KGD-600 Ver.C

Web Management Interface

User's Manual

Software Rev.1.0 or up

DOC.171015

TRADEMARKS

Ethernet is a registered trademark of Xerox Corp.

KTI Networks Inc. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of KTI Networks Inc. to provide notification of such revision or change.

For more information, contact:
15F-7, No. 79, Sec. 1, Hsin-Tai-Wu Rd.
Hsi-chih, New Taipei City, Taiwan
Fax: 886-2-26983873
E-mail: kti@ktinet.com.tw
URL: http://www.ktinet.com.tw/

Table of Contents

1. Web Management

The switch features an http server which can serve the management requests coming from any web browser software over TCP/IP network.

Web Browser

Compatible web browser software with JAVA script support

Microsoft Internet Explorer 4.0 or later

Set IP Address for the System Unit

Before the switch can be managed from web browser software, make sure a unique IP address is configured for the switch.

1.1 Start Browser Software and Making Connection

Start your browser software and enter the IP address of the switch unit to which you want to connect. The IP address is used as URL for the browser software to search the device.

URL: http://xxx.xxx.xxx.xxx/

Factory default IP address: *192.168.0.2*

Factory default username: *admin*

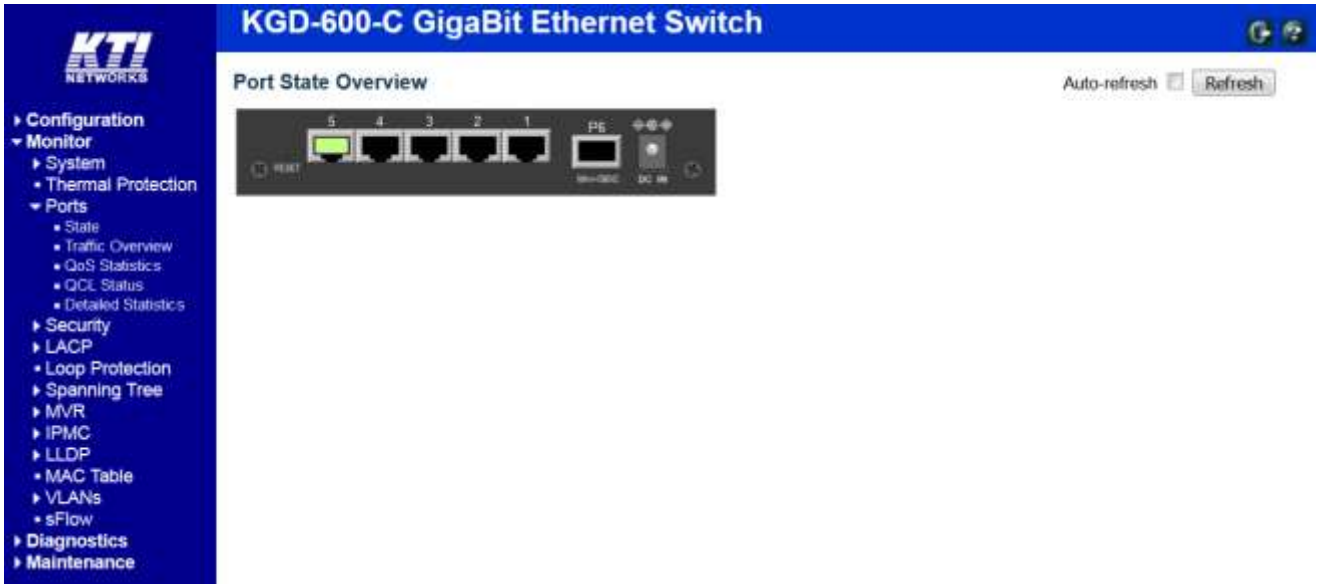
Factory default password: ↵

Note: no password with factory defaults

1.2 Login to the Switch Unit

When browser software connects to the switch unit successfully, a Login screen is provided for you to login to the device as the left display below:

"Port State Overview" page is displayed after a successful login.



[Logout] button and [Show Help] button

Auto-refresh

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

Refresh

Click to refresh the current page.

Port state icons are:

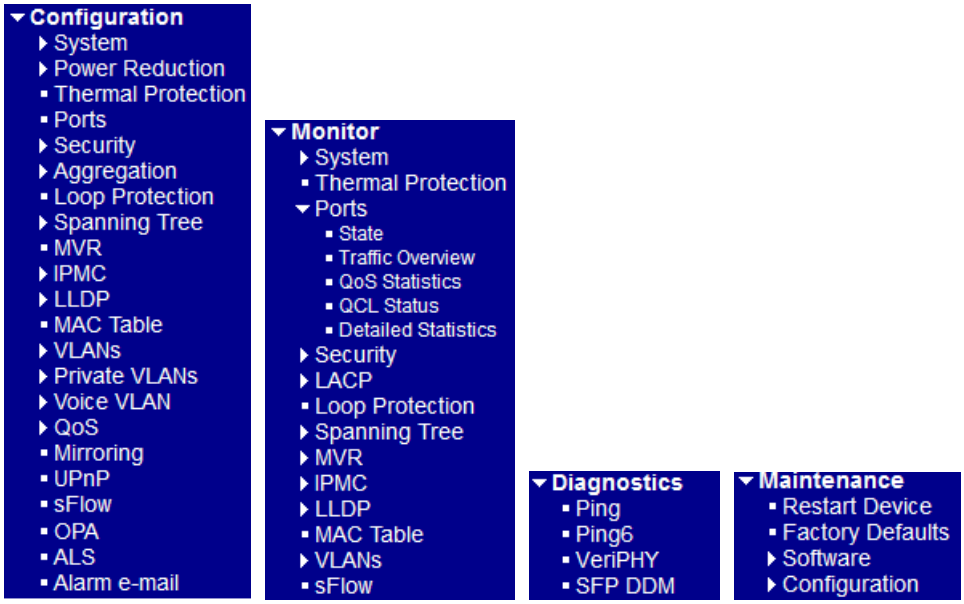
Status	Description
	RJ-45 port disabled
	RJ-45 port link down
	RJ-45 port link up
	SFP port disabled
	SFP port link down
	SFP port link in 1G full duplex
	SFP port link in 100M full duplex

The switch can accept more than one successful management connection simultaneously.

1.3 Main Management Menu

Main Menu:

Sub-menus:



Configuration

System	Switch information, IP configuration, SNTP setting, and Password setting
Power Reduction	EEE power saving configuration
Thermal Protection	Thermal protection is used to protect the chip from getting overheated.
Ports	Port operation related configuration, frame size, and power saving control
Security	Switch & UI authentication configuration, Port access security control
Aggregation	Static and LACP port link aggregation related configuration
Loop Protection	Configuration for port loop detection and protection
Spanning Tree	STP bridge, MSTI and CIST configuration
MVR	MVR feature enables multicast traffic forwarding on the Multicast VLANs.
IPMC	IGMP and MLD Snooping
LLDP	LLDP configuration
MAC Table	MAC address learning settings and static MAC address port configuration
VLANs	VLAN groups and VLAN port-related configuration
Private VLANs	PVLAN groups and port isolation configuration
Voice VLAN	The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN,
QoS	QoS port ingress, egress and QCL configuration, Port rate control, QCL wizard

Mirroring	Port mirroring settings
UPnP	Configuration for UPnP (**U**niversal **P**lug and **P**lay) feature
sFlow	sFlow is an industry standard technology for monitoring switched networks.
OPA	Optical Power Alarm function
ALS	Auto Laser Shutdown function (Hardware Ver.E up)
Alarm e-mail	Alarm notification configuration via SMTP Email

Monitor

System	System information and system log information
Thermal Protection	Display port temperature and status
Ports	Port link status, traffic statistics, QoS statistics
Security	Switch & UI authentication, Port access security status
LACP	LACP system and port status
Loop Protection	Display port configuration and status for loop protection
Spanning Tree	Bridge status, Port status and RSTP/STP/MSTP statistics
MVR	Display IGMP and MLD snooping status and counters
IPMC	IGMP Snooping & MLR snooping groups learned, Router ports, Statistics
LLDP	LLDP neighbors information, Port statistics
MAC Table	Display of MAC address table
VLANs	Display VLAN membership and VLAN port status
sFlow	Display sFlow receiver status and port sample counters

Diagnostics

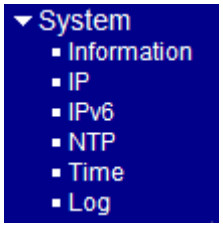
Ping	ICMP ping utility
Ping6	Ping utility for IPv6 devices
VeriPHY	Copper cable diagnostics for all copper ports
SFP DDM	SFP DDM information

Maintenance

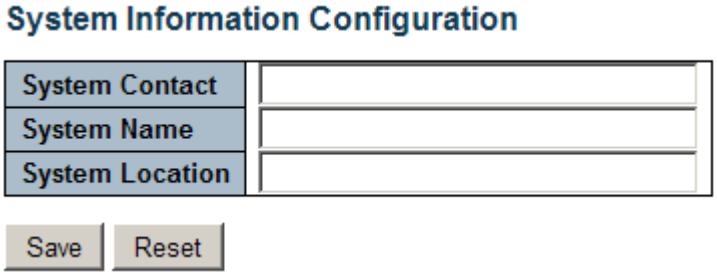
Restart Device	Command to reboot the switch
Factory Defaults	Command to restore the switch with factory default settings
Software	Command to update the switch firmware
Configuration	Command to save or upload the system configuration

2. Configuration

2.1 System



2.1.1 Information

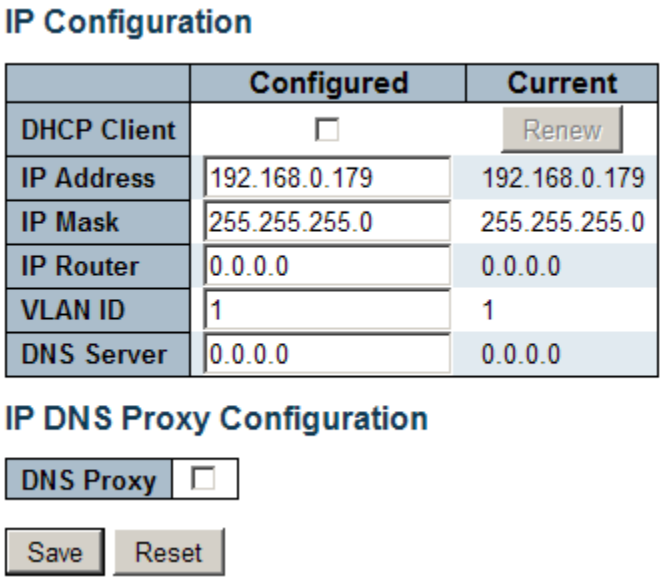


Configuration	Description
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is *0* to *255*, and the allowed content is the ASCII characters from *32* to *126*.
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is *0* to *255*.
System Location	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is *0* to *255*, and the allowed content is the ASCII characters from *32* to *126*.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Note:

1. *It is suggested to give each switch unit a system name as an alternative unique identification beside IP address.*
2. *The system Name, Contact, and Location settings are also used as SNMP MIBs.*

2.1.2 IP



Configuration	Description
DHCP Client	Enable the DHCP client by checking this box.
IP Address	Provide the IP address of this switch unit.
IP Mask	Provide the IP mask of this switch unit.
IP Router	Provide the IP address of the default router for this switch unit.
VLAN ID	Provide the managed VLAN ID. The allowed range is 1 through 4095. This setting is also called **MVID (Management VID)** as abbreviation.
DNS Server	Provide the IP address of the DNS Server in dotted decimal notation.
DNS Proxy	When DNS proxy is enabled, DUT will relay DNS requests to the current configured DNS server on DUT, and reply as a DNS resolver to the client device on the network.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Renew	Click to renew DHCP. This button is only available if DHCP is enabled.

Note:

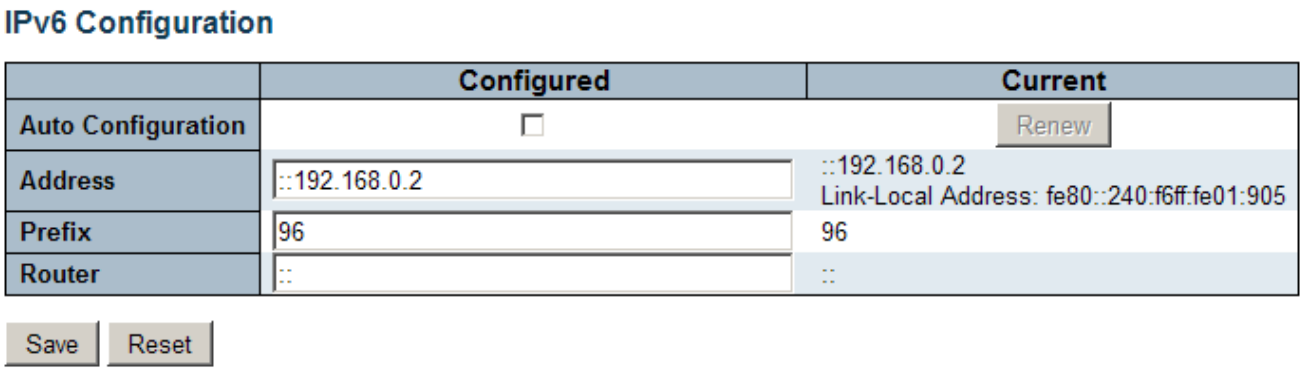
1. *If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.*
2. *The IP addresses should be in dotted decimal notation.*

2.1.2.1 Management VID (MVID) Operation Rules

The MVID setting restricts the ports that are allowed to communicate with the embedded system processor. The allowed ports are limited in the member ports of the VLAN with MVID. The operation rules are:

1. The embedded processor only accepts untagged management frames and rejects tagged frames.
2. The ingress port's VLAN ID (PVID) for the incoming management frames must match MVID value. Otherwise, the frames are dropped. Refer to Section 2.14.2 for PVID configuration.
3. The egress ports of the frames replied by the system processor are limited in the member ports of the VLAN with MVID.

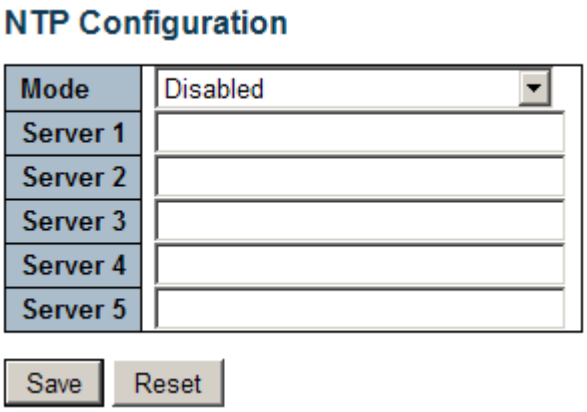
2.1.3 IPv6



Configuration	Description
Auto Configuration	DHCP Client Enable IPv6 auto-configuration by checking this box. If system cannot obtain the stateless address in time, the configured IPv6 settings will be used. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer. Enable the DHCP client by checking this box.
Address	Provide the IPv6 address of this switch. 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'.
Prefix	Provide the IPv6 Prefix of this switch. The allowed range is 1 to 128.
Router	Provide the IPv6 gateway address of this switch. 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'.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Renew	Click to renew IPv6 AUTOCONF. This button is only available if IPv6 AUTOCONF is enabled.

2.1.4 NTP



Configuration	Description
Mode	Indicates the NTP mode operation. Possible modes are: *Enabled*: Enable NTP mode operation. When enable NTP mode operation, the agent forward and to transfer NTP messages between the clients and the server when they are not on the same subnet domain. *Disabled*: Disable NTP mode operation.
Server #	Provide the NTP IPv4 or IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates 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 only appear once. It also used a following legally IPv4 address. For example, '::192.1.2.34'.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.1.5 Time

Time Zone Configuration

Time Zone Configuration	
Time Zone	None
Acronym	(0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled

Start Time settings	
Month	Jan
Date	1
Year	2000
Hours	0
Minutes	0
End Time settings	
Month	Jan
Date	1
Year	2000
Hours	0
Minutes	0
Offset settings	
Offset	1 (1 - 1440) Minutes

Save Reset

Configuration	Description
Time Zone	Indicates the NTP mode operation. Possible modes are:
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	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)

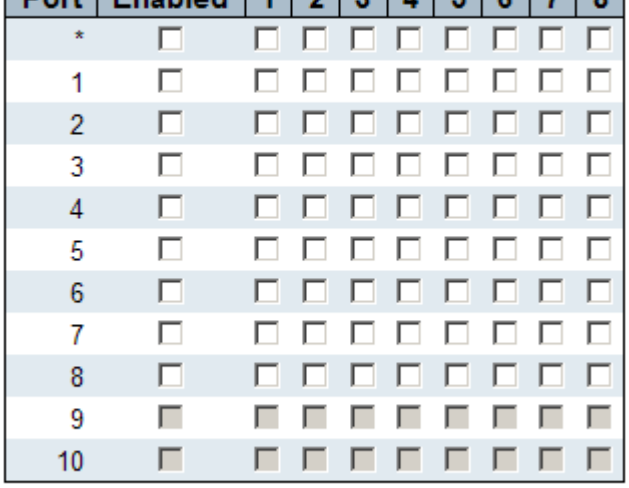
Start time settings

Month	Select the starting month.
Date	Select the starting day.
Year	Select the starting year number.
Hours	Select the starting hour.
Minutes	Select the starting minute.

