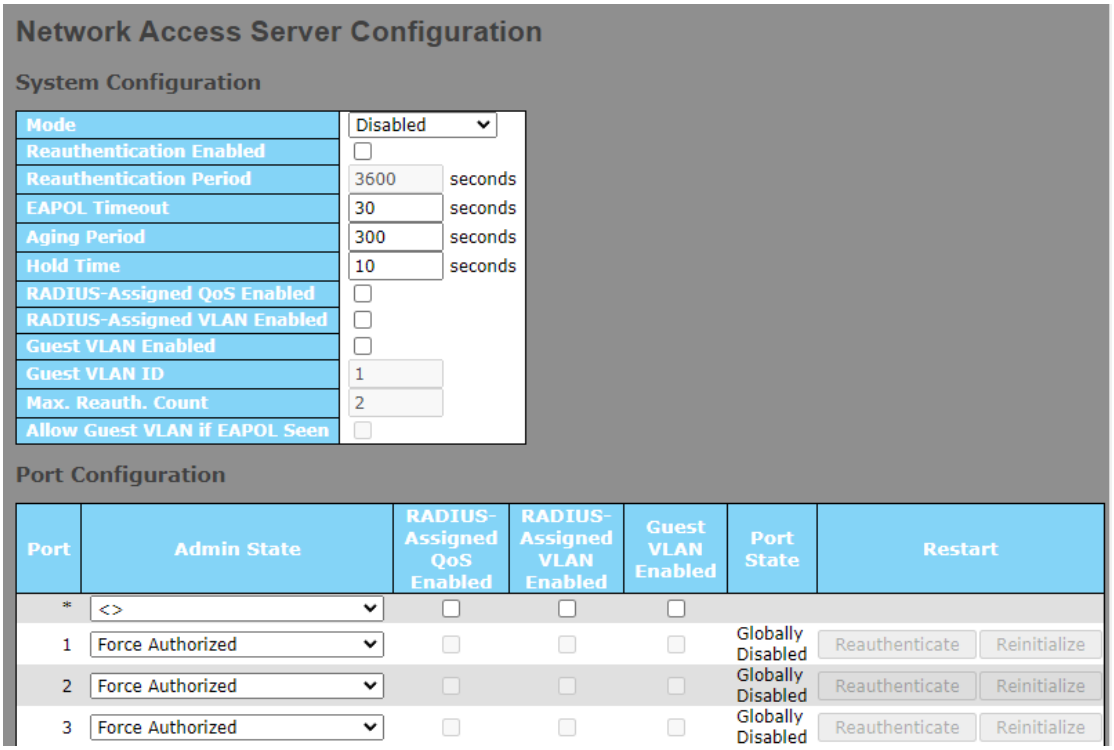
Overview of MAC-Based Authentication

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. 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. 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: **MAC-Based Auth**.: When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. 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: **MAC-Based Auth**.: If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "**Configuration→Security→AAA**" page) - the client is put on hold in Unauthorized state. The hold timer does not count during an on-going authentication. The switch will ignore new frames coming from the client during the hold time. The hold time can be set to a number between 10 and 1000000 seconds.
Port	The port number for which the configuration below applies
Admin State	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: **Force Authorized** In this mode, the switch will send one EAPOL Success frame when the port link is 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 is up, and any client on the port will be disallowed network access. **Port-based 802.1X** 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. 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

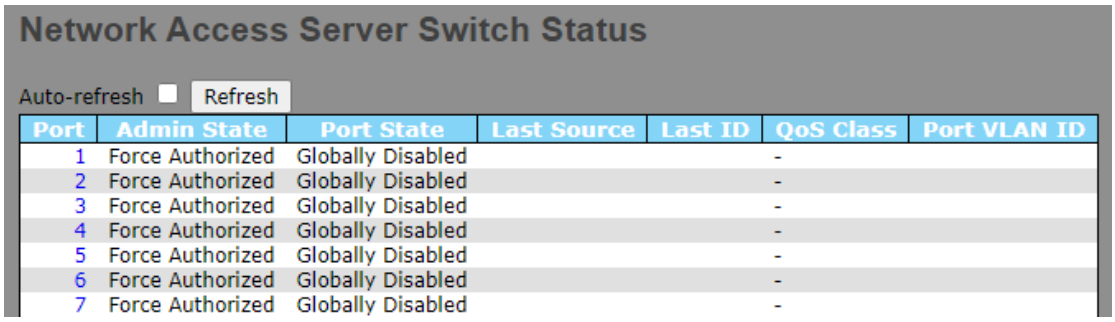
	loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate. **a. Single 802.1X** In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they are not authenticated individually. To overcome this security breach, use the Single 802.1X variant. 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. **b. Multi 802.1X** In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they are not authenticated individually. To overcome this security breach, use the Multi 802.1X variant. 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. 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. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality. **MAC-based Auth.** Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string 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. 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: **Globally Disabled**: NAS is globally disabled. **Link Down**: NAS is globally enabled, but there is no link on the port. **Authorized**: the port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. **Unauthorized:** the port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. **X Auth/Y Unauth**: the port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect. **Reauthenticate**: schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect on successfully authenticated clients on the port and will not cause the clients to be temporarily unauthorized. **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.

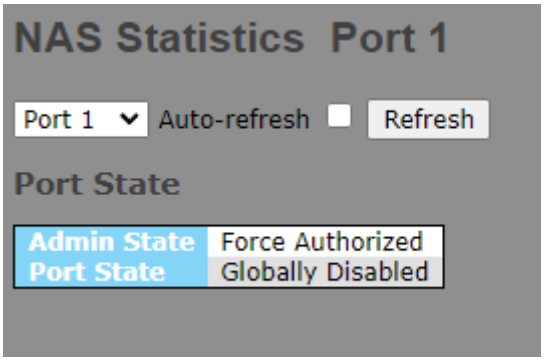
Switch

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



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: • **Force Authorized** • **Force Unauthorized** • 802.1X
Backend Server Counters	These backend (RADIUS) frame counters are available for the following administrative states: • **802.1X** • **MAC-based Auth.**

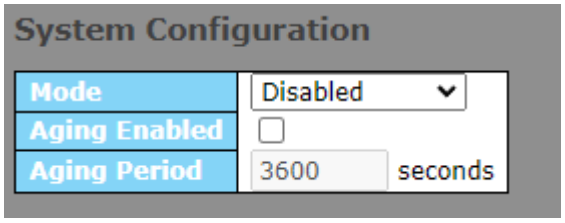
EAPOL Counters

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

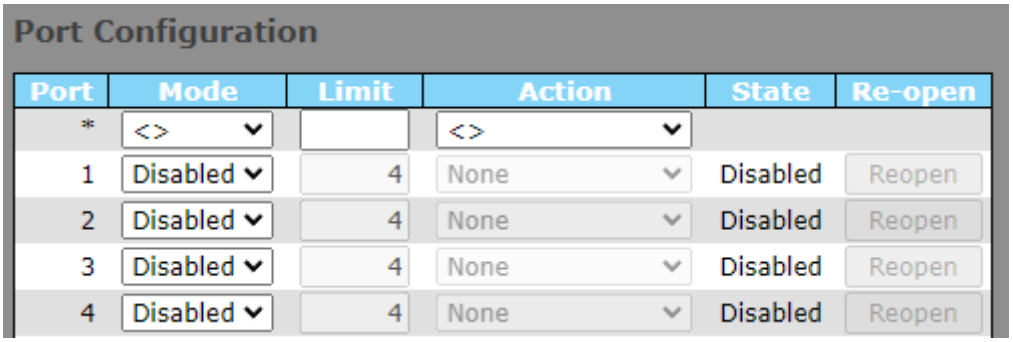
	Backend Server Counters **Direction** / **Name** / **IEEE Name** / **Description** Rx — **Access Challenges** — dot1xAuthBackendAccessChallenges — **Port-based**: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. **MAC-based**: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table). Rx — **Other Requests** — dot1xAuthBackendOtherRequestsToSupplicant — **Port-based**: 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. **MAC-based**: Not applicable. Rx — **Auth. Successes** — dot1xAuthBackendAuthSuccesses — **Port- and MAC-based**: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server. Rx — **Auth. Failures** — dot1xAuthBackendAuthFails — **Port- and MAC-based**: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server. Tx — **Responses** — dot1xAuthBackendResponses — **Port-based:** 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. **MAC-based:** Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.
Last Supplicant/Client Info	Information about the last supplicant/client that attempts to authenticate. This information is available for the following administrative states: • **802.1X** • **MAC-based Auth.** **Last Supplicant/Client Info** **Name** / **IEEE Name** / **Description** **MAC Address** — dot1xAuthLastEapolFrameSource — The MAC address of the last supplicant/client. **VLAN ID** — - — The VLAN ID on which the last frame from the last supplicant/client was received. **Version** — dot1xAuthLastEapolFrameVersion — **802.1X-based**: The protocol version number carried in the most recently received EAPOL frame. **MAC-based**: Not applicable. **Identity** — - — **802.1X-based**: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. **MAC-based**: Not applicable.