End time settings

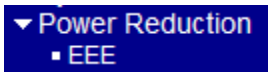
Month	Select the ending month.
Date	Select the ending day.
Year	Select the ending year number.
Hours	Select the ending hour.
Minutes	Select the ending minute.
Offset	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

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



Configuration	Description
Server Mode	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: *Enabled*: Enable server mode operation. *Disabled*: Disable server mode operation.
Server Address	Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.
Syslog Level	Indicates what kind of message will send to syslog server. Possible modes are: *Info*: Send information, warnings and errors. *Warning*: Send warnings and errors. *Error*: Send errors.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.2 Power Reduction



2.2.1 EEE

EEE Configuration

		EEE Urgent Queues							
Port	Enabled	1	2	3	4	5	6	7	8
*	☐	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐

Save Reset

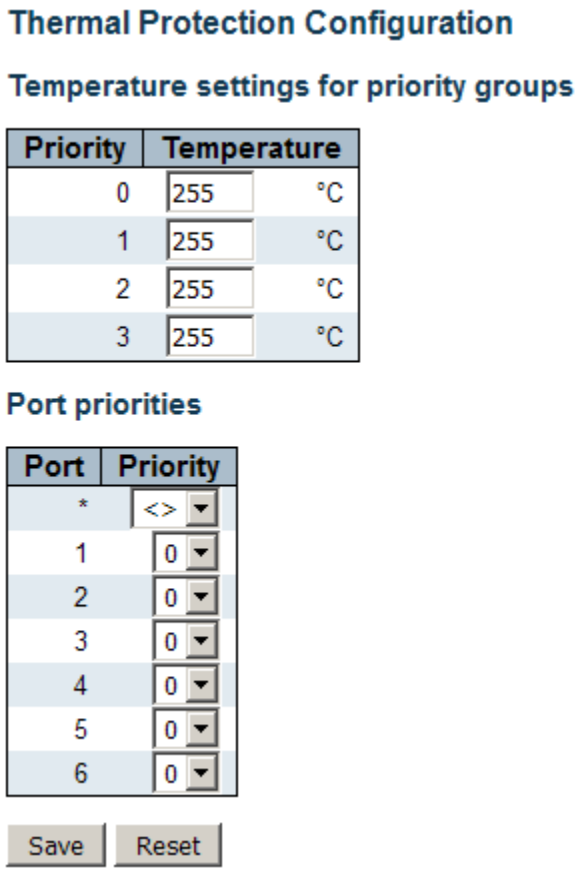
EEE is a power saving option that reduces the power usage when there is low or no traffic utilization.
EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The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

For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until 3000 bytes of data is ready to be transmitted. For not introducing a large delay in case that data less then 3000 bytes shall be transmitted, data are always transmitted after 48 us, giving a maximum latency of 48 us + the wakeup time.

If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.
EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode.
Ports that are not EEE-capable are grayed out and thus impossible to enable EEE for.

Configuration	Description
Port	The switch port number of the logical EEE port.
Enabled	Controls whether EEE is enabled for this switch port.
EEE Urgent Queues	Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until 3000 bytes are ready to be transmitted.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

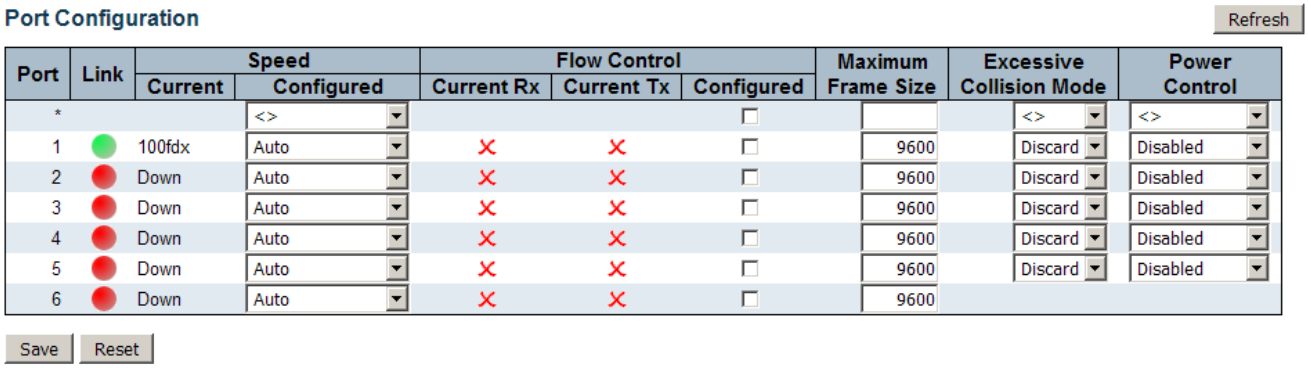
2.3 Thermal Protection



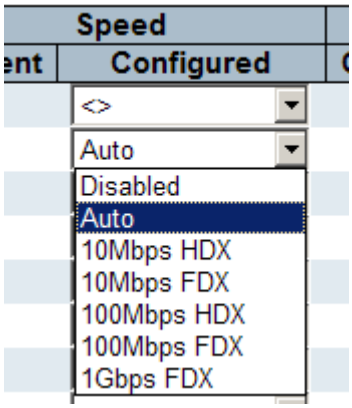
This page allows the user to inspect and configure the current setting for controlling thermal protection. Thermal protection is used to protect the chip from getting overheated. When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to decrease the power consumption. It is possible to arrange the ports with different priorities. Each priority can be given a temperature at which the corresponding ports shall be turned off.

Configuration	Description
Temperature settings for priority groups	
Temperature	The temperature at which the ports with the corresponding priority will be turned off. Temperatures between 0 and 255℃ are supported.
Port Priorities	The priority the port belongs to. 4 priorities are supported.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.4 Ports



Configuration	Description
Port	The port number associated to this configuration row
Link	The current link status is displayed graphically. Green indicates the link is up and red that it is down.
Speed - Current	Provide the current link speed of the port.
Speed - Configured	Select any available link speed for the given switch port.



***Disabled**:* disables the switch port operation.

***Auto**:* selects the highest speed that is compatible with a link partner.

***10Mbps HDX**:* selects fixed 10Mbps and half duplex

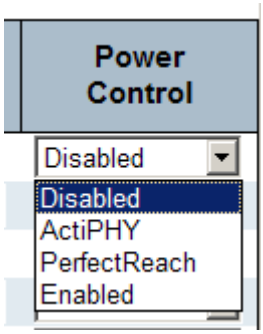
***10Mbps FDX**:* selects fixed 10Mbps and full duplex

***100Mbps HDX**:* selects fixed 100Mbps and half duplex

***100Mbps FDX**:* selects fixed 100Mbps and full duplex

***1Gbps FDX**:* selects auto-negotiation 1000Mbps and full duplex

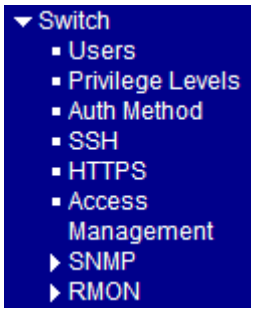
Flow Control – Current Rx	Whether pause frames on the port are obeyed
Flow Control – Current Tx	Whether pause frames on the port are transmitted
Flow Control – Configured	Click to enable flow control for fixed speed settings. When "*Auto*" Speed is selected for a port, this selection indicates the flow control capability that is advertised to the link partner.

Maximum Frame Size	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is *1518* bytes to *9600* bytes.
Excessive Collision Mode	Configure port transmission collision behavior. *Discard*: Discard frame after 16 collisions (default). *Restart*: Restart back-off algorithm after 16 collisions.
Power Control	The configured column allows for changing the power savings mode parameters per port.  ***Disabled***: All power savings mechanisms are disabled. ***ActiPHY***: Link down power savings is enabled. ***PerfectReach***: Link up power savings is enabled. ***Enabled***: Both link up and link down power savings are enabled.
Link Alarm	Port link fault alarm relay configuration Click to enable relay alarm function for the port

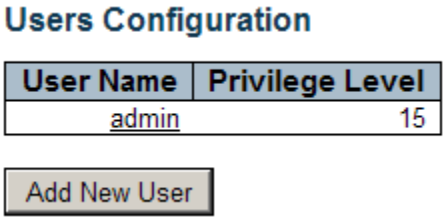
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Refresh	Click to refresh the page. Any changes made locally will be undone.

2.5 Security

2.5.1 Switch

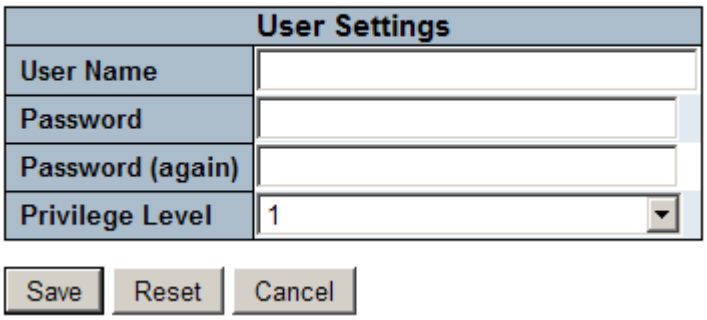


2.5.1.1 Users



Configuration	Description
User Name	The name identifying the user. Click also to edit a configured user.
Privilege Level	The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.
Add New User	Click to configure a new user.

Add User



Configuration	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 is a combination of letters, numbers and underscores. The name is for identifying the user.
Password	The password of the user The allowed string length is 0 to 31.
Privilege Level	The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most group privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Cancel	Click to undo any changes made locally and return to the Users.
Delete User	Delete the current user. This button is not available for new configurations. (Add new user)

2.5.1.2 Privilege Level

Privilege Level Configuration

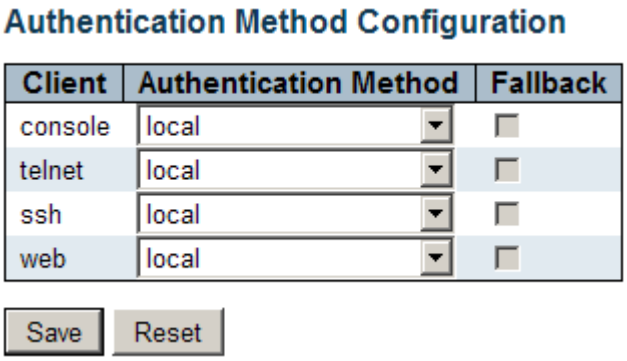
Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Debug	1	1	1	1
Diagnostics	5	10	5	10
EEE	5	10	5	10
IP	5	10	5	10
IPMC_LIB	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
LLDP_MED	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
MVR	5	10	5	10
Maintenance	15	15	15	15
Mirroring	5	10	5	10
PHY	5	10	5	10
POE	5	10	5	10
Port_Security	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
SNMP	5	10	5	10
Security	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
Timer	5	10	5	10
UPnP	5	10	5	10
VCL	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
kamr	5	10	5	10
ring	5	10	5	10
sFlow	5	10	5	10

Save Reset

Configuration	Description
Group Name	The name identifying the privilege group In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details: System: Contact, Name, Location, Timezone, Daylight Saving Time, Log. Security: Authentication, System Access Management, Port (contains Dot1x port,

	MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard. IP: Everything except 'ping'. Port: Everything except 'VeriPHY'. Diagnostics: 'ping' and 'VeriPHY'. Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance. Debug: Only present in CLI.
Privilege Levels	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.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

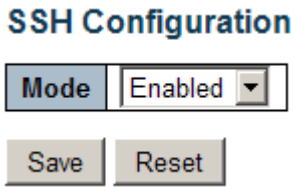
2.5.1.3 Auth Method



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

Configuration	Description
Client	The management client for which the configuration below applies.
Authentication Method	Authentication Method can be set to one of the following values: *none*: authentication is disabled and login is not possible. *local*: use the local user database on the switch stack for authentication. *radius*: use a remote RADIUS server for authentication. *tacacs+*: use a remote TACACS+ server for authentication.
Fallback	Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to a value other than 'none' or 'local'.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

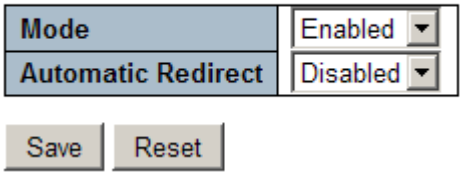
2.5.1.4 SSH



Configuration	Description
Mode	Indicates the SSH mode operation. Possible modes are: *Enabled*: Enable SSH mode operation. *Disabled*: Disable SSH mode operation.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

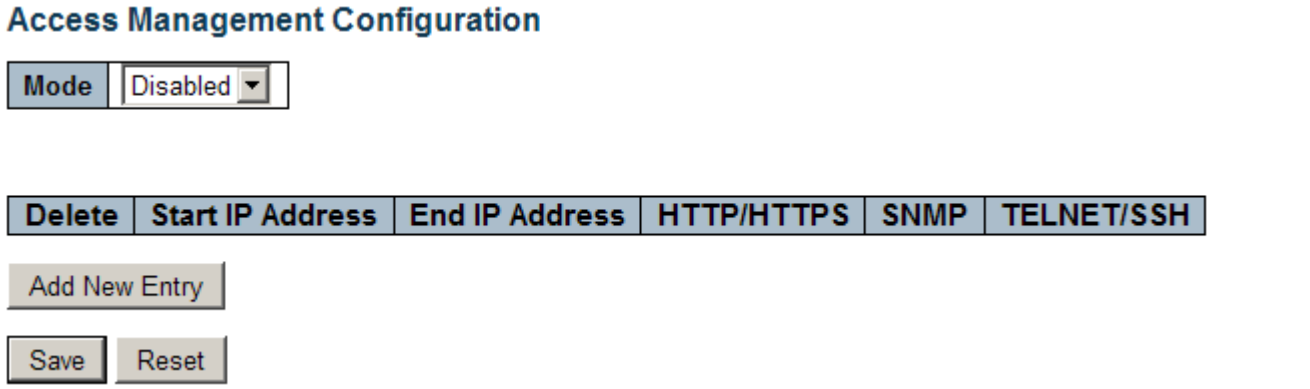
2.5.1.5 HTTPS

HTTPS Configuration

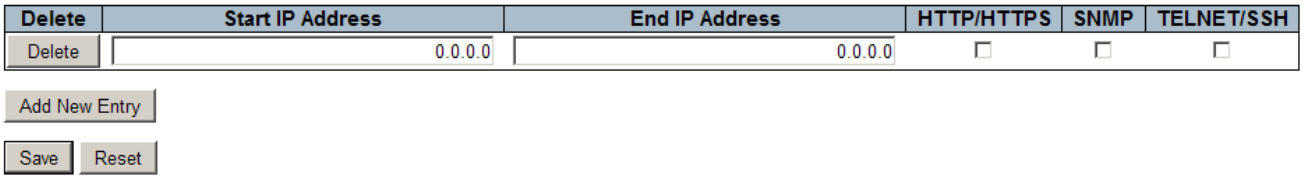


Configuration	Description
Mode	Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are: *Enabled*: Enable HTTPS mode operation. *Disabled*: Disable HTTPS mode operation.
Automatic Redirect	Indicates the HTTPS redirect mode operation. It is only significant if HTTPS mode "Enabled" is selected. Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled. Possible modes are: *Enabled*: Enable HTTPS redirect mode operation. *Disabled*: Disable HTTPS redirect mode operation.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.5.1.6 Access Management



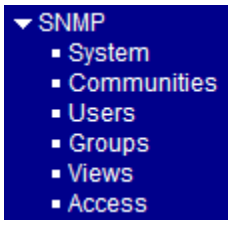
Add New Entry



Configure access management table on this page. The maximum number of entries is 16. If the application's type match any one of the access management entries, it will allow access to the switch.

Configuration	Description
Mode	Indicates the access management mode operation. Possible modes are: *Enabled*: Enable access management mode operation. *Disabled*: Disable access management mode operation.
Delete	Check to delete the entry. It will be deleted during the next save.
Start IP Address	Indicates the start IP address for the access management entry.
End IP Address	Indicates the end IP address for the access management entry.
HTTP/HTTPS	Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
SNMP	Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.
TELNET/SSH	Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.
Add New Entry	Click to add a new access management entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.5.1.7 SNMP



2.5.1.7.1 System

SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

SNMP Trap Configuration

Trap Mode	Enabled
Trap Version	SNMP v1
Trap Community	public
Trap Destination Address	192.168.0.100
Trap Destination IPv6 Address	::
Trap Authentication Failure	Enabled
Trap Link-up and Link-down	Enabled
Trap OPA	Enabled
Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	1
Trap Inform Retry Times	5

Save Reset

System Configuration	Description
Mode	Indicates the SNMP mode operation. Possible modes are: Enabled: Enable SNMP mode operation. ***Disabled:*** Disable SNMP mode operation.
Version	Indicates the SNMP supported version. Possible versions are: ***SNMP v1:*** Set SNMP supported version 1. ***SNMP v2c:*** Set SNMP supported version 2c.

	SNMP v3: Set SNMP supported version 3.
Read Community	Indicates the community read access string to permit access to SNMP agent. The allowed string length is ***0 ~ 255***, and the allowed content is the ASCII characters from 33 to 126. *Note: This field only suits when SNMP version is setting SNMPv1 or SNMPv2c. If SNMP version is setting SNMPv3, the community string will associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can use to restrict source subnet.*
Write Community	Indicates the community write-access string to permit access to SNMP agent. The allowed string length is ***0 ~ 255***, and the allowed content is the ASCII characters from 33 to 126. *Note: This field only suits when SNMP mode version setting SNMPv1 or SNMPv2c. If SNMP version is setting SNMPv3, the community string will associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can use to restrict source subnet.*
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.

Trap Configuration	**Description**
Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: ***Enabled:*** Enable SNMP trap mode operation. ***Disabled:*** Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Possible versions are: ***SNMP v1:*** Set SNMP trap supported version 1. ***SNMP v2c:*** Set SNMP trap supported version 2c. **SNMP v3:** Set SNMP trap supported version 3.
Trap Community	Indicates the community access string when send SNMP trap packet. The allowed string length is ***0 ~ 255***, and the allowed content is the ASCII characters from 33 to 126.
Trap Destination Address	Indicates the SNMP trap destination address.
Trap Destination IPv6 Address	Provide the trap destination IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates 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 only appear once. It also used a following legally IPv4 address. For example, '::192.1.2.34'.
Trap Authentication Failure	Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes are: ***Enabled:*** Enable SNMP trap authentication failure. ***Disabled:*** Disable SNMP trap authentication failure.
Trap Link-up and Link-down	Indicates the SNMP trap link-up and link-down mode operation. Possible modes are: ***Enabled:*** Enable SNMP trap link-up and link-down mode operation. ***Disabled:*** Disable SNMP trap link-up and link-down mode operation.
Trap OPA	Indicates the SNMP agent is permitted to generate SNMP OPA trap. ***Enabled:*** Enable SNMP OPA trap ***Disabled:*** Disable SNMP OPA trap
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: ***Enabled:*** Enable SNMP trap inform mode operation. ***Disabled:*** Disable SNMP trap inform mode operation.
Trap Inform Timeout	Indicates the SNMP trap inform timeout (seconds). The allowed range is ***0 ~ 2147***.
Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is ***0 ~ 255***.
Trap Probe Security Engine ID	Available for SNMP v3, 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	Available for SNMP v3, 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 between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
Trap Security Name	Available for SNMP v3, 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.

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

2.5.1.7.2 Communities

SNMPv3 Community Configuration

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

Add New Entry | Save | Reset

Configuration	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 the allowed content is the ASCII characters from 33 to 126. The community string will treat as security name and map a SNMPv1 or SNMPv2c community string.
Source IP	Indicates the SNMP access source address. A particular range of source addresses can use to restrict source subnet when combined with source mask.
Source Mask	Indicates the SNMP access source address mask.
Add New Entry	Click to add a new community entry.
Delete	Click to cancel the new entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click Add New Entry:

SNMPv3 Community Configuration

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

Add New Entry | Save | Reset

2.5.1.7.3 Users

SNMPv3 User Configuration

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

Add New Entry | Save | Reset

Configuration	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 the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In othe words, if user engine ID equal system engine ID then it is local user; otherwize it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: ***NoAuth, NoPriv:*** None authentication and none privacy. ***Auth, NoPriv:*** Authentication and none privacy. ***Auth, Priv:*** Authentication and privacy. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: ***None***: None authentication protocol. ***MD5***: An optional flag to indicate that this user using MD5 authentication protocol. ***SHA***: An optional flag to indicate that this user using SHA authentication protocol. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Password	A string identifying the authentication 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. The allowed content is the ASCII characters from 33 to 126.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: ***None:*** None privacy protocol. ***DES***: An optional flag to indicate that this user using DES authentication protocol.
Privacy Password	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

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

Click Add New Entry:

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
Delete			Auth, Priv	MD5		DES	

2.5.1.7.4 Groups

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	usm	default_user	default_rw_group

Add New Entry Save Reset

Configuration	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: ***v1:*** Reserved for SNMPv1. ***v2c:*** Reserved for SNMPv2c. ***usm:*** User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed

	string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

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

Click Add New Entry:

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	usm	default_user	default_rw_group
Delete	v1	public	

Add New Entry Save Reset

2.5.1.7.5 Views

SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
☐	default_view	included	.1

Add New Entry Save Reset

Configuration	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: ***included:*** An optional flag to indicate that this view sub-tree should be included.

	excluded: An optional flag to indicate that this view sub-tree should be excluded. General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID sub-tree overstep the 'excluded' view entry.
OID Subtree	The OID defining the root of the sub-tree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

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

Click Add New Entry:

SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
☐	default_view	included	.1
Delete		included	

Add New Entry Save Reset

2.5.1.7.6 Access

SNMPv3 Access Configuration

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

Add New Entry Save Reset

Configuration	**Description**
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: ***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 are: ***NoAuth, NoPriv:*** None authentication and none privacy. ***Auth, NoPriv:*** Authentication and none privacy. ***Auth, Priv:*** Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

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

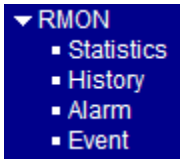
Click Add New Entry:

SNMPv3 Access Configuration

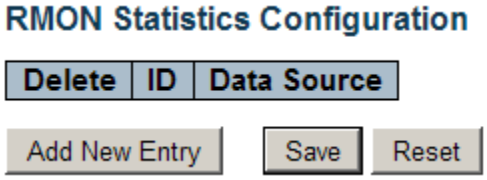
Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_ro_group	any	NoAuth, NoPriv	default_view	None
☐	default_rw_group	any	NoAuth, NoPriv	default_view	default_view
Delete	default_ro_group	any	NoAuth, NoPriv	None	None

Add New Entry Save Reset

2.5.1.8 RMON

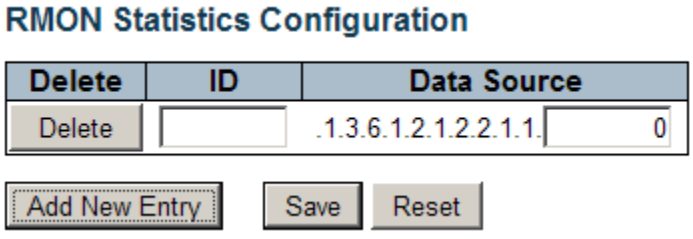


2.5.1.8.1 Statistics



Configuration	Description
Delete	Check to delete the RMON 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 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005.
Add New Entry	Click to add a new entry.
Delete	Click to cancel the new entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click Add New Entry:



2.5.1.8.2 History

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted

Add New Entry | Save | Reset

Configuration	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 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005.
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.
Add New Entry	Click to add a new entry.
Delete	Click to cancel the new entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click Add New Entry:

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1. 0	1800	50	

Add New Entry | Save | Reset

2.5.1.8.3 Alarm

RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index

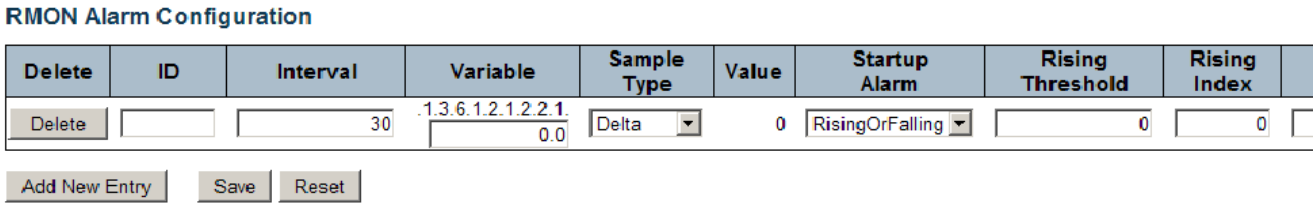
Add New Entry | Save | Reset

Configuration	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
Variable	Indicates the particular variable to be sampled, the possible variables are: ***InOctets***: The total number of octets received on the interface, including framing characters. ***InUcastPkts***: The number of uni-cast packets delivered to a higher-layer protocol. ***InNUcastPkts***: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. ***InDiscards***: The number of inbound packets that are discarded even the packets are normal. ***InErrors***: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. ***InUnknownProtos***: the number of the inbound packets that were discarded because of the unknown or un-support protocol. ***OutOctets***: The number of octets transmitted out of the interface , including framing characters. ***OutUcastPkts***: The number of uni-cast packets that request to transmit. ***OutNUcastPkts***: The number of broad-cast and multi-cast packets that request to transmit. ***OutDiscards***: The number of outbound packets that are discarded event the packets is normal. ***OutErrors***: The The number of outbound packets that could not be transmitted because of errors. ***OutQLen***: The length of the output packet queue (in packets).
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: ***Absolute***: Get the sample directly.

	Delta: Calculate the difference between samples (default).
Value	The value of the statistic during the last sampling period.
Startup Alarm	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: RisingTrigger alarm when the first value is larger than the rising threshold. FallingTrigger alarm when the first value is less than the falling threshold. RisingOrFallingTrigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
Rising Threshold	Rising threshold value (-2147483648-2147483647).
Rising Index	Rising event index (1-65535).
Falling Threshold	Falling threshold value (-2147483648-2147483647)
Falling Index	Falling event index (1-65535).

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

Click Add New Entry:



2.5.1.8.4 Event

RMON Event Configuration

Delete	ID	Desc	Type	Community	Event Last Time

Add New Entry | Save | Reset

Configuration	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***: The total number of octets received on the interface, including framing characters. ***log***: The number of uni-cast packets delivered to a higher-layer protocol. ***snmptrap***: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. ***logandtrap***: The number of inbound packets that are discarded even the packets are normal.
Community	Specify the community when trap is sent, the string length is from 0 to 127, the default is "public".
Event Last Time	Indicates the value of sysUpTime at the time this event entry last generated an event.
Add New Entry	Click to add a new entry.
Delete	Click to cancel the new entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

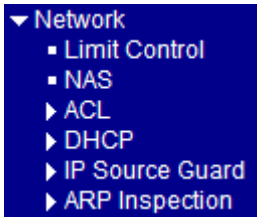
Click Add New Entry:

RMON Event Configuration

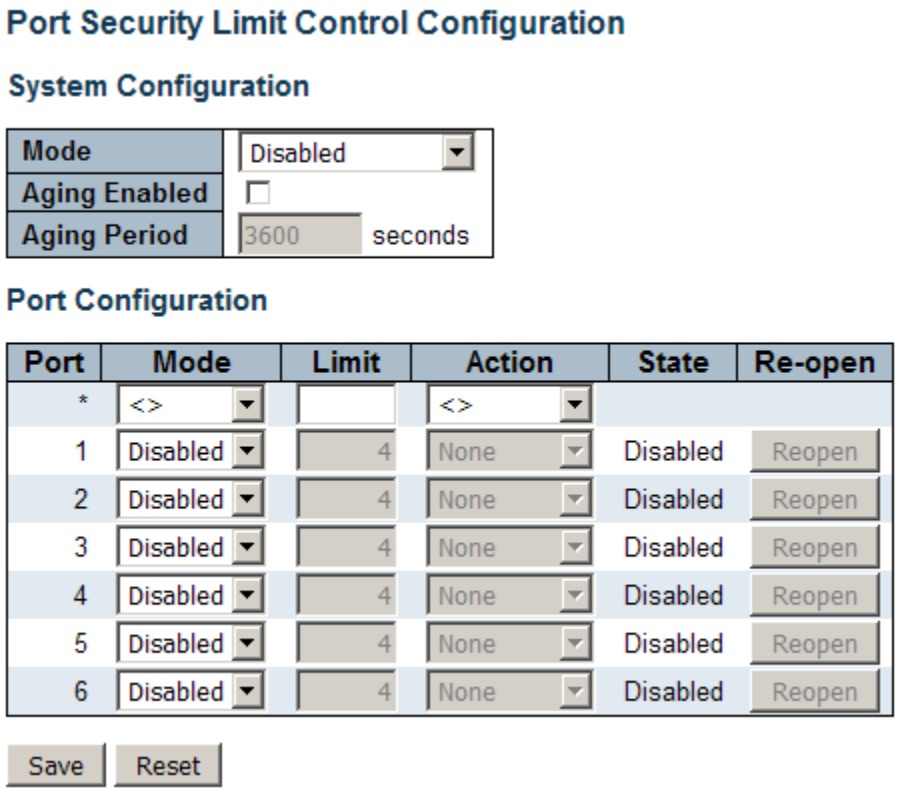
Delete	ID	Desc	Type	Community	Event Last Time
Delete			none	public	0

Add New Entry | Save | Reset

2.5.2 Network



2.5.2.1 Limit Control



Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below. The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learned on the port. The Limit Control configuration consists of two sections, a system- and a port-wide.

Configuration	Description
System Configuration	
Mode	Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks

	and corresponding actions are disabled.
Aging Enabled	If checked, secured MAC addresses are subject to aging as discussed under Aging Period.
Aging Period	If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality. The Aging Period can be set to a number between 10 and 10,000,000 seconds. To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.
Port Configuration	
Port	The port number to which the configuration below applies.
Mode	Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.
Limit	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.
Action	If Limit is reached, the switch can 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 are seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded. ***Shutdown***: If (Limit + 1) MAC addresses are seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down.

	There are three ways to re-open the port: 1) Boot the stack or elect a new masterthe switch, 2) Disable and re-enable Limit Control on the port or the stackswitch, 3) Click the Reopen button. ***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*.
Reopen	If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to *Shutdown* in the Action section. Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.5.2.2 NAS

Network Access Server Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	☐
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	☐
RADIUS-Assigned VLAN Enabled	☐
Guest VLAN Enabled	☐
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	☐

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	☐	☐	☐			
1	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize

Save Reset

System Configuration	Description
Mode	Indicates if NAS is globally enabled or disabled on the switch stack. If globally disabled, all ports are allowed forwarding of frames.
Reauthentication Enabled	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Age Period below).
Reauthentication Period	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is

checked. Valid values are in the range 1 to 3600 seconds.

EAPOL Timeout — Determines the time between retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 255 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:

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between *10* and *1000000* seconds.

If reauthentication is enabled and the port is in a 802.1X-based mode, this is not so criticial, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Hold Time — This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Un-authorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the The switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between *10* and *1000000* seconds.

RADIUS-Assigned QoS Enabled

RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the

switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description). The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned QoS Class is enabled for that port. When unchecked, RADIUS-server assigned QoS Class is disabled for all ports.

RADIUS-Assigned VLAN Enabled

RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled for that port. When unchecked, RADIUS-server assigned VLAN is disabled for all ports.

Guest VLAN Enabled — A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled for all ports.

Guest VLAN ID — This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [*1: 4095*].

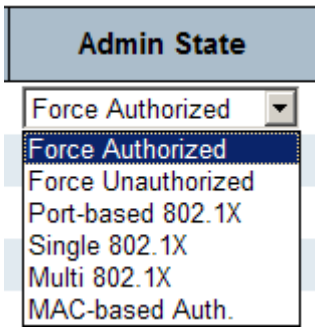
Max. Reauth. Count — The number of times that the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [*1: 255*].