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.

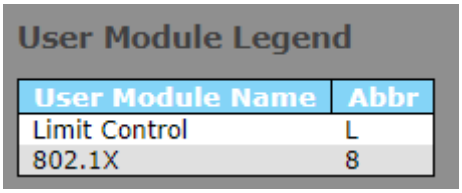


Label	Description
Mode	Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.
Limit	The 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: **None**: Do not allow more than Limit MAC addresses on the port, but take no further action.

	Trap: If Limit + 1 MAC addresses is seen on the port, send an *SNMP (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. **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. **Trap & Shutdown**: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.
State	This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values: **Disabled**: Limit Control is either globally disabled or disabled on the port. **Ready**: The limit is not yet reached. This can be shown for all actions. **Limit Reached**: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap. **Shutdown**: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.
Re-open	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. Note that clicking the **Re-open** button causes the page to be refreshed, so non-committed changes will be lost.

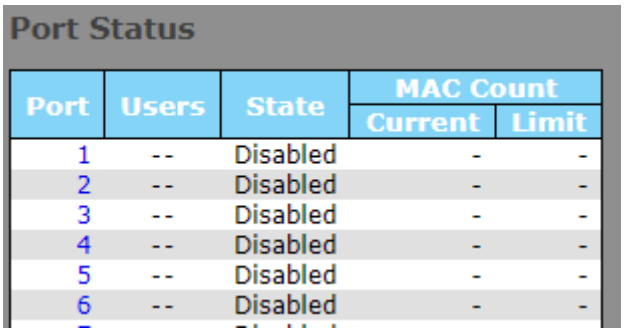
Switch

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.

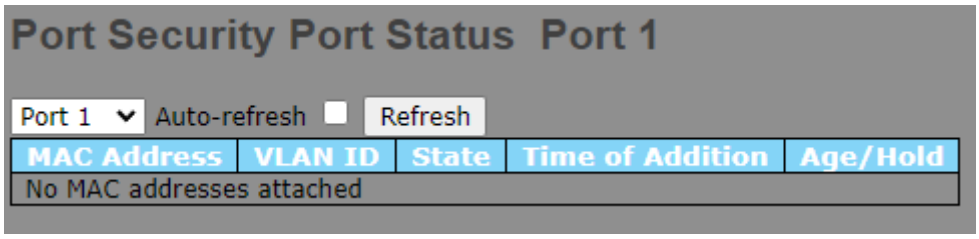


Label	Description
Users	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.
State	Shows the current state of the port which includes the following values: **Disabled**: No user modules are currently using the Port Security service. **Ready**: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. **Limit Reached**: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. **Shutdown**: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.
MAC Count	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.

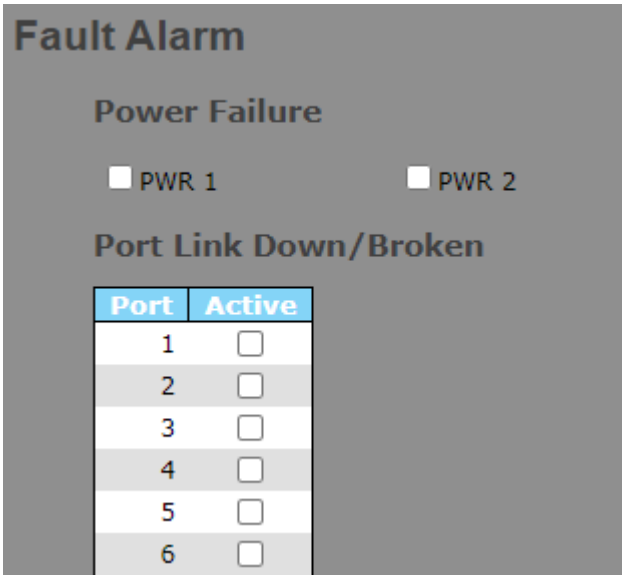


Label	Description
MAC Address	The MAC address that is seen on this port. If no MAC addresses are learned, a single row stating No MAC addresses attached is displayed.
VLAN ID	The VLAN ID that is seen on this port.
State	Indicates whether the corresponding MAC address is blocked or forwarding. If blocked, 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. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

1.10 Warning

1.10.1 Fault Alarm

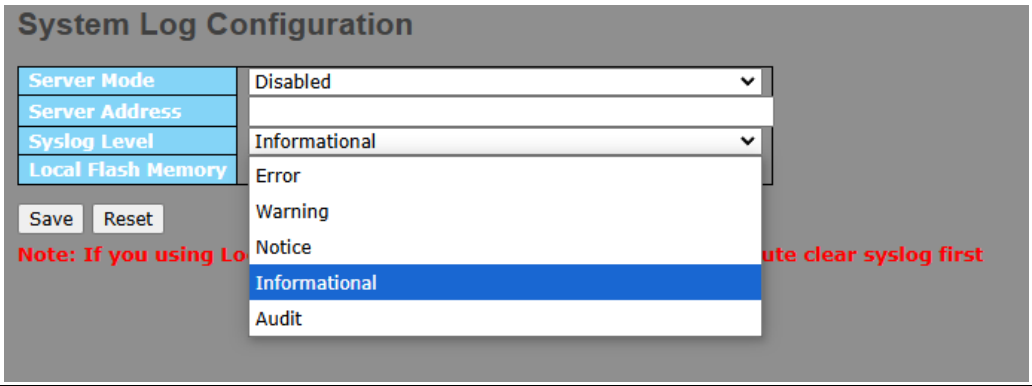
When any selected fault event happens, the Fault LED on the switch panel will light up and the electric relay will signal at the same time.



1.10.2 System Warning

SYSLOG Setting

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

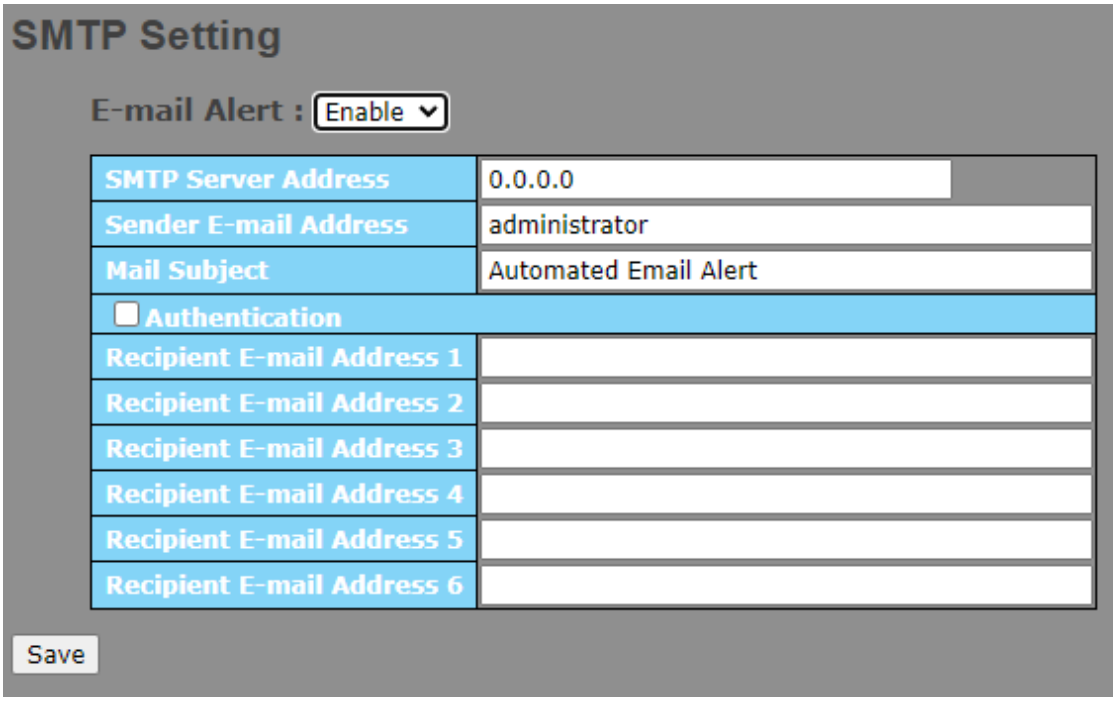


Label	Description
Server Mode	Indicates existing server mode. When the mode operation is enabled, the syslog message will be sent to syslog server. The syslog protocol is based on UDP communications and received on UDP port 514 and the syslog server will not send acknowledgments back to the sender since 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:

	Enabled: enable server mode **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	Indicates what kind of message will send to syslog server. Possible modes are: **Error:** Send the specific messages which severity code is less or equal than Error(3). **Warning:** Send the specific messages which severity code is less or equal than Warning(4). **Notice:** Send the specific messages which severity code is less or equal than Notice(5). Informational: Send the specific messages which severity code is less or equal than Informational(6). **Audit:** Send the specific messages which severity code is less or equal than Audit(7).