Allow Guest VLAN if EAPOL Seen

The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received

on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration	Description
Port	The port number for which the configuration below applies.
Admin State	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:



Force Authorized: In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

Force Unauthorized: In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

Port-based 802.1X: In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

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

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Single 802.1X: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant. Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not

an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

MAC-based Auth.: Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

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

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

malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

RADIUS-Assigned QoS Enabled

When RADIUS-Assigned QoS is both globally enabled and enabled (checked) for a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

• Port-based 802.1X

• Single 802.1X

RADIUS attributes used in identifying a QoS Class:

Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

• All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3].

RADIUS-Assigned VLAN Enabled

When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port,

the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

• Port-based 802.1X

• Single 802.1X

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

RADIUS attributes used in identifying a VLAN ID:

RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

• The *Tunnel-Medium-Type*, *Tunnel-Type*, and *Tunnel-Private-Group-ID* attributes must all be present at least once in the Access-Accept packet.

• The switch looks for the first set of these attributes that have the same Tag value and fulfill the following requirements (if Tag == 0 is used, the *Tunnel-Private-Group-ID* does not need to include a Tag):

- Value of *Tunnel-Medium-Type* must be set to "IEEE-802" (ordinal 6).
- Value of *Tunnel-Type* must be set to "VLAN" (ordinal 13).
- Value of *Tunnel-Private-Group-ID* must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

Guest VLAN Enabled

When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

This option is only available for EAPOL-based modes, i.e.:

• Port-based 802.1X

• Single 802.1X

• Multi 802.1X

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

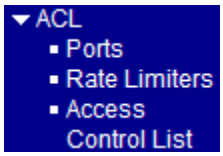
Guest VLAN Operation:

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between

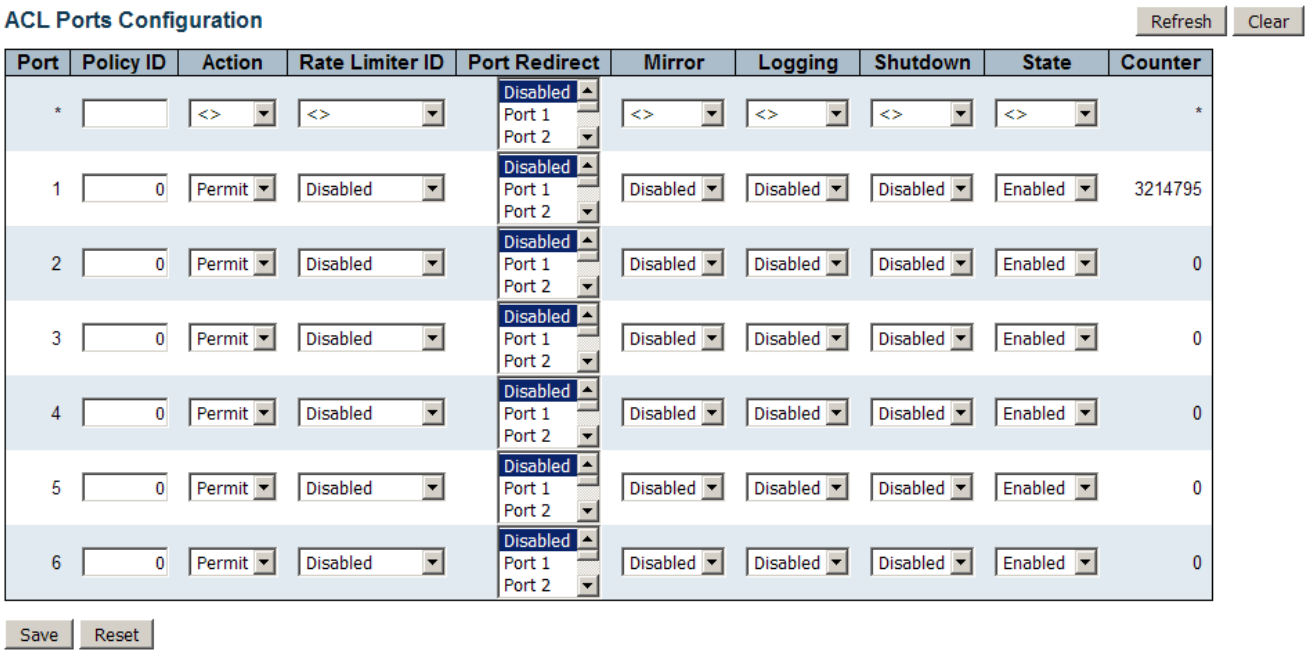
	transmissions of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.
Port State	The current state of the port. It can undertake one of the following values: ***Globally Disabled:*** NAS is globally disabled. ***Link Down:*** NAS is globally enabled, but there is no link on the port. ***Authorized:*** The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. ***Unauthorized:*** The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. ***X Auth/Y Unauth:*** The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect. Reauthenticate: Schedules a reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized. Reintialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

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

2.5.2.3 ACL



2.5.2.3.1 Ports



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

Mirror	Specify the mirror operation of this port. The allowed values are: *Enabled*: Frames received on the port are mirrored. *Disabled*: Frames received on the port are not mirrored. The default value is "*Disabled*".
Logging	Specify the logging operation of this port. The allowed values are: *Enabled*: Frames received on the port are stored in the System Log. *Disabled*: Frames received on the port are not logged. The default value is "*Disabled*". *Please note that the System Log memory size and logging rate is limited.*
Shutdown	Specify the port shut down operation of this port. The allowed values are: *Enabled*: If a frame is received on the port, the port will be disabled. *Disabled*: Port shut down is disabled. The default value is "*Disabled*".
State	Specify the port state of this port. The allowed values are: *Enabled*: To reopen ports by changing the volatile port configuration of the ACL user module. *Disabled*: To close ports by changing the volatile port configuration of the ACL user module. The default value is "*Enabled*".
Counter	Counts the number of frames that match this ACE.

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

2.5.2.3.2 Rate Limits

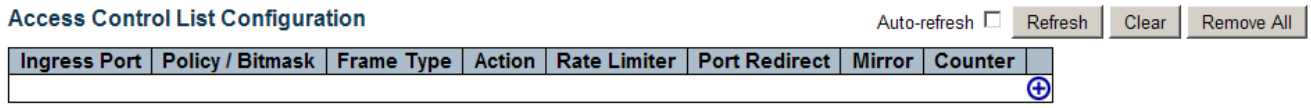
ACL Rate Limiter Configuration

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

Save Reset

Configuration	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The allowed values are: 0-3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.
Unit	Specify the rate unit. The allowed values are: *pps*: packets per second. *kbps*: Kbits per second.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.5.2.3.3 Access Control List



Configuration	Description
Ingress Port	Indicates the ingress port of the ACE. Possible values are: *All*: The ACE will match all ingress port. *Port*: The ACE will match a specific ingress port.
Policy/Bitmask	Indicates the policy number and bitmask of the ACE.
Frame Type	Indicates the frame type of the ACE. Possible values are: *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.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are *Disabled* or a specific port number. When *Disabled* is displayed, the port redirect operation is disabled.
Mirror	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: *Enabled*: Frames received on the port are mirrored. *Disabled*: Frames received on the port are not mirrored. The default value is "*Disabled*".
Counter	The counter indicates the number of times the ACE was hit by a frame.

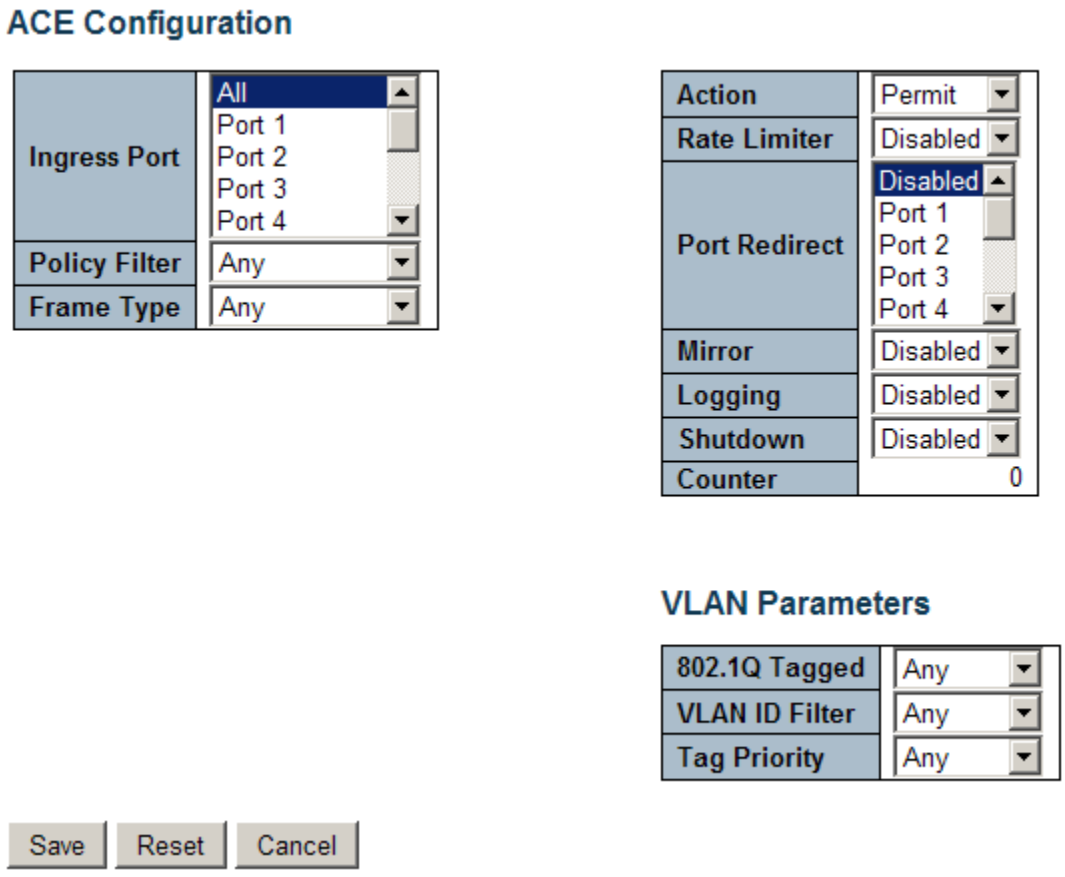
ACE modification buttons:

(+)	Inserts a new ACE before the current row.

(e)	Edits the ACE.
(↑)	Moves the ACE up the list.
(↓)	Moves the ACE down the list.
(X)	Deletes the ACE.
(+)	The lowest plus sign adds a new entry at the bottom of the list of ACL.

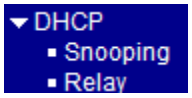
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page; any changes made locally will be undone.
Clear	Click to clear the counters.
Remove All	Click to remove all ACEs.

Click (+) to add one ACE entry:

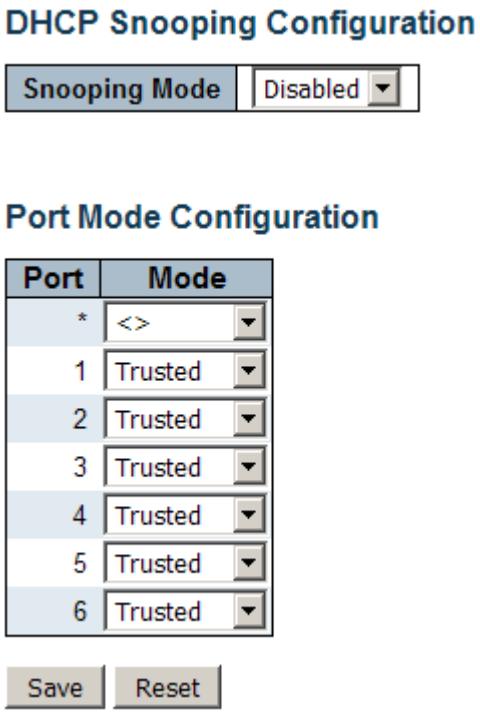


Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Cancel	Click to return to the previous page.

2.5.2.4 DHCP

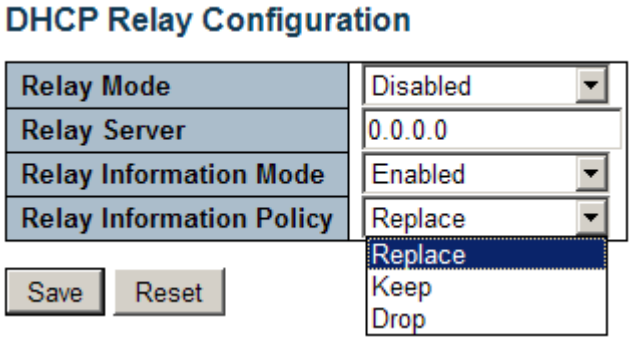


2.5.2.4.1 Snooping



Configuration	Description
Snooping Mode	Indicates the DHCP snooping mode operation. Possible modes are: ***Enabled*:** Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. ***Disabled*:** Disable DHCP snooping mode operation.
Port Mode	Indicates the DHCP snooping port mode. Possible port modes are: ***Trusted:*** Configures the port as trusted sources of the DHCP message. ***Untrusted*:** Configures the port as un-trusted sources of the DHCP message.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.5.2.4.2 Relay

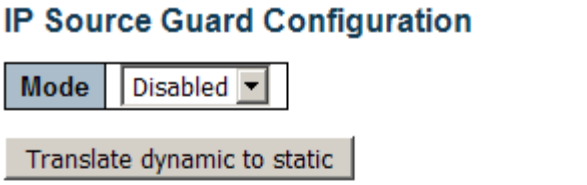


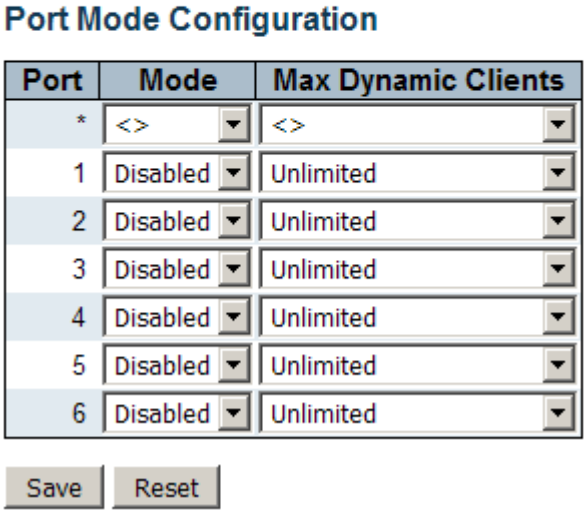
Configuration	Description
Relay Mode	Indicates the DHCP relay mode operation. Possible modes are: ***Enabled:*** Enable DHCP relay mode operation. When enable DHCP relay mode operation, the agent forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain. And the DHCP broadcast message won't flood for security considered. ***Disabled:*** Disable DHCP relay mode operation.
Relay Server	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.
Relay Information Mode	Indicates the DHCP relay information mode option operation. Possible modes are: ***Enabled:*** Enable DHCP relay information mode operation. When enable DHCP relay information mode operation, the agent insert specific information (option 82) into a DHCP message when forwarding to DHCP server and remove it from a DHCP message when transferring to DHCP client. It only works under DHCP relay operation mode enabled. ***Disabled:*** Disable DHCP relay information mode operation.
Relay Information Policy	Indicates the DHCP relay information option policy. When enable DHCP relay information mode operation, if agent receives a DHCP message that already contains relay agent information. It will enforce the policy. And it only works under DHCP relay information operation mode enabled. Possible policies are: ***Replace:*** Replace the original relay information when receive a DHCP message that already contains it. ***Keep:*** Keep the original relay information when receive a DHCP message that already contains it. ***Drop:*** Drop the package when receive a DHCP message that already contains relay information.

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

2.5.2.5 IP Source Guard

2.5.2.5.1 Configuration

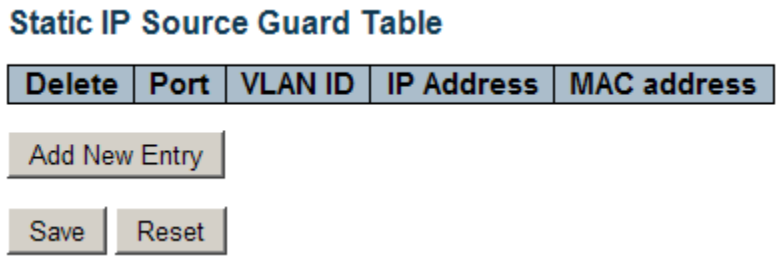




Configuration	Description
Mode of IP Source Guard Configuration	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
Port Mode Configuration	Specify IP Source Guard is enabled on which ports. Only when both Global Mode and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

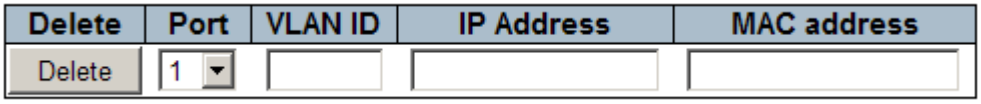
Translate dynamic to static	Click to translate all dynamic entries to static entries.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.5.2.5.2 Static Table

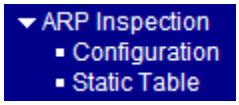


Configuration	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings
VLAN ID	The VLAN ID for the settings
IP Address	Allowed Source IP address
MAC Address	Allowed MAC address
Add new entry	Click to add a new entry to the Static IP Source Guard table.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

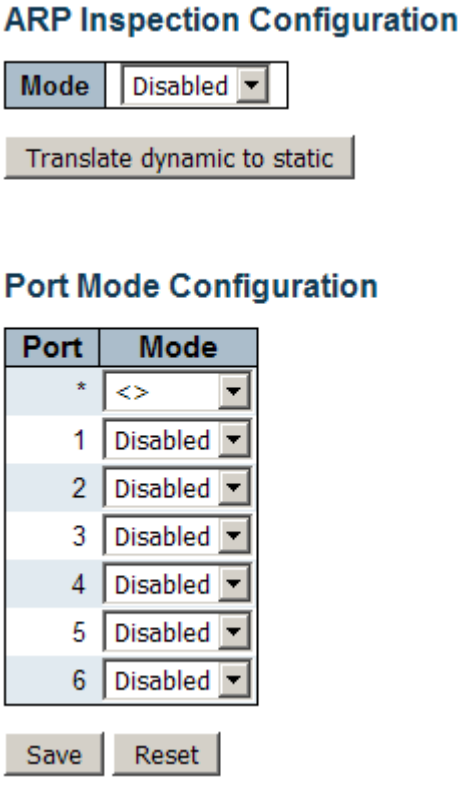
Click Add New Entry:



2.5.2.6 ARP Inspection

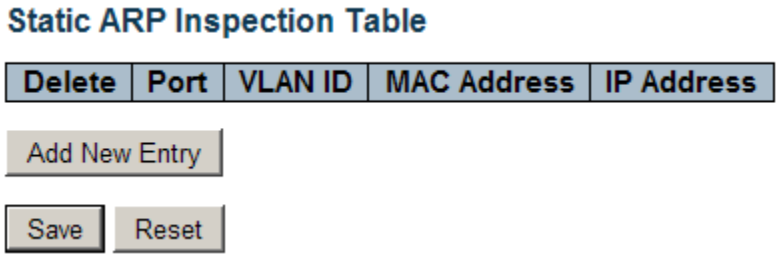


2.5.2.6.1 Configuration



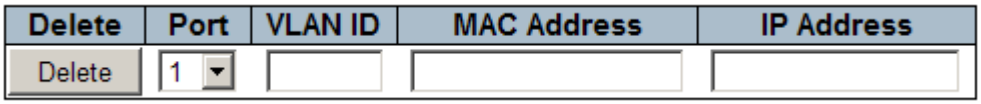
Configuration	Description
ARP Inspection Mode	Enable the Global ARP Inspection or disable the Global ARP Inspection.
Port Mode	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port.
Translate dynamic to static	Click to translate all dynamic entries to static entries.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.5.2.6.2 Static Table



Configuration	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings
VLAN ID	The VLAN ID for the settings
MAC Address	Allowed MAC address
IP Address	Allowed Source IP address
Add new entry	Click to add a new entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click Add New Entry:



2.5.3 AAA

Authentication Server Configuration

Common Server Configuration

Timeout	15	seconds
Dead Time	300	seconds

RADIUS Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	☐		1812	
2	☐		1812	
3	☐		1812	
4	☐		1812	
5	☐		1812	

RADIUS Accounting Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	☐		1813	
2	☐		1813	
3	☐		1813	
4	☐		1813	
5	☐		1813	

TACACS+ Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	☐		49	
2	☐		49	
3	☐		49	
4	☐		49	
5	☐		49	

Save Reset

Common Server	**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 timeframe, 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.
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.

RADIUS Authentication Server Configuration

#	The RADIUS authentication server number for which the configuration applies
Enabled	Enable the server by checking this box.
IP Address(Hostname)	The IP address of the server expressed in dotted decimal notation.
Port	The UDP port to use on the server. If the port is set to zero (0), the default port (1812) is used for the server.
Secret	The secret - up to 29 characters long - shared between the server and the switch unit.

RADIUS Accounting Server Configuration

#	The RADIUS accounting server number for which the configuration applies
Enabled	Enable the server by checking this box.
IP Address(Hostname)	The IP address of the server expressed in dotted decimal notation.
Port	The UDP port to use on the server. If the port is set to zero (0), the default port (1812) is used for the server.
Secret	The secret - up to 29 characters long - shared between the server and the switch unit.

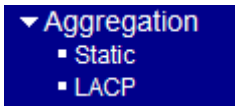
TACACS+ Authentication Server Configuration

#	The TACACS+ authentication server number for which the configuration applies
Enabled	Enable the server by checking this box.
IP Address(Hostname)	The IP address of the server expressed in dotted decimal notation.
Port	The UDP port to use on the server. If the port is set to zero (0), the default port (1812) is used for the server.
Secret	The secret - up to 29 characters long - shared between the server and the switch unit.

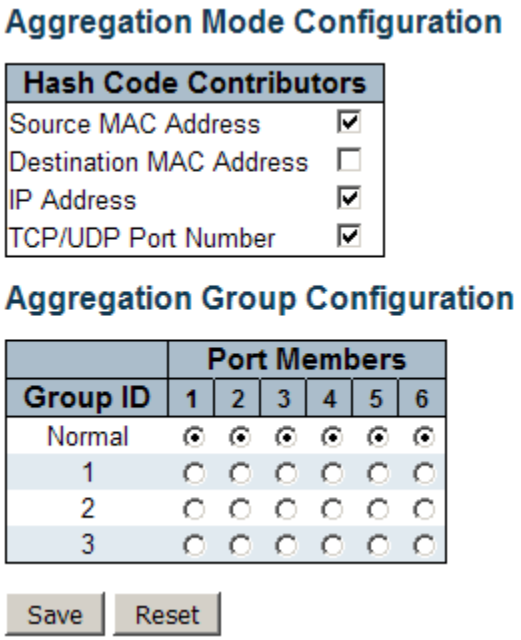
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.6 Aggregation

The Port Link Aggregation function can combine multiple physical switched ports, called "Aggregation Group" into one logical port. It allows making connection between two switches using more than one physical links to increase the connection bandwidth between two switches. Two aggregation modes, "Static" and "LACP" are supported.



2.6.1 Static



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

default, TCP/UDP Port Number is enabled.

Aggregation Group Configuration	
Group ID	Indicates the group ID for the settings contained in the same row. Group ID "*Normal*" indicates there is no aggregation. Only one group ID is valid per port.
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.6.2 LACP

LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	
1	☐	Auto		Active	Fast	32768
2	☐	Auto		Active	Fast	32768
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768

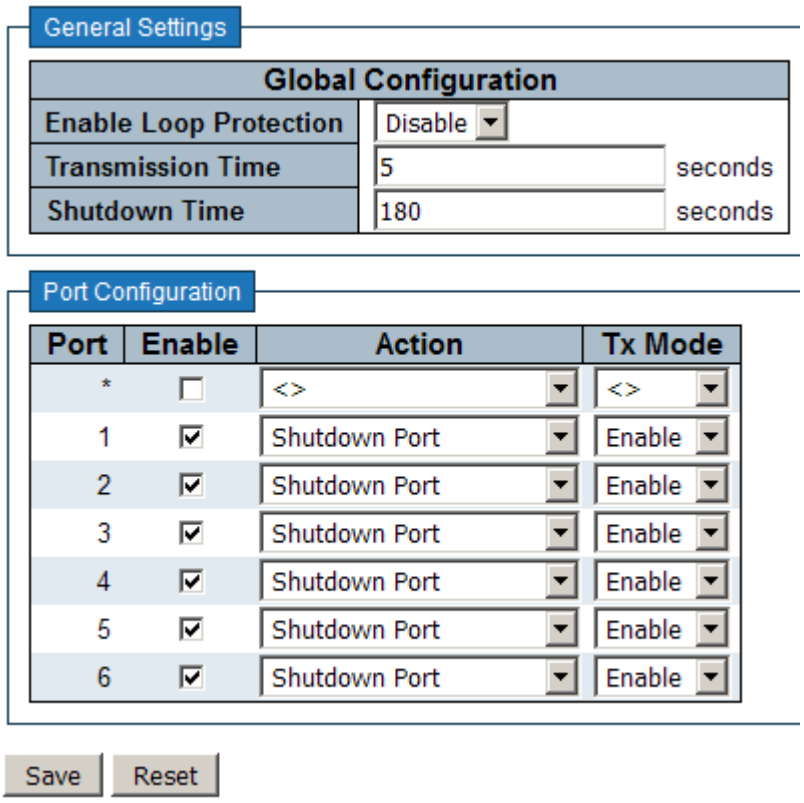
Save Reset

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

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

2.7 Loop Protection



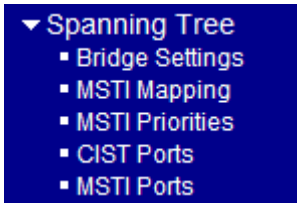
Configuration	**Description**
Enable Loop Protection	Controls whether loop protections is enabled (as a whole).
Transmission Time	The interval between each loop protection PDU sent on each port. valid values are 1 to 10 seconds.
Shutdown Time	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).
Port	The switch port number of the port
Enable	Controls whether loop protection is enabled on this switch port.

Action	Configures the action performed when a loop is detected on a port. Valid values are *Shutdown Port*, *Shutdown Port and Log* or *Log Only*.
Tx Mode	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

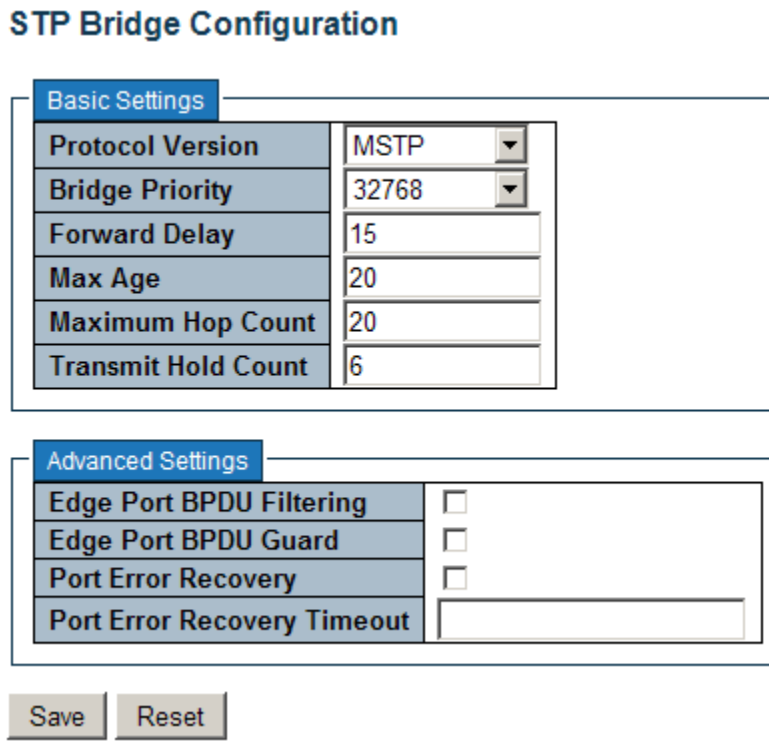
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.8 Spanning Tree

This section is used to set configuration for supporting Spanning Tree protocols including STP, RSTP, and MSTP.



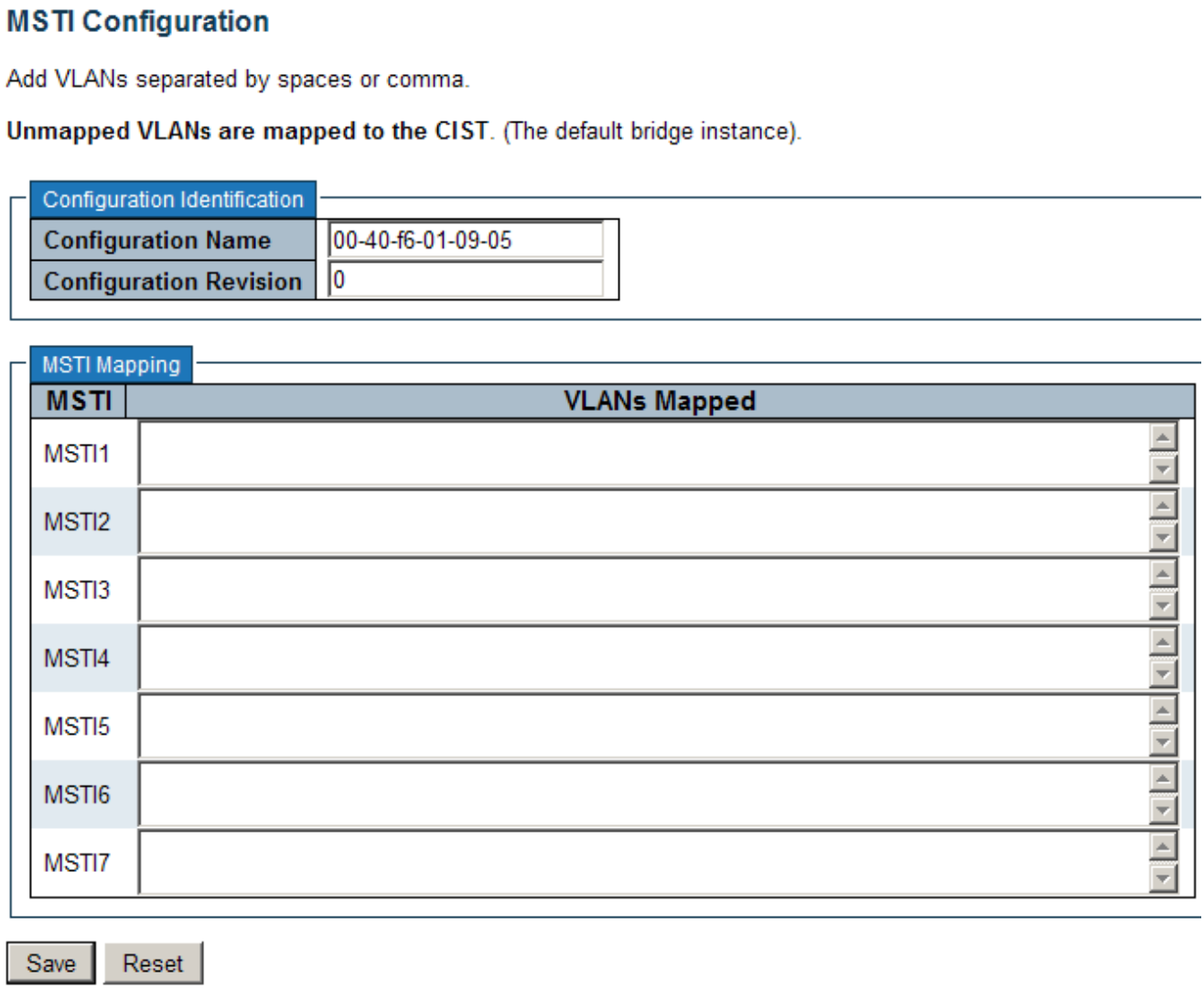
2.8.1 Bridge Settings



Basic Configuration	Description
Protocol Version	The STP protocol version setting Valid values: ***STP, RSTP, MSTP***
Bridge Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values: ***4 ~ 30 seconds***
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge Valid values: ***6 ~ 40 seconds*** *(Max Age must be <= (FwdDelay-1)*2)*
Maximum Hop Count	It defines how many bridges a root bridge can distribute its BPDU information. This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region.
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: ***1 ~ 10*** *BPDU's per second*
Advanced Configuration	
Edge Port BPDU Filtering	Check to configure a port *explicitly* 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 that has to pass before a port in the *error-disabled* state can be enabled. Valid values: ***30 ~ 86400*** *seconds (24 hours)*
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