SMTP Setting

The SMTP is Short for Simple Mail Transfer Protocol. It's a protocol for e-mail transmission across the Internet. Please refer to RFC 821 - Simple Mail Transfer Protocol.

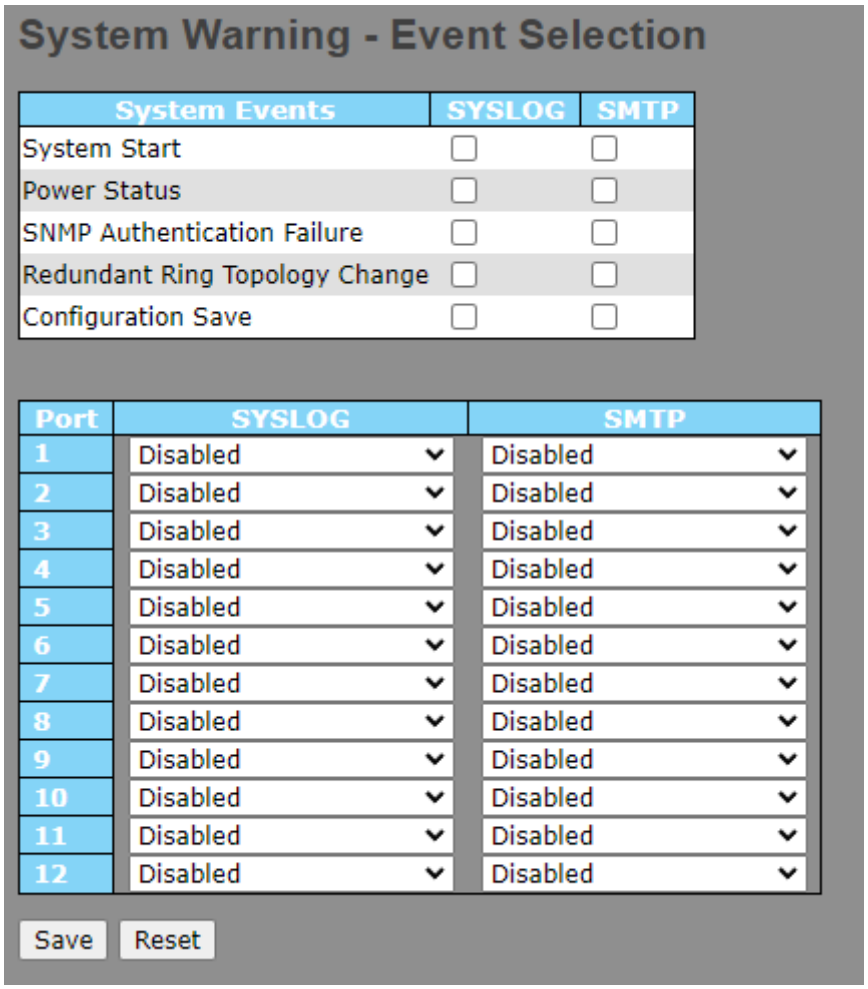


Label	Description
E-mail Alert	Enable/Disable transmission system warning events by e-mail.

SMTP Server Address	The SMTP server IP address.
Sender E-mail Address	The sender's E-mail address of the mail.
Mail Subject	The Subject of the mail.
Authentication	Checked if the SMTP server needs authentication.
Username	The authentication username.
Password	The authentication password.
Confirm Password	Re-enter password.
Recipient E-mail Address	The recipient's E-mail address. It supports 6 recipients for a mail.

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.

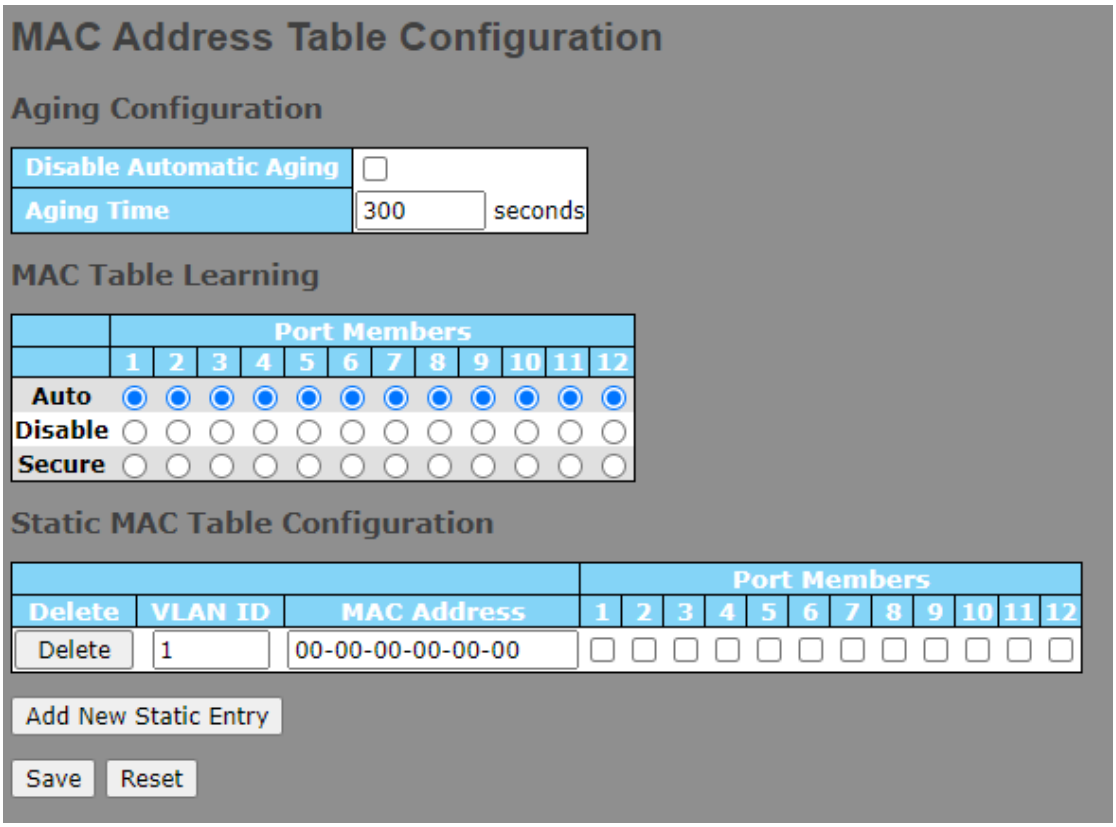


Label	Description
System Cold Start	Sends out alerts when the system is restarted
Power Status	Sends out alerts when power is up or down
SNMP Authentication Failure	Sends out alert when SNMP authentication fails
Redundant-Ring Topology Change	Sends out alerts when Redundant-Ring topology changes
Port Event SYSLOG	■ **Disable** ■ **Link Up** ■ **Link Down** ■ **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.

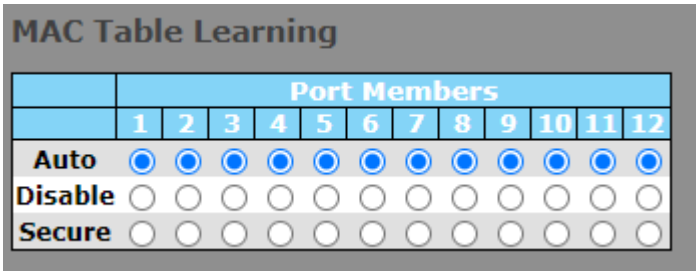
The allowed range is 10 to 1000000 seconds.

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.