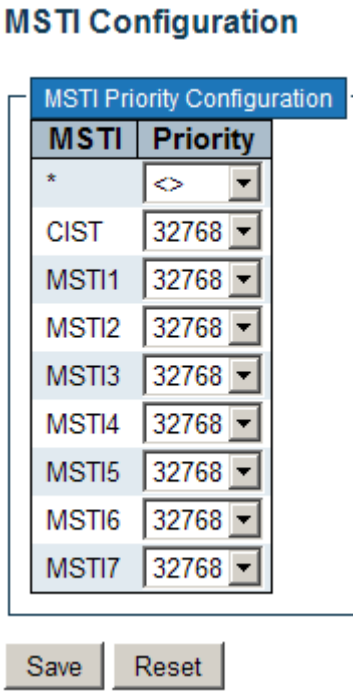
2.8.2 MSTI Mapping



Configuration	Description
Configuration Name	The name identifying the VLAN to MSTI mapping Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region) The name is at most 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between ***0 ~ 65535***.
MSTI Mapping	
MSTI	The bridge instance The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

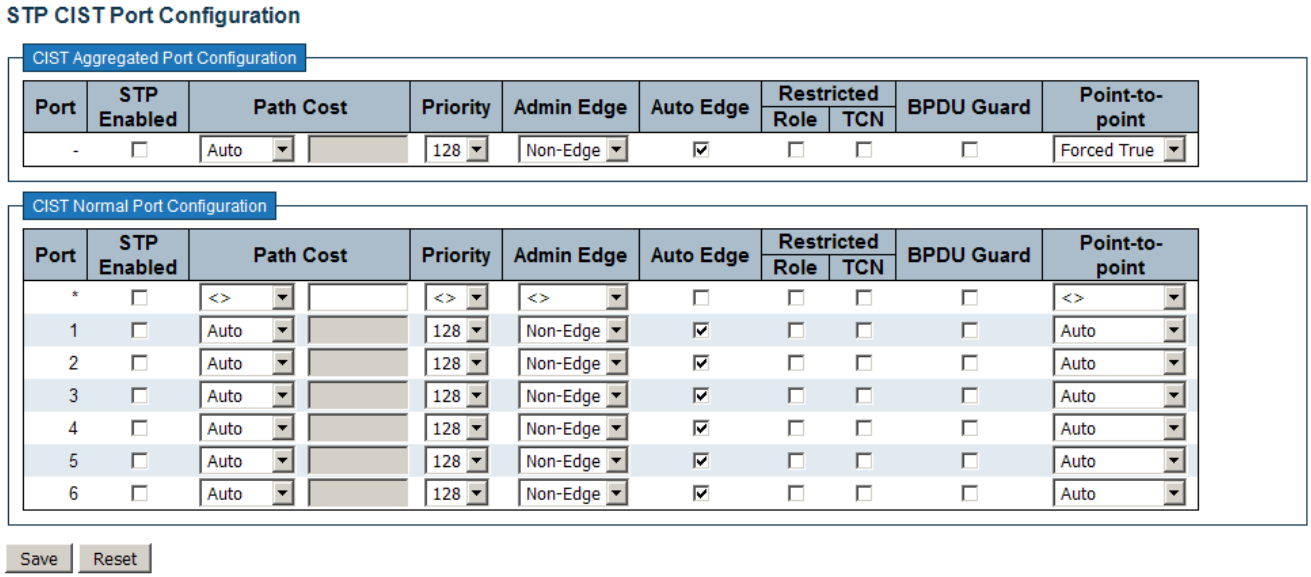
VLANs Mapped	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to *one* MSTI. An unused MSTI should just be left empty. (i.e. not having any VLANs mapped to it.)
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.8.3 MSTI Priorities



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

2.8.4 CIST Ports



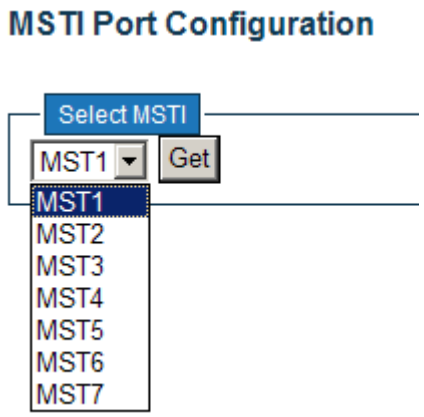
Configuration	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The *Auto* setting will set the path cost as appropriate by the physical link speed, using the 802.1D 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: *1 to 200000000*
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
AdminEdge	Controls whether the *operEdge* flag should start as being set or cleared. (The initial *operEdge* state when a port is initialized). ***operEdge**:* 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.
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.
BPDU Guard	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port *Edge* status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
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 the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Note: This configuration applies to physical and Link Aggregation ports.

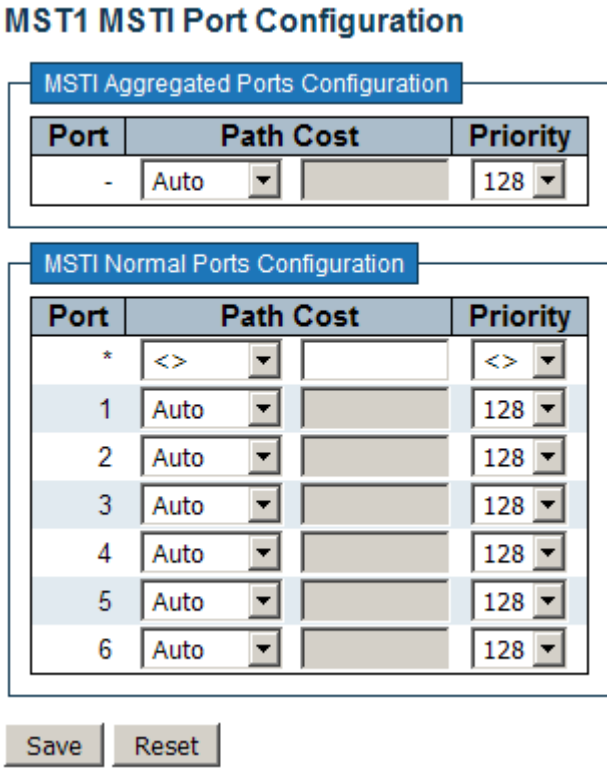
2.8.5 MSTI Ports

A MSTI port is a virtual port, which is instantiated separately 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.



Configuration	Description
MSTI	Select an MSTI for pop-up configuration.
Get	Click to pop-up configuration page.

Click Get :

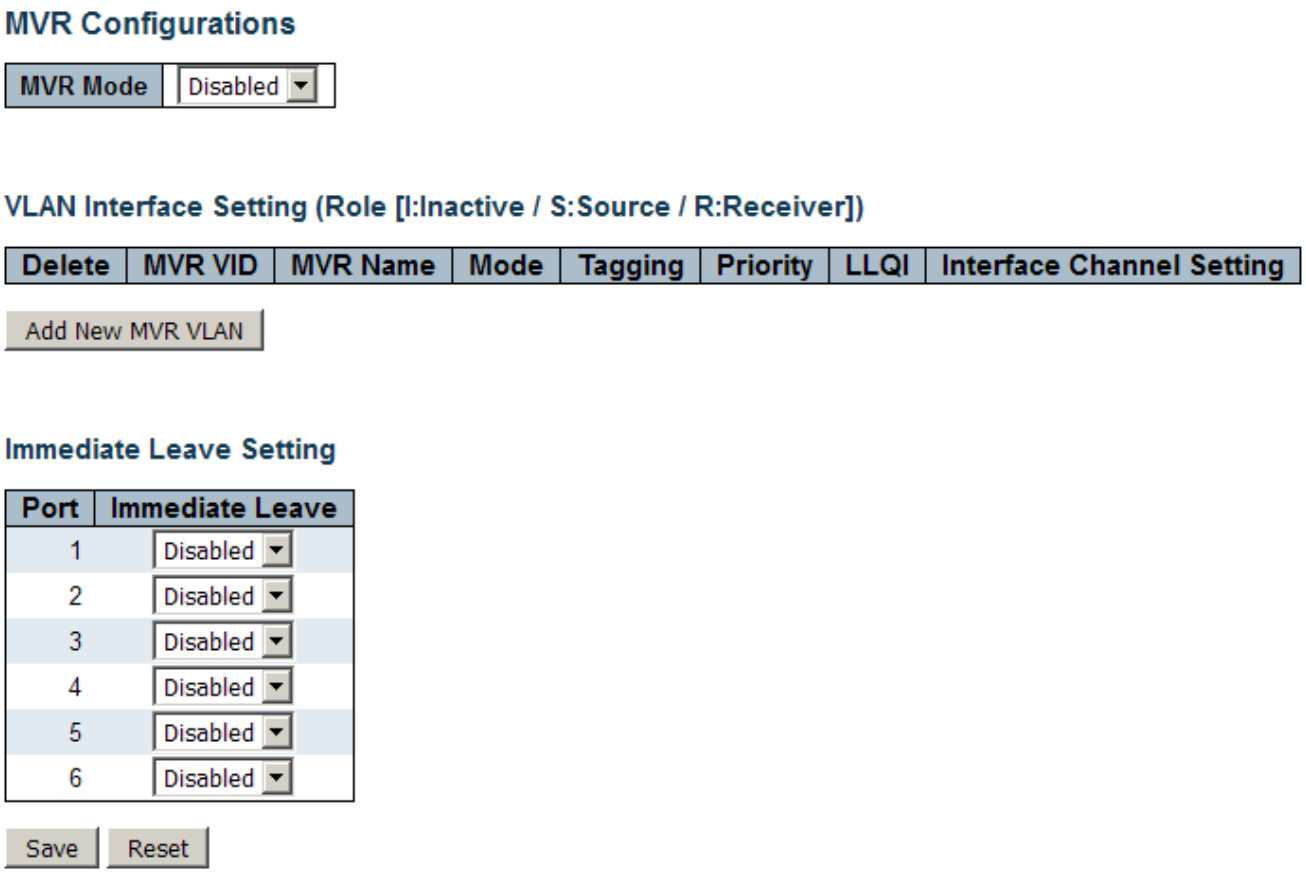


Configuration	Description (Example with MSTI1)
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The *Auto* setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using 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: *1 ~ 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 the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.9 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLANs. In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top

boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports. It is allowed to create at maximum 8 MVR VLANs with corresponding channel settings for each Multicast VLAN. There will be totally at maximum 256 group addresses for channel settings.

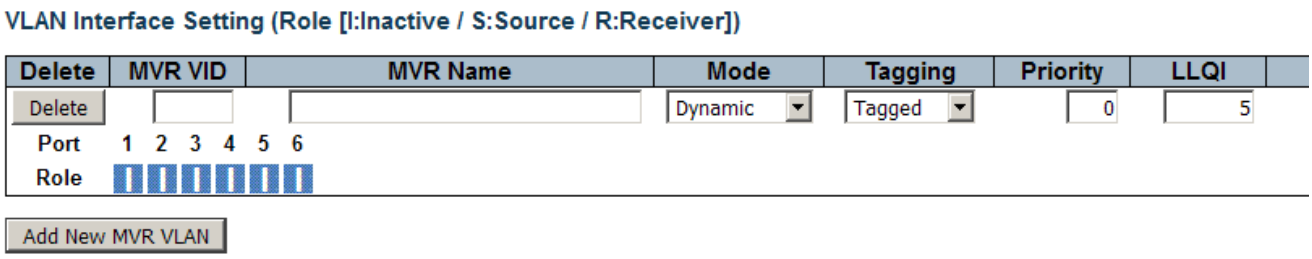


Configuration	Description (Example with MSTI1)
MVR Mode	Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
MVR VID	Specify the Multicast VLAN ID. *Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.*
MVR Name	MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can

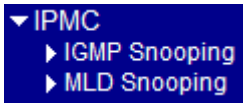
	only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.
Mode	Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.
Tagging	Specify whether the traversed IGMP/MLD control frames will be sent as *Untagged* or *Tagged* with MVR VID. The default is *Tagged*.
Priority	Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.
LLQI	Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.
Interface Channel Setting	
	When the MVR VLAN is created, click the Edit symbol to expand the corresponding multicast channel settings for the specific MVR VLAN. Summary about the Interface Channel Setting (of the MVR VLAN) will be shown besides the Edit symbol.
Port	The logical port for the settings
Port Role	Configure an MVR port of the designated MVR VLAN as one of the following roles. *Inactive*: The designated port does not participate MVR operations. *Source*: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. *Receiver*: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages. *Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.* Select the port role by clicking the Role symbol to switch the setting. *I:* indicates Inactive; *S:* indicates Source; R indicates Receiver The default Role is Inactive.
Immediate Leave	Enable the fast leave on the port.

Add New MVR VLAN	
	Click to add a new entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

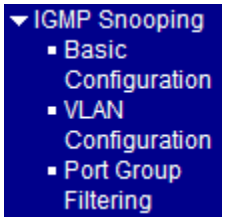
Click Add New MVR VLAN:



2.10 IPMC



2.10.1 IGMP Snooping



2.10.1.1 Basic Configuration

IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	☐
Unregistered IPMCv4 Flooding Enabled	☑
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	☐
Proxy Enabled	☐

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☐	☐	unlimited

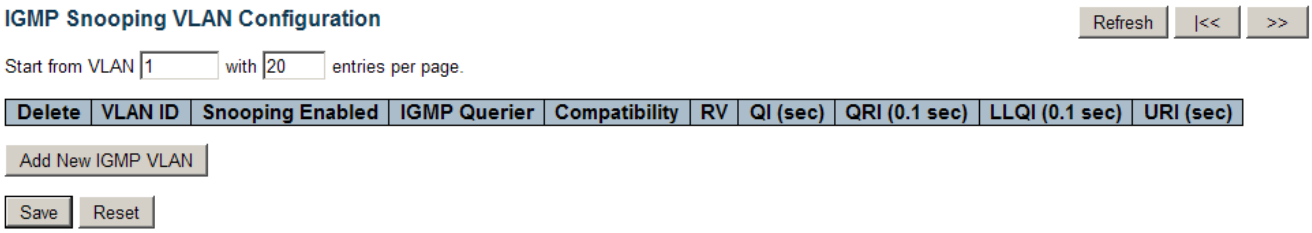
Save Reset

Configuration	Description (Example with MSTI1)
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMCv4 Flooding Enabled	Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always

	active in spite of this setting.
IGMP SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
Leave Proxy Enabled	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.10.1.2 VLAN Configuration

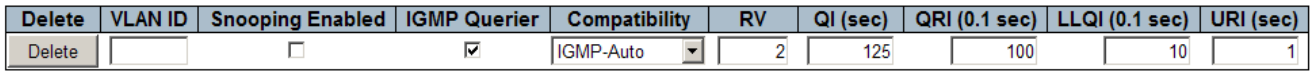
Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN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



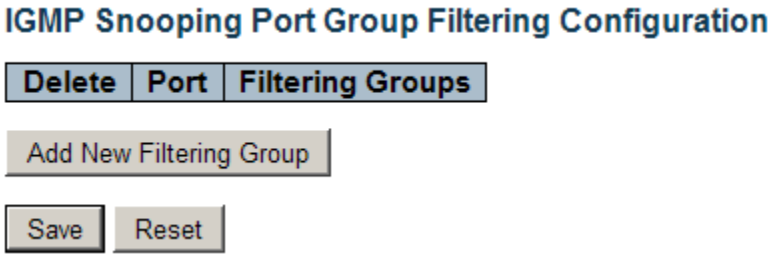
Configuration	Description (Example with MSTI1)
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
IGMP Querier	Enable the IGMP Querier in the VLAN.
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*.
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.
Refresh	Refreshes the displayed table starting from the "VLAN" input fields.
|<<	Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
>>	Updates the table, starting with the entry after the last entry currently displayed.
Add New IGMP VLAN	Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click Add New IGMP VLAN :

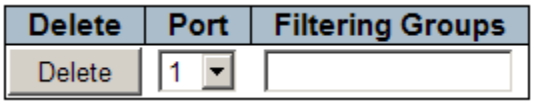


2.10.1.3 Port Group Filtering

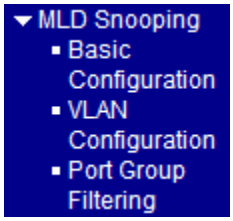


Configuration	Description (Example with MSTI1)
Delete	Check to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings.
Filtering Groups	The IP Multicast Group that will be filtered.
Add New Filtering Group	Click to add a new entry to the Group Filtering table. Specify the Port, and Filtering Group of the new entry. Click "Save".
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click Add New Filtering Group:



2.10.2 MLD Snooping



2.10.2.1 Basic Configuration

MLD Snooping Configuration

Global Configuration	
Snooping Enabled	☐
Unregistered IPMCv6 Flooding Enabled	☑
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	☐
Proxy Enabled	☐

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☐	☐	unlimited

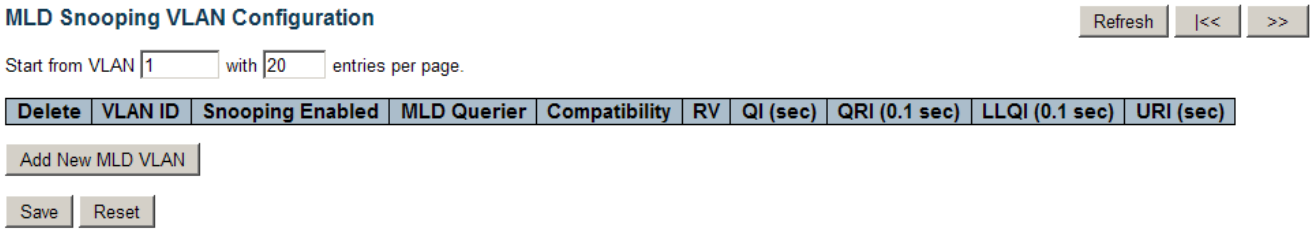
Save Reset

Configuration	Description (Example with MSTI1)
Snooping Enabled	Enable the Global MLD Snooping.
Unregistered IPMCv6 Flooding Enabled	Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.
MLD SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
Leave Proxy Enabled	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.

Throttling	Enable to limit the number of multicast groups to which a switch port can belong.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.10.2.2 VLAN Configuration

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



Configuration	Description (Example with MSTI1)
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
MLD Snooping Enabled	Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.
MLD Querier	Enable the MLD Querier in the VLAN.
Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is *MLD-Auto*, *Forced MLDv1*, *Forced MLDv2*, default compatibility value is *MLD-Auto*.
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	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.

Refresh	Refreshes the displayed table starting from the "VLAN" input fields.
|<<	Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
>>	Updates the table, starting with the entry after the last entry currently displayed.
Add New MLD VLAN	Click to add new MLD VLAN. Specify the VID and configure the new entry. Click "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click Add New MLD VLAN:

Delete	VLAN ID	Snooping Enabled	MLD Querier	Compatibility	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Delete		☐	☑	MLD-Auto	2	125	100	10	1

2.10.2.3 Port Group Filtering

MLD Snooping Port Group Filtering Configuration

Delete	Port	Filtering Groups

Add New Filtering Group

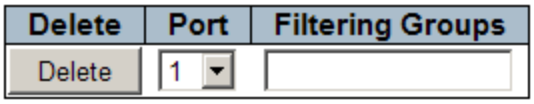
Save Reset

Configuration	**Description (Example with MSTI1)**
Delete	Check to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings.
Filtering Groups	The IP Multicast Group that will be filtered.

Add New Filtering Group	Click to add a new entry to the Group Filtering table. Specify the Port, and Filtering

	Group of the new entry. Click "Save".
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click Add New Filtering Group:



2.11 LLDP

2.11.1 LLDP

LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Port Configuration

			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☐	☐	☐	☐	☐
1	Disabled	☐	☑	☑	☑	☑	☑
2	Disabled	☐	☑	☑	☑	☑	☑
3	Disabled	☐	☑	☑	☑	☑	☑
4	Disabled	☐	☑	☑	☑	☑	☑
5	Disabled	☐	☑	☑	☑	☑	☑
6	Disabled	☐	☑	☑	☑	☑	☑

Save Reset

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

Tx Reinit	When a port 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: ***1 – 10 seconds***
Port Configuration	
Port	The switch port number of the logical LLDP port.
Mode	Select LLDP mode. ***Rx only:*** The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. ***Tx only:*** The switch will drop LLDP information received from neighbors, but will send out LLDP information. ***Disabled:*** The switch will not send out LLDP information, and will drop LLDP information received from neighbors. ***Enabled:*** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
CDP Aware	Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP for the port is enabled. Only CDP TLVs that can be mapped into a corresponding field in the LLDP neighbors table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frame are not shown in the LLDP statistic. Only). CDP TLVs are mapped into LLDP neighbors table as shown below. CDP TLV "Device ID" is mapped into the LLDP "Chassis ID" field. CDP TLV "Address" is mapped into the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table. CDP TLV "Port ID" is mapped into the LLDP "Port ID" field. CDP TLV "Version and Platform" is mapped into the LLDP "System Description" field. Both the CDP and LLDP supports "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors table. If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.

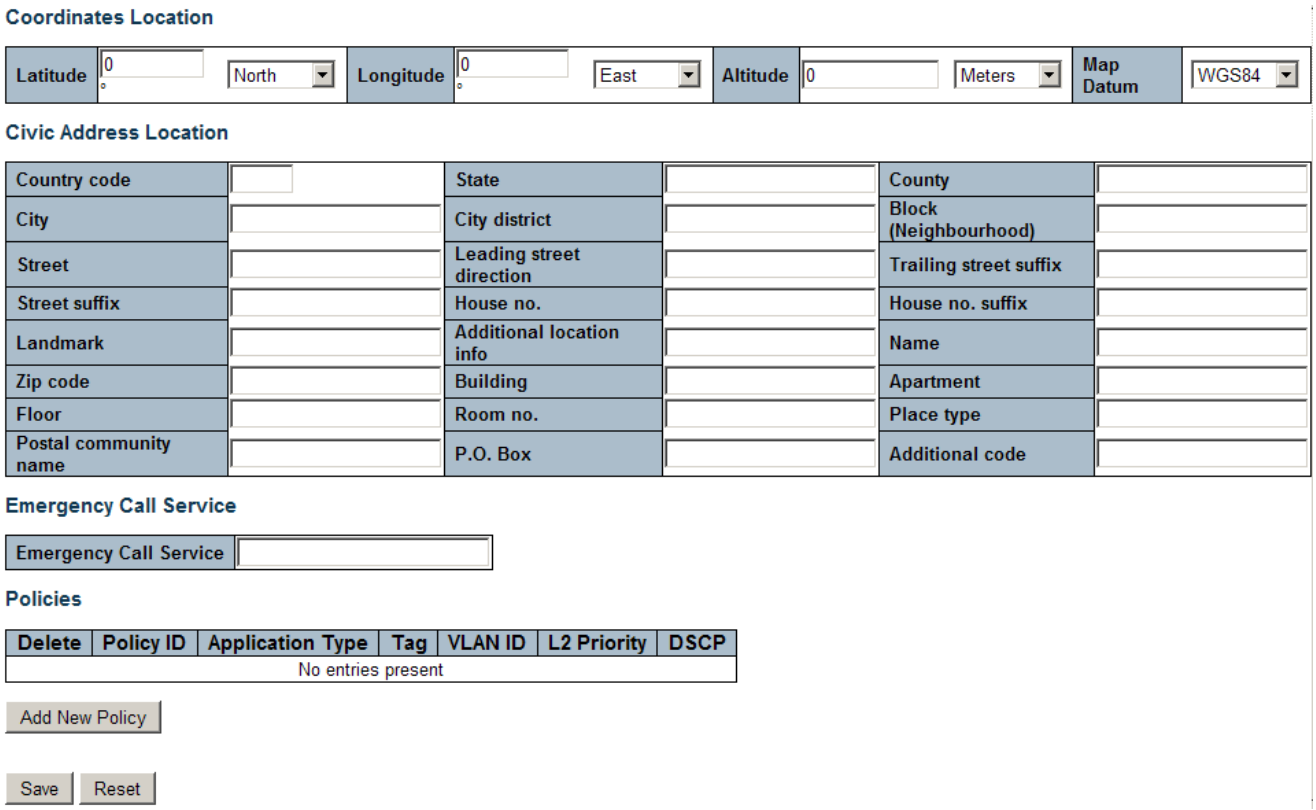
Note: When CDP awareness for a port is disabled the CDP information isn't removed immediately, but will be removed when the hold time is exceeded.

Optional TLV

Port Descr	When checked the "port description" is included in LLDP information transmitted.
Sys Name	When checked the "system name" is included in LLDP information transmitted.
Sys Descr	When checked the "system description" is included in LLDP information transmitted.
Sys Capa	When checked the "system capability" is included in LLDP information transmitted.
Mgmt Addr	When checked the "management address" is included in LLDP information transmitted.

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

2.11.2 LLDP-MED



Configuration	Description
Fast start repeat count	The number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a LLDP frame with new information is received.
Coordinates Location	

Latitude	Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either *North* of the equator or *South* of the equator.
Longitude	Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either *East* of the prime meridian or *West* of the prime meridian.
Altitude	Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). *Meters*: Representing meters of Altitude defined by the vertical datum specified. *Floors*: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
Map Datum	The Map Datum used for the coordinates given in this Option ***WGS84***: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich. ***NAD83/NAVD88***: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW). ***NAD83/MLLW***: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

Country code	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
State	National subdivisions (state, canton, region, province, prefecture).
County	County, parish, gun (Japan), district.
City	City, township, shi (Japan) - Example: Copenhagen
City district	City division, borough, city district, ward, chou (Japan)
Block (Neighborhood)	Neighborhood, block
Street	Street - Example: Poppelvej
Leading street direction	Leading street direction - Example: N
Trailing street suffix	Trailing street suffix - Example: SW

Street suffix	Street suffix - Example: Ave, Platz
House no.	House number - Example: 21
House no. suffix	House number suffix - Example: A, 1/2
Landmark	Landmark or vanity address - Example: Columbia University
Additional location info	Additional location info - Example: South Wing
Name	Name (residence and office occupant) - Example: Flemming Jahn
Zip code	Postal/zip code - Example: 2791
Building	Building (structure) - Example: Low Library
Apartment	Unit (Apartment, suite) - Example: Apt 42
Floor	Floor - Example: 4
Room no.	Room number - Example: 450F
Place type	Place type - Example: Office
Postal community name	Postal community name - Example: Leonia
P.O. Box	Post office box (P.O. BOX) - Example: 12345
Additional code	Additional code - Example: 1320300003

Emergency Call Service

Emergency Call Service	Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.
Add New Policy	Click to configure a new policy.

Policies

Delete	Policy Id	Application Type	Tag	VLAN ID	L2 Priority	DSCP
Delete	0	Voice	Tagged	1	0	0

Delete	Check to delete the policy. It will be deleted during the next save.
Policy ID	ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.
Application Type	Intended use of the application types: 1. ***Voice*** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. 2. ***Voice Signaling*** (conditional) - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type

	should not be advertised if all the same network policies apply as those advertised in the ***Voice*** application policy. 3. ***Guest Voice*** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. 4. ***Guest Voice Signaling*** (conditional) - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the **Guest Voice** application policy. 5. ***Softphone Voice*** - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance. 6. ***Video Conferencing*** 7. ***Streaming Video*** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. 8. ***Video Signaling*** (conditional) - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the ***Video Conferencing*** application policy.
Tag	Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. ***Untagged*** indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. ***Tagged*** indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.
VLAN ID	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003
L2 Priority	**L2 Priority** is the Layer 2 priority to be used for the specified application type. **L2**

	Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
DSCP	**DSCP** value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. **DSCP** may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Port Policies Configuration	
Port	The port number for which the configuration applies.
Policy Id	The set of policies that shall apply for a given port The set of policies is selected by checkmarking the checkboxes that corresponds to the policies

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

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service. **Policies** are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice

2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

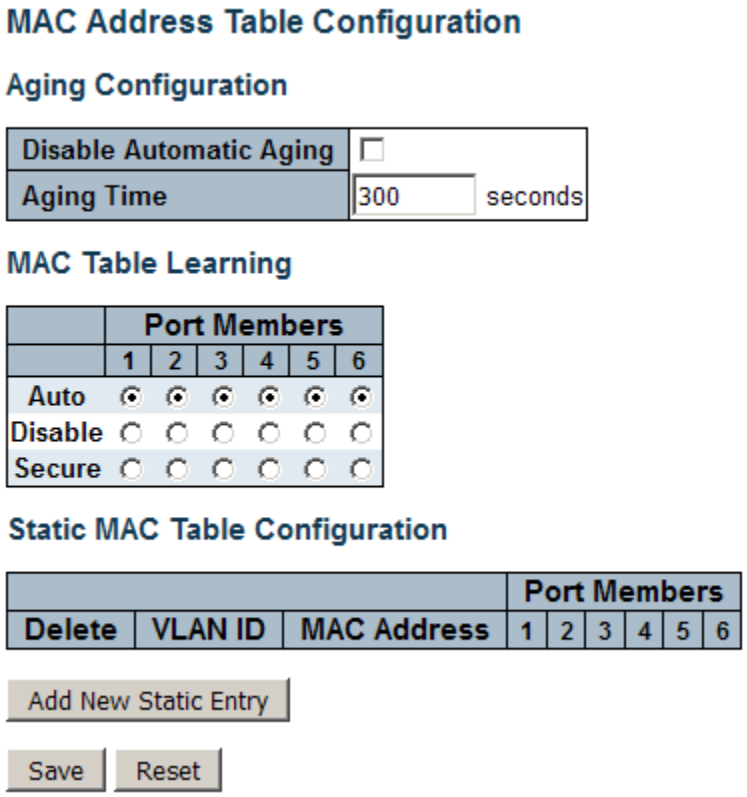
A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Port Policies Configuration

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

2.12 MAC Table



Aging Configuration	**Description**
Disable Automatic Aging	Check to disable aging for MAC address entries. By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging.
Aging Time	Configure aging time by entering a value here in seconds Valid values: ***10 to 1000000 seconds***
Port MAC Table Learning	
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. ***Note:*** *Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.*
Add New Static Entry	Click to configure a new static MAC address entry in the MAC table.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click Add New Static Entry :

Static MAC Table Configuration

			Port Members					
Delete	VLAN ID	MAC Address	1	2	3	4	5	6
Delete	1	00-00-00-00-00-00	☐	☐	☐	☐	☐	☐

2.13 VLANs

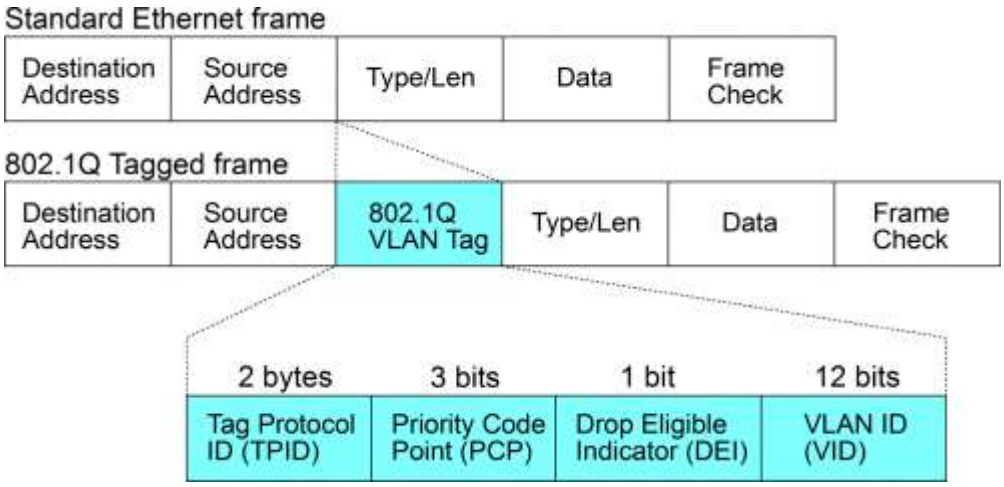
- VLANs
  - VLAN Membership
  - Ports

2.13.1 Abbreviation

Ingress Port: Ingress port is the input port on which a packet is received.

Egress Port: Egress port is the output port from which a packet is sent out.

IEEE 802.1Q Packets: A packet which is embedded with a VLAN Tag field



IEEE 802.1Q VLAN Tag: In IEEE 802.1Q packet format, 4-byte tag field is inserted in the original Ethernet frame between the Source Address and Type/Length fields. Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI). The TCI field is further divided into PCP, DEI, and VID.

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID

TPID Tag protocol identifier: a 16-bit field set to a value of 0x8100 (standard) in order to identify the frame

as an IEEE 802.1Q-tagged frame. This field is located at the same position as the EtherType/length field in untagged frames, and is thus used to distinguish the frame from untagged frames.