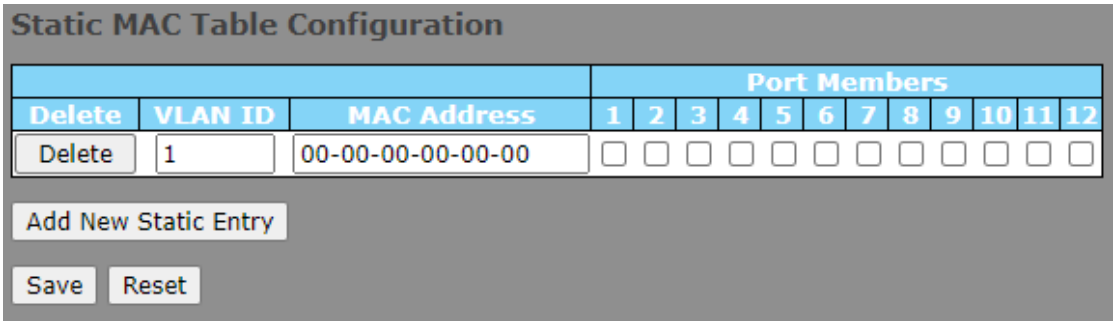
You can configure the port to dynamically learn the MAC address based upon the following settings:



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.

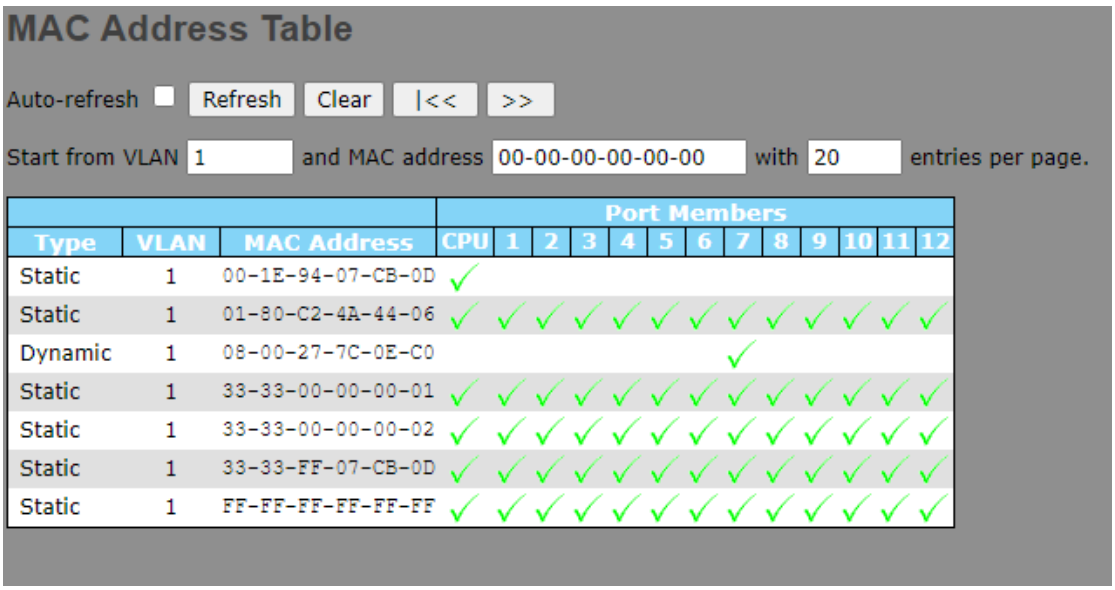
MAC Table

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.

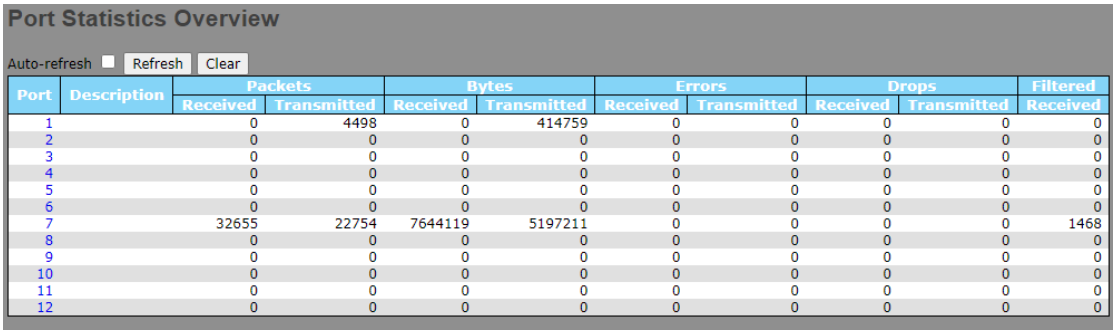


Label	Description
Type	Indicates whether the entry is a static or dynamic entry
MAC Address	The MAC address of the entry
VLAN	The VLAN ID of the entry
Port Members	The ports that are members of the entry.

1.11.2 Port Statistics

Traffic Overview

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



Port	Description	Packets		Bytes		Errors		Drops		Filtered
		Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1		0	4498	0	414759	0	0	0	0	0
2		0	0	0	0	0	0	0	0	0
3		0	0	0	0	0	0	0	0	0
4		0	0	0	0	0	0	0	0	0
5		0	0	0	0	0	0	0	0	0
6		0	0	0	0	0	0	0	0	0
7		32655	22754	7644119	5197211	0	0	0	0	1468
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

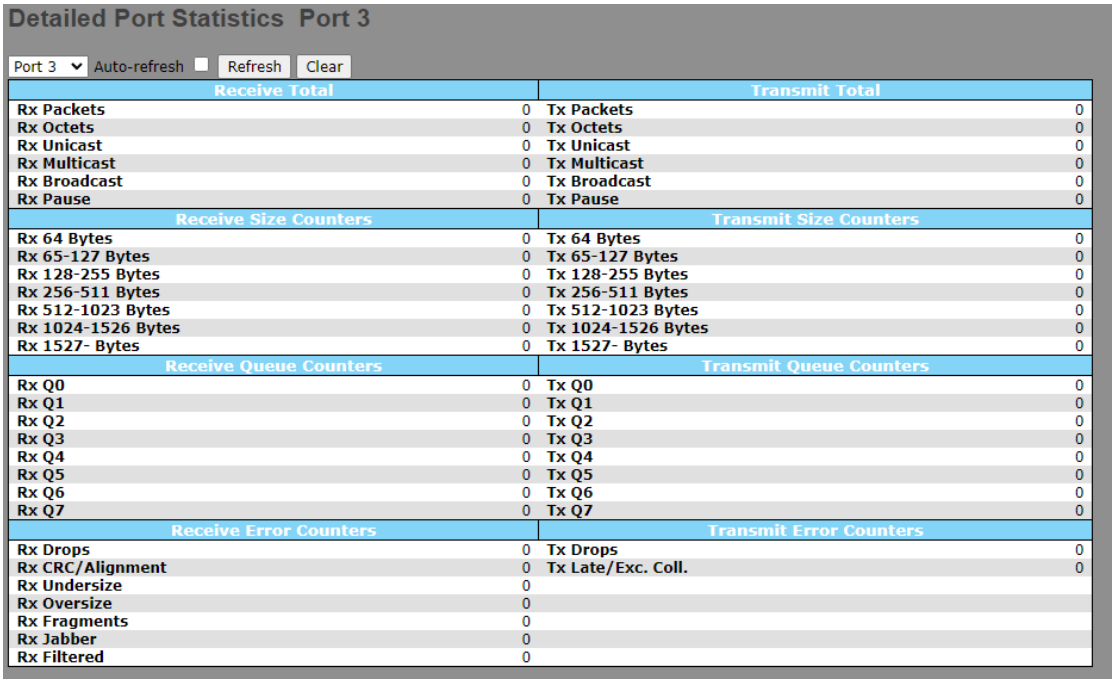
Label	Description
Port	The switch port number to which the following settings will be applied.
Packets	The number of received and transmitted packets per port
Bytes	The number of received and transmitted bytes per port
Errors	The number of frames received in error and the number of incomplete transmissions 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



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.

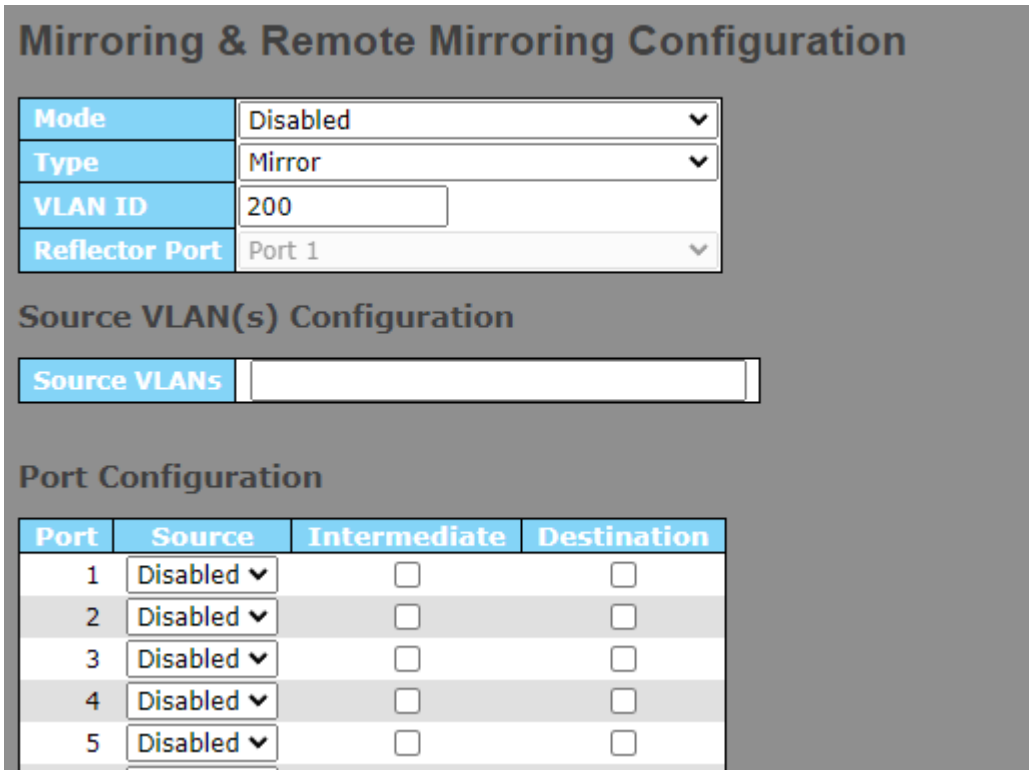
1.11.3 Port Monitoring

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.

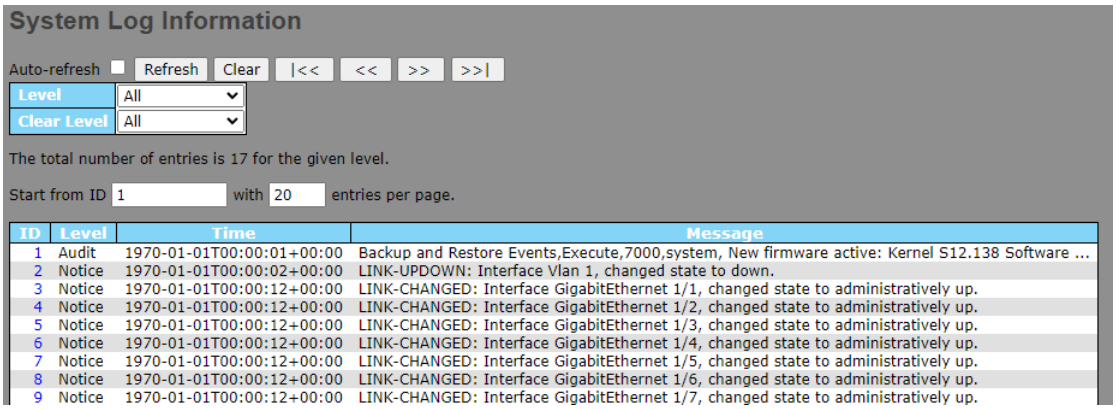


Label	Description
Mode	Enable or disable this function.
Type	Mirror: the switch is running on mirror mode. The source port(s) and destination port are located on this switch.

	Source: the switch is a source node for monitor flow. The source port(s) and intermediate port(s) are located on this switch. 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. 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. **Disabled**: Neither frames transmitted nor frames received are mirrored. **Both**: Frames received and frames transmitted are mirrored on the Intermediate/Destination port. **Rx only**: Frames received on this port are mirrored on the Intermediate/Destination port. Frames transmitted are not mirrored. **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

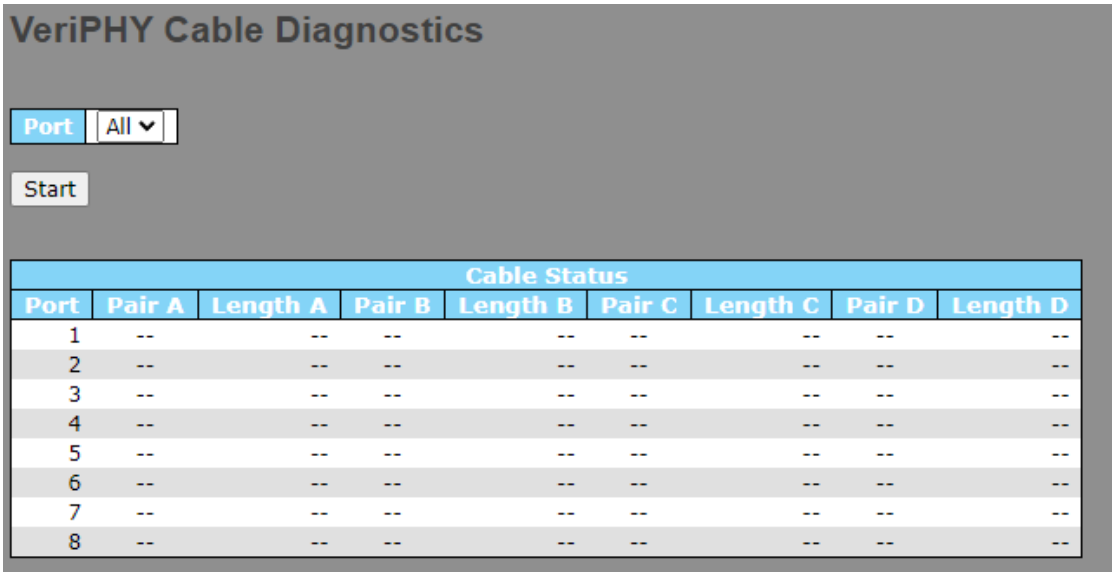
This page provides switch system log information.



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: **Notice:** Log messages that represent significant condition but not errors. **Informational**: Log informational messages. **Warning**: Log warning messages. **Error**: Log error messages. **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.



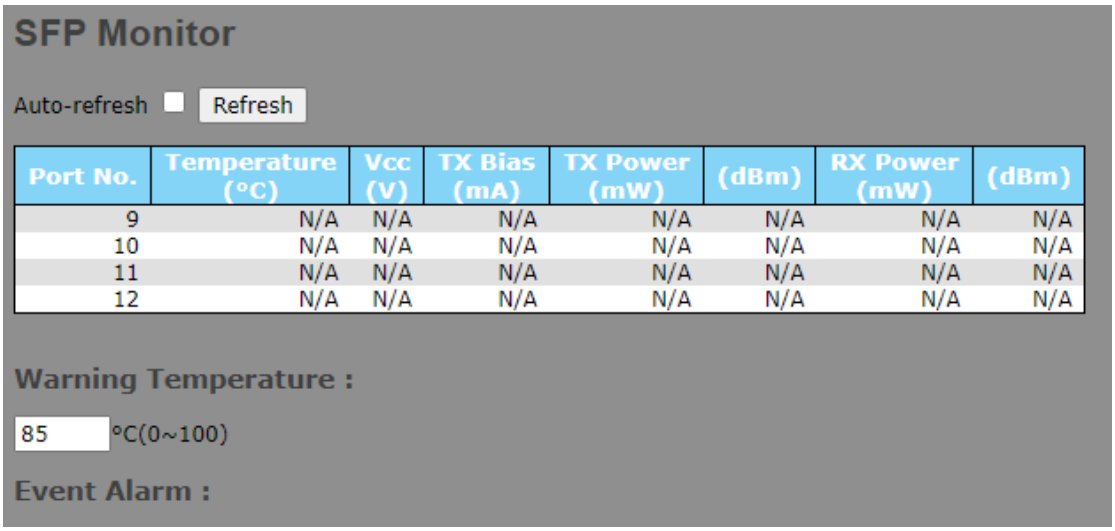
Press **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY diagnostics 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 Pair: the status of the cable pair Length: the length (in meters) of the cable pair

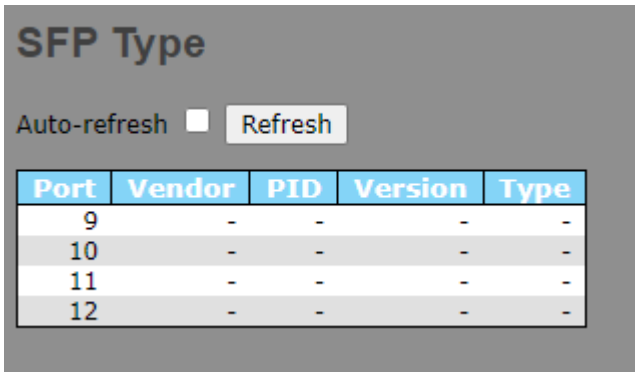
1.11.6 SFP Monitor

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.



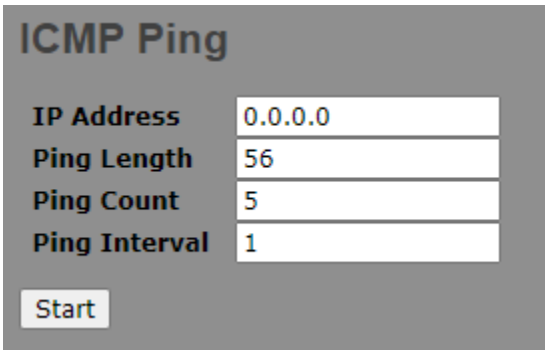
1.11.7 SFP Type

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



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

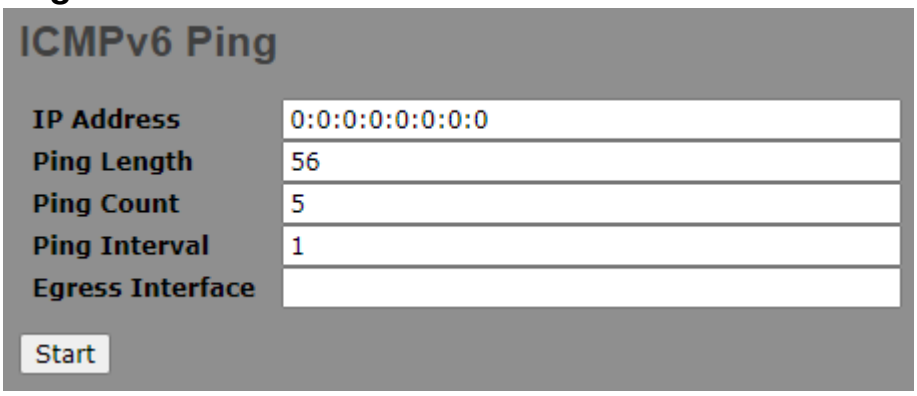
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms

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

1.11.9 CPU Load

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

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The

last 120 samples are graphed, and the last numbers are displayed as text as well.

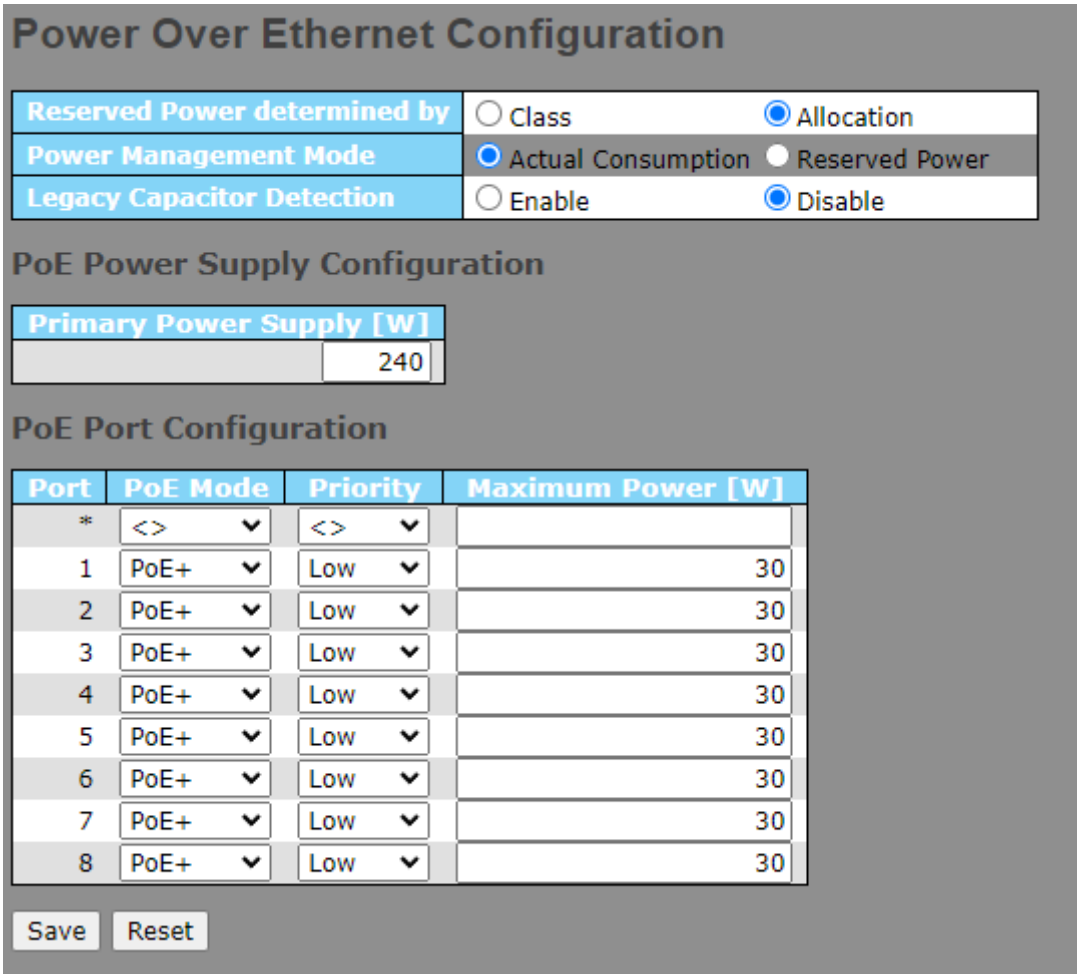
In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

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.



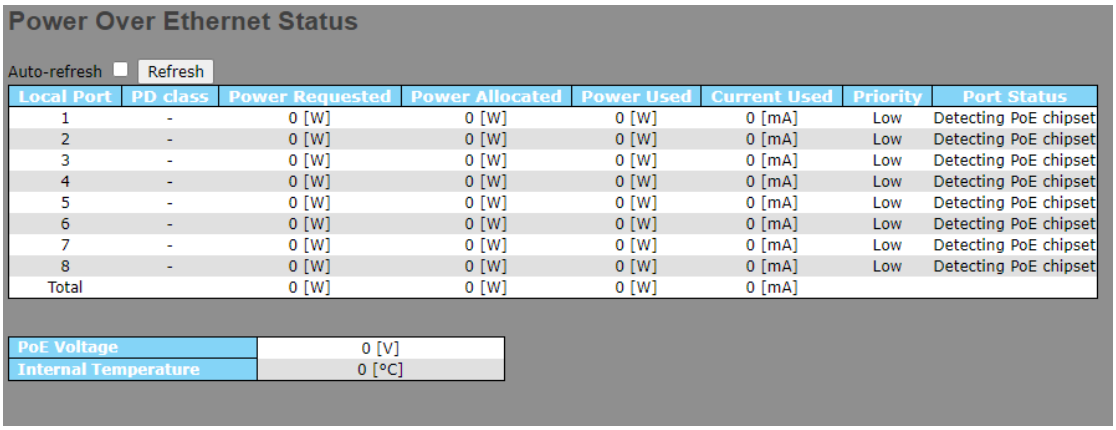
Label	Description
Reserved Power determined by	There are three modes for configuring how the ports/PDs may reserve power. 1. Allocated mode: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields. 2. Class mode: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect. 3. LLDP-MED mode: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available

	for a port, the port will reserve power using the class mode In this mode the Maximum Power fields have no effect For all modes: If a port uses more power than the reserved power for the port, the port is shut down.
Power Management Mode	There are 2 modes for configuring when to shut down the ports: 1. Actual Consumption: In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down. 2. Reserved Power: In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.
Legacy Capacitor Detection	Controls capacitor detection for legacy PD devices. Disabled: This feature is disabled. Enabled: This feature is enabled.
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. Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.
PoE Mode	The PoE Mode represents the PoE operating mode for the port. Disabled: PoE disabled for the port.

	PoE : Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W) PoE+ : Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W)
Priority	The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical. The priority is used in the case where the remote devices requires more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.
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.

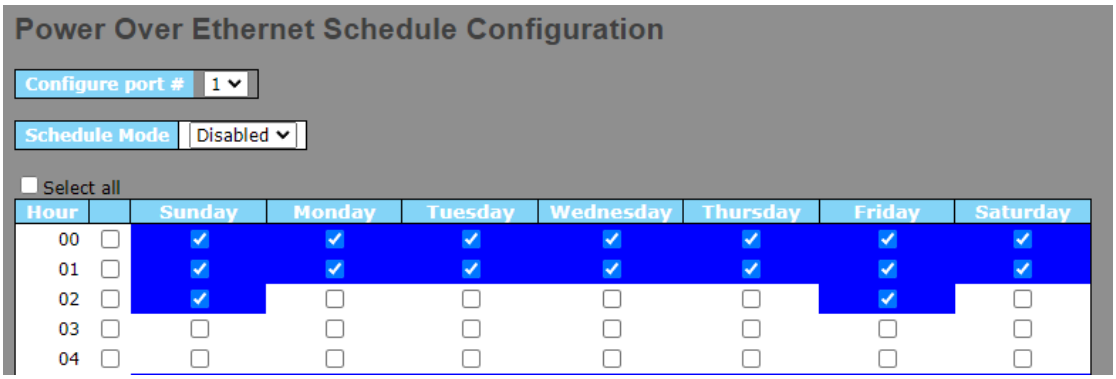


Label	Description
Local Port	This is the logical port number for this row.
PD Class	Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class. Five Classes are defined: Class 0: Max. power 15.4 W Class 1: Max. power 4.0 W Class 2: Max. power 7.0 W

	Class 3: Max. power 15.4 W Class 4: Max. power 30.0 W
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: PoE not available - No PoE chip found - PoE not supported for the port. PoE turned OFF - PoE disabled : PoE is disabled by user. PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down. No PD detected - No PD detected for the port. 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. Invalid PD - PD detected, but is not working correctly.
PoE Voltage	Display the working current of POE
Internal Temperature	Displays the operating temperature of the POE IC.

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.



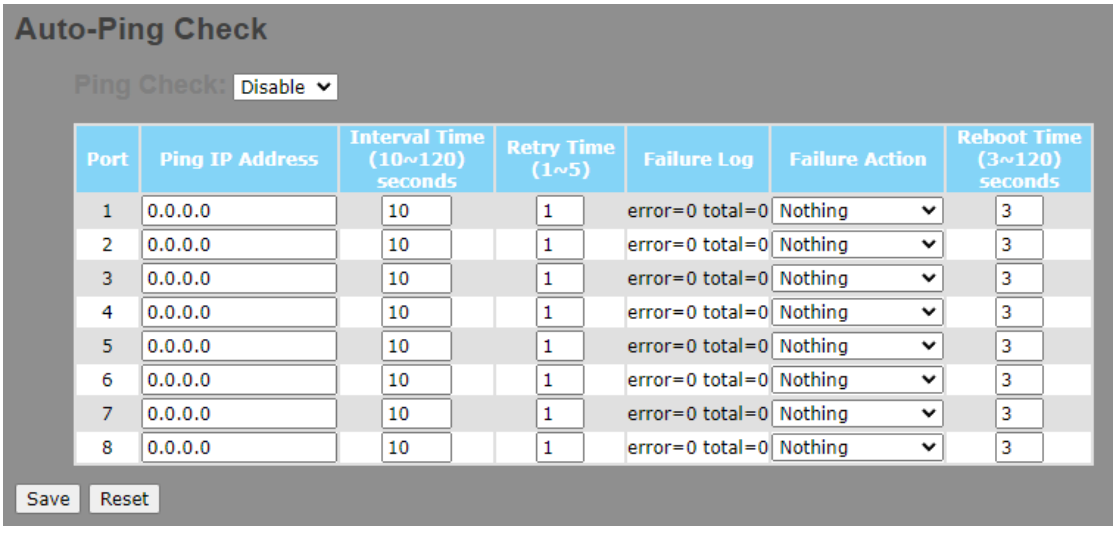
Label	Description
Configure Port	Choose port of the switch port number to configure
Mode	Indicates the PoE Schedule mode operation. Possible modes are: Enabled: Enable PoE Schedule configure. Disabled: Disable PoE Schedule configure.
Daily Schedule Form	Check Hours and Week checkbox to set port working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

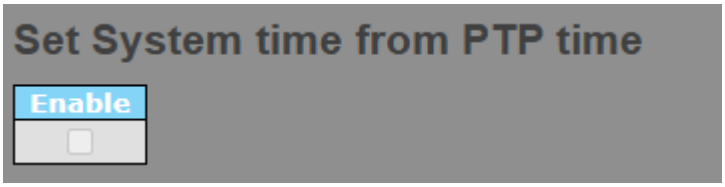
	Disabled: Disable Auto-Ping configure
Port	Port of the switch port number.
Ping IP Address	Send alive-checking packets to ip adress.
Interval Time	Set (10~120)seconds to control switch sending alive-checking packets each Interval Time.
Retry Time	If the connected devices fail to response, retry until numbers of set frequency .
Failure Log	Monitor connection status. If the connected devices succeed to response,total plus one; 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; Nothing: Nothing to do. Restart Forever: Try to supply power and cut power until connected devices success. Restart Once:Try to cut power and supply power once. Power On:Supply power to device. Power Off:Stop supplying power to device.
Reboot Time	Configure the switch delay (3-120)seconds sending alive-checking packet when the users choose 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.

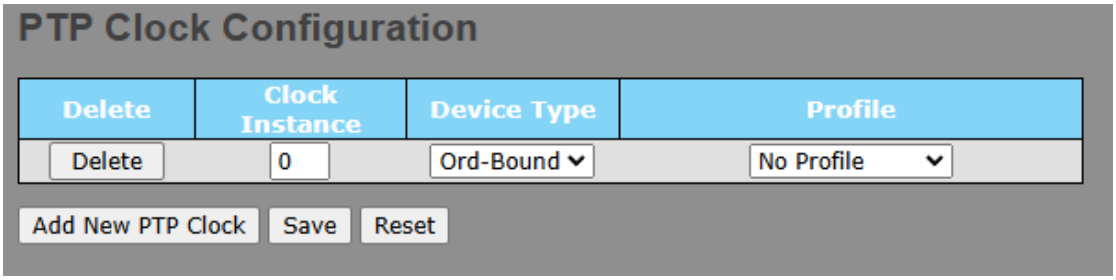
Set System time from PTP Time

Enable this function , switch will auto sync ptp time to system time .



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]. 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. **1. Ord-Bound -** clock's Device Type is Ordinary-Boundary Clock. **2. P2p Transp -** clock's Device Type is Peer to Peer Transparent Clock. **3. E2e Transp -** clock's Device Type is End to End Transparent Clock. **4. Master Only -** clock's Device Type is Master Only. **5. Slave Only -** clock's Device Type is Slave Only.
Add New PTP Clock	Create PTP instance
Save	Save PTP instance config .
reset	Cancel PTP Instance config .

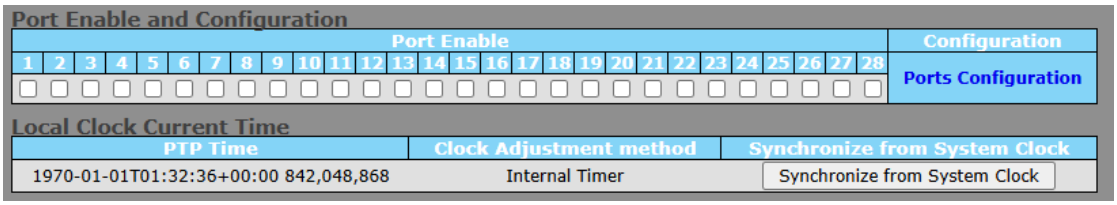
PTP Clock Instance

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

Clock type and Profile

This page will show the PTP instance Device type and Profile info

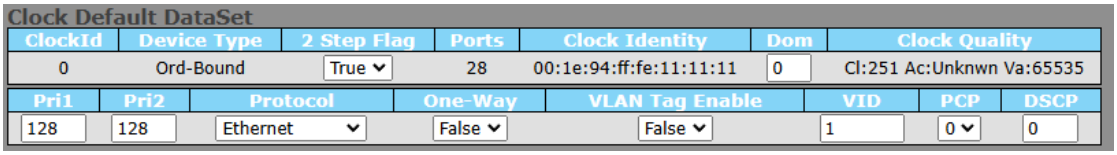
Lock Current Time



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. **1. Ord-Bound -** Clock's Device Type is Ordinary-Boundary Clock.

	2. P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock. **3. E2e Transp -** Clock's Device Type is End to End Transparent Clock. **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. 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 Ethernet PTP over Ethernet multicast EthernetMixed PTP using a combination of Ethernet multicast and unicast IPv4Multi PTP over IPv4 multicast IPv4Mixed PTP using a combination of IPv4 multicast and unicast 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:11:11:11	0	False	0	0	00:1e:94:ff:fe:11:11:11	Cl:251 Ac:Unknwn Va:65535	128	128

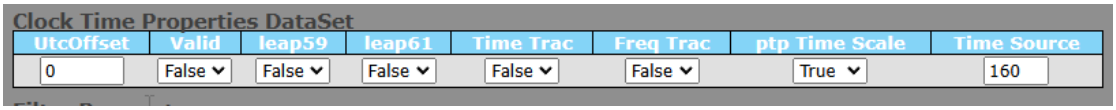
Label	Description
Parent Port Identity	Clock identity for the parent clock, if the local clock is not a slave, the value is the clocks own id.
Port	Port Id for the parent master port
P Stat	Parents Stats (always false).
Var	It is observed parent offset scaled log variance
Change Rate	Observed Parent 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:



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

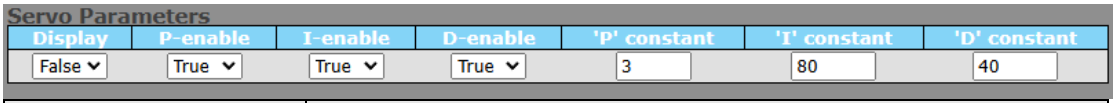
The default clock servo uses a PID regulator to calculate the current clock rate. i.e.

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

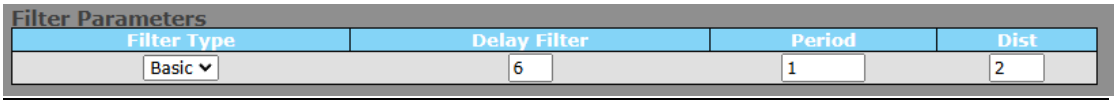
i.e. The minimum measured offset during Period samples is used in the calculation.

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,

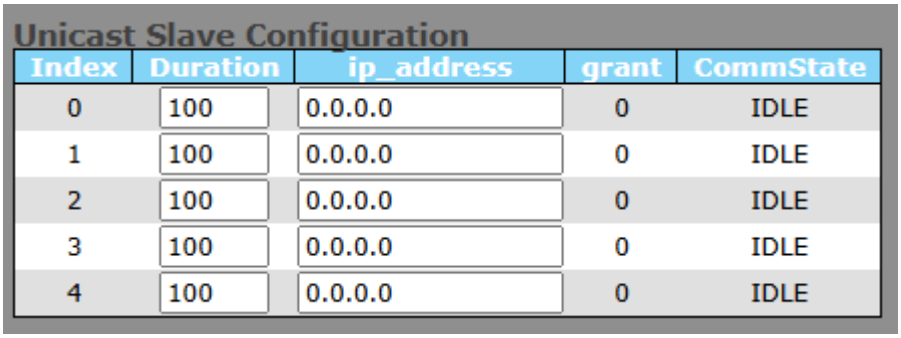
If Dist is >1 the offset is calculated using 'min' offset.



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

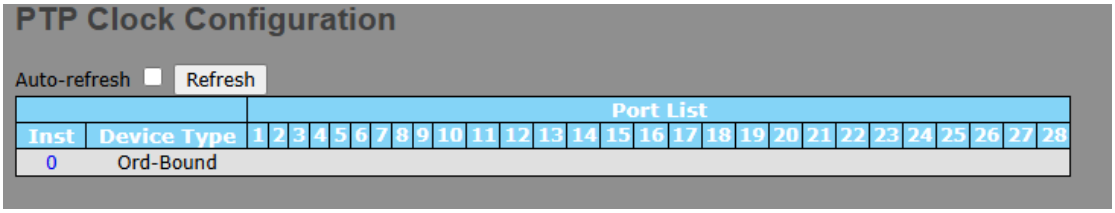
When operating in IPv4 Unicast mode, the slave is configured up to 5 master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then request Sync messages from the selected master.



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

PTP Status

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

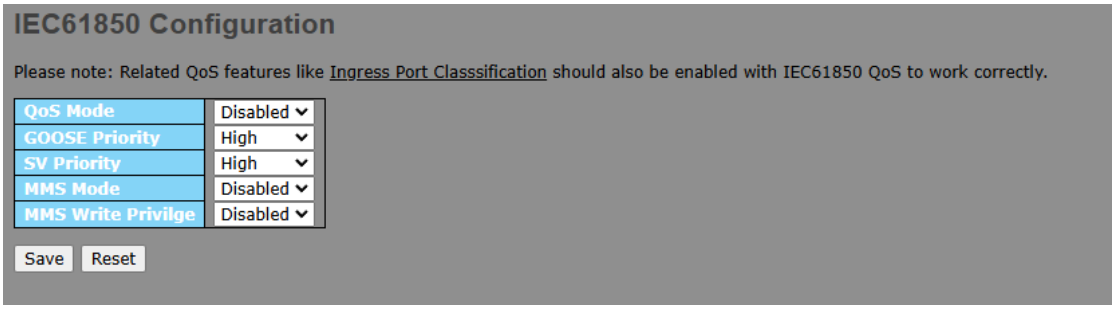


Label	Description
Inst	Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to monitor the Clock details.
Device Type	Indicates the Type of the Clock Instance. There are five Device Types. **1. Ord-Bound -** Clock's Device Type is Ordinary-Boundary Clock. **2. P2p Transp -** Clock's Device Type is Peer to Peer Transparent Clock.

	3. E2e Transp - Clock's Device Type is End to End Transparent Clock. **4. Master Only -** Clock's Device Type is Master Only. **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 .

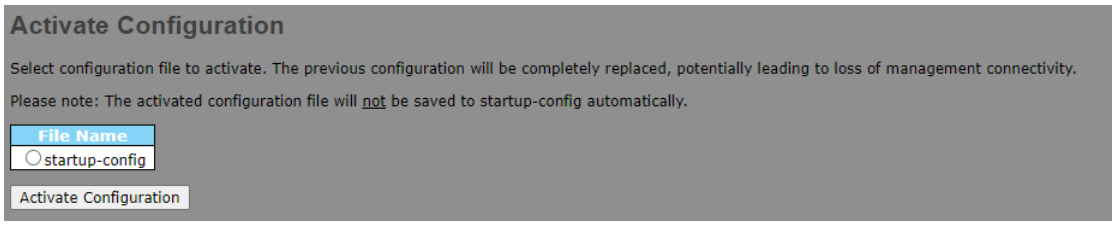


Label	Description
QoS Mode	Enable or Disable the QOS Mode.
GOOSE Priority	Setting Goose packet forwarding priority. (high / medium / low)
SV Priority	Setting Sampled Values protocol forwarding priority. (high / medium / low)
MMS Mode	Enable or Disable the MMS Mode.
MMS Write Privilge	Enable or Disable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

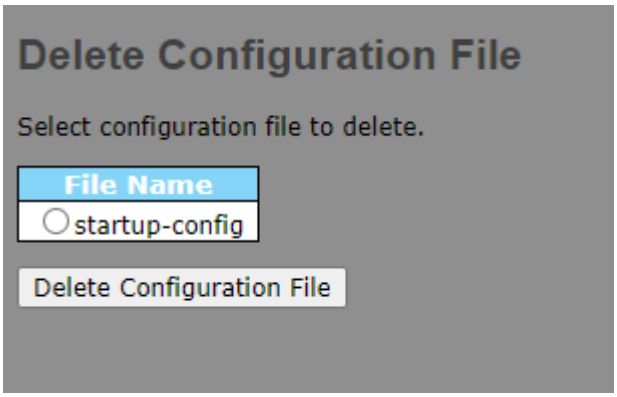
1.15 Configuration

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

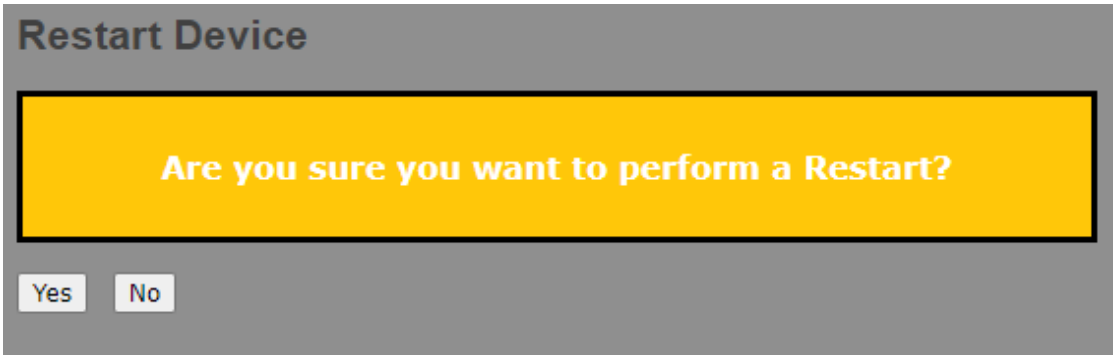
1.17.1 Factory Defaults

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

Label	Description
Keep IP	Select the check box ,after factory default , the switch will keep current IP Address .
Keep User / Password	Select the check box ,after factory default , the switch will keep current
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