Tag control information (TCI): divided into PCP, DEI, and VID

Priority code point (PCP): a 3-bit field which refers to the IEEE 802.1p class of service and maps to the frame priority level.

Drop eligible indicator (DEI): a 1-bit field. (formerly CFI). It may be used separately or in conjunction with PCP to indicate frames eligible to be dropped in the presence of congestion.

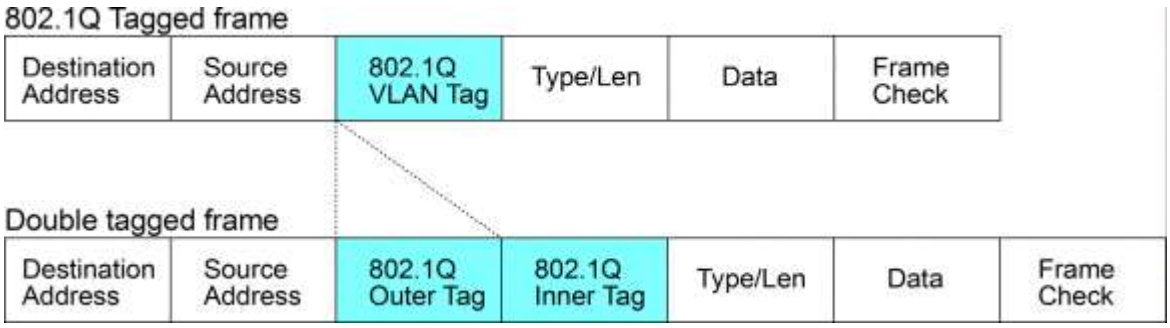
VLAN identifier (VID): a 12-bit field specifying the VLAN to which the frame belongs.

Untagged frame: A standard Ethernet frame with no VLAN Tag field

Priority-tagged frame: An IEEE 802.1Q frame which VID field value is zero (VID=0)

VLAN-Tagged frame: An IEEE 802.1Q frame which VID field value is not zero (VID>0)

Double tagging, Double Tags: With the IEEE standard 802.1ad, double-tagging can be useful for Internet service providers, allowing them to use VLANs internally while mixing traffic from clients that are already VLAN-tagged. The outer (next to source MAC and representing ISP VLAN) S-TAG (service tag) comes first, followed by the inner C-TAG (customer tag). In such cases, 802.1ad specifies a TPID of 0x88a8 for service-provider outer S-TAG.



C-tag: Tag with TPID 0x8100

S-tag: Tag with TPID 0x88A8

Priority S-tagged frame: Priority tagged frame with S-tag (TPID=0x88A8, VID=0)

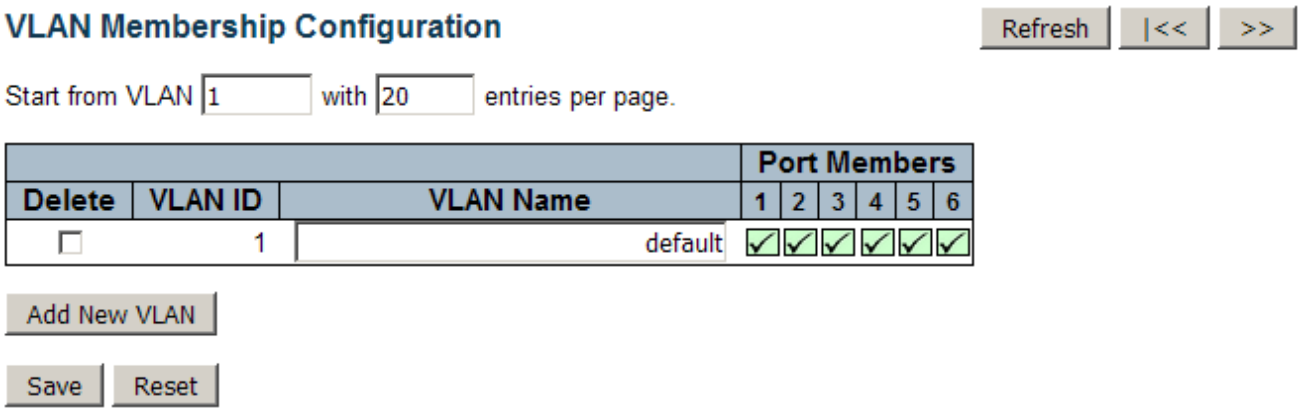
Priority C-tagged frame: Priority tagged frame with C-tag (TPID=0x8100, VID=0)

VLAN S-tagged frame: Tagged frame with S-tag (TPID=0x88A8, VID>0)

VLAN C-tagged frame: Tagged frame with C-tag (TPID=0x8100, VID>0)

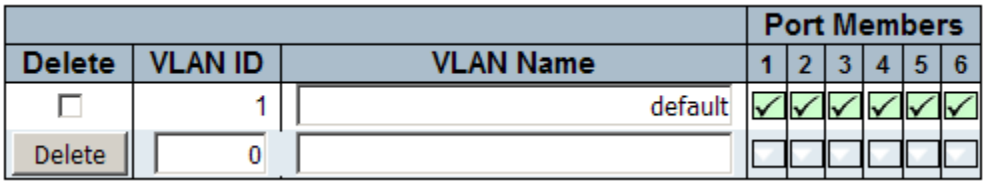
PVID (Port VID): PVID is the default VID of an ingress port. It is used in 802.1Q filtering for untagged packets. It is also often used as [Default Tag - VID] for egress tagging operation.

2.13.2 VLAN Membership

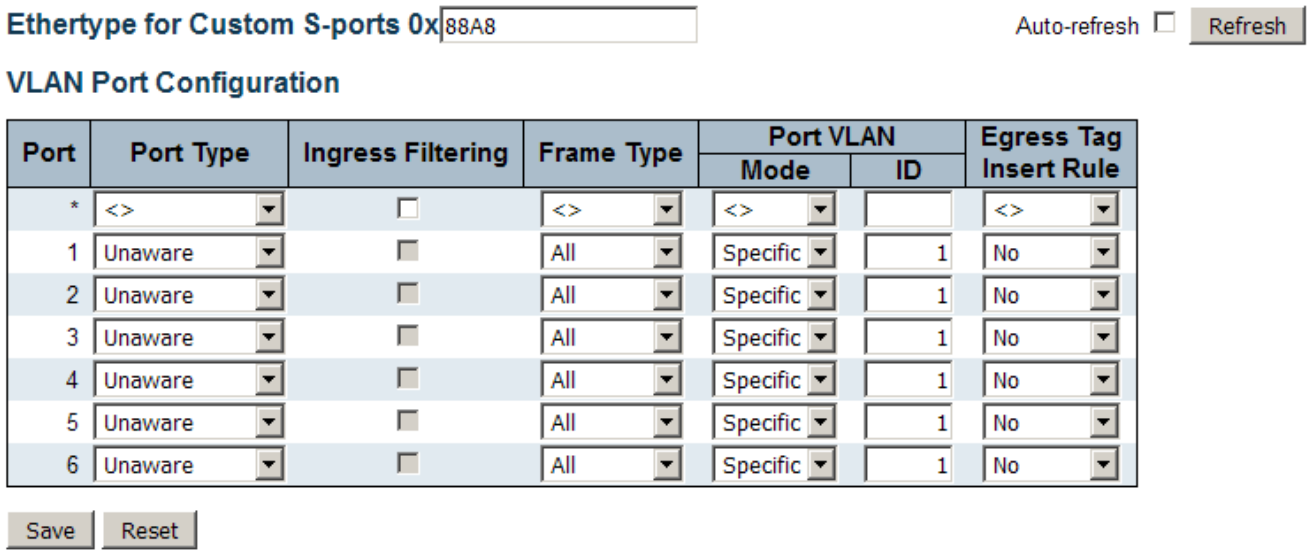


Configuration	Description
Start from VLAN …..	Select range of VLAN table entries.
Delete	Check to delete a VLAN entry. The entry will be deleted on the switch unit during the next Save.
VLAN ID	Indicates the ID of this particular VLAN.
VLAN Name	Indicates the name of the VLAN. Maximum length of the VLAN Name String is 32. VLAN Name can be null. If it is not null, it must contain alphabets or numbers. At least one alphabet must be present in a non-null VLAN name. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Add New VLAN	Click to add a new VLAN entry. An empty row is added to the table, and the VLAN can be configured as needed.
Refresh	Click to refresh the page; any changes made locally will be undone.
|<<	Click to display the first page.
>>	Click to display the last page.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click Add New VLAN :



2.13.3 Ports



Configuration	Description
Ethertype for Custom S-ports 0x	This field specifies the ether type used for S-custom-ports. This is a global setting for all the S-custom-ports.
Port	This is the logical port number of this row.
Port Type	Port can be one of the following types: *Unaware*, *Customer port(C-port)*, *Service port(S-port)*, *Custom Service port(S-custom-port)* Each frame received on an ingress port will be classified to a VLAN before it is forwarding to other ports. The classified VLAN is abbreviated as **Classified VID**. The VLAN classification rules for each of the port types are: *Unaware* **Received frame type** / **Classified VID** Untagged / PVID (Ingress Port VLAN ID) Priority tagged (VID = 0) / PVID (Ingress Port VLAN ID) All tagged (VID > 0) / PVID (Ingress Port VLAN ID) *C-port, S-port, C-custom-port*

Received frame type	Classified VID
Untagged	PVID (Ingress Port VLAN ID)
Priority tagged (VID = 0)	PVID (Ingress Port VLAN ID)
All tagged (VID > 0)	The frame's embedded VID

The tag removal rules for different port types are:

Unaware	No frame tag is removed.
C-port *S-port* *S-custom-port*	The tag is removed for 1-tag frames. The outer tag is removed for double-tagged frames.

Ingress Filtering — Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).

Frame Type — Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to *All*. The rules of the accepted frames for different port types are:

Unaware port

Untag	Untagged & Priority C-tag & S-tag frames
Tag	C-tag & S-tag tagged frames
All	All above frames

C-port

Untag	Untagged & Priority C-tag frames
Tag	C-tag tagged frames
All	All above frames

S-port

Untag	Untagged & Priority S-tag frames
Tag	S-tag tagged frames
All	All above frames

S-custom-port

Untag	Untagged & Priority S-custom-tag frames
Tag	S-custom-tag tagged frames
All	All above frames

Port VLAN Mode	The allowed values are ***None*** or ***Specific***. This parameter affects VLAN ingress and egress processing. ***None*** - a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches. Tx tag should be set to *Untag_pvid* when this mode is used. ***Specific*** (the default value) - a Port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.
Port VLAN ID (PVID)	Configures the VLAN identifier for the port. The setting is abbreviated as PVID. The allowed values are from 1 through 4095. The default value is 1. *Note: The port must be a member of the same VLAN as the Port VLAN ID.*
Tx Tag	Determines egress tagging of a port. ***Untag_pvid*** - All frames except the configured PVID will be tagged. The frames that the associated classified VID match egress port's PVID are NOT inserted with any tag. All other frames are with the associated classified tag in egress. ***Tag_all*** - All frames are tagged. All frames are inserted with the associated classified tag in egress. ***Untag_all*** - All frames are untagged. All frames are NOT inserted with the associated classified tag in egress.

Note:

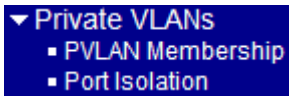
1. *The value of TPID (Ethertype) for the inserted tag determined by the egress port type as follows:*

Unaware	C-tag (0x8100)
C-port	C-tag (0x8100)
S-port	S-tag (0x88A8)
S-custom-port	The setting of Ethertype for Customer S-port

2. *The inserted tag is inserted at the outer tag position in a frame.*

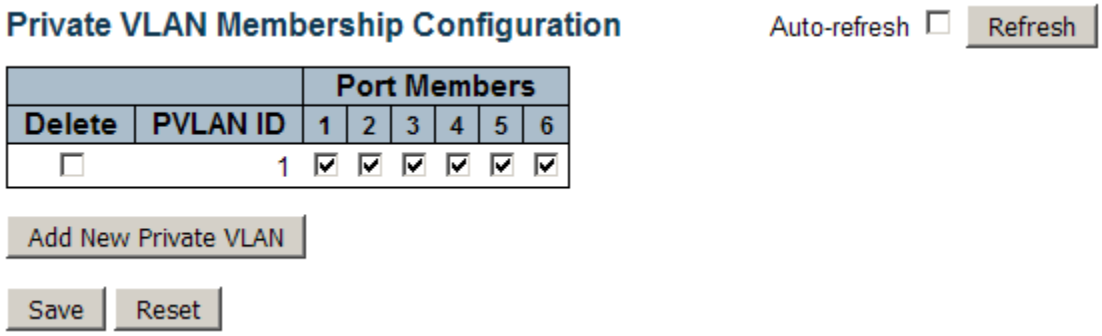
Refresh	Click to refresh the page; any changes made locally will be undone.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.14 Private VLANs



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.

2.14.1 PVLAN Membership



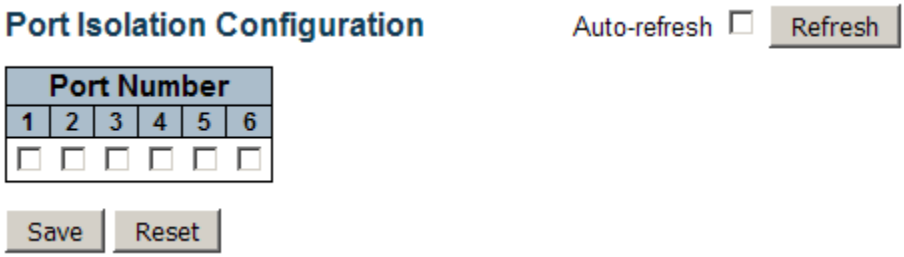
Configuration	Description
Delete	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Add New Private VLAN	Click to add a new VLAN entry. An empty row is added to the table, and the VLAN can be configured as needed.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click 

:

		Port Members					
Delete	PVLAN ID	1	2	3	4	5	6
☐	1	☑	☑	☑	☑	☑	☑
Delete	0	☐	☐	☐	☐	☐	☐

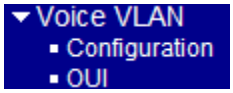
2.14.2 Port Isolation



A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

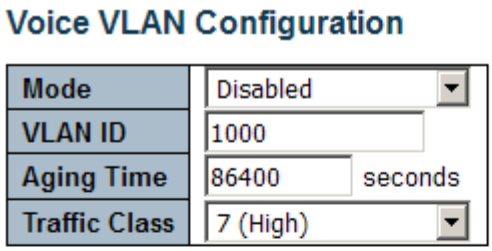
Configuration	Description
Port Members	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

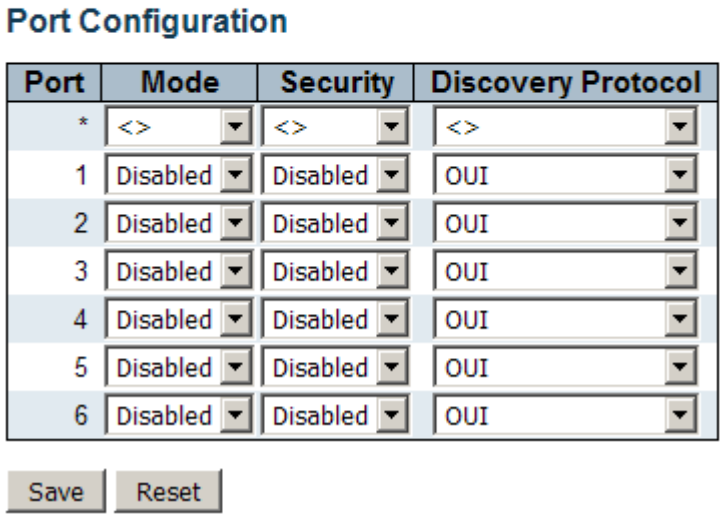
2.15 Voice VLAN



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

2.15.1 Configuration





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

Aging Time	Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.
Traffic Class	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.
Port Mode	Indicates the Voice VLAN port mode. When the port mode isn't equal disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible port modes are: *Disabled*: Disjoin from Voice VLAN. *Auto*: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically. *Forced*: Force join to Voice VLAN.
Port Security	Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are: *Enabled*: Enable Voice VLAN security mode operation. *Disabled*: Disable Voice VLAN security mode operation.
Port Discovery Protocol	Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "*LLDP*" or "*Both*". Changing the discovery protocol to "*OUI*" or "*LLDP*" will restart auto detect process. Possible discovery protocols are: *OUI*: Detect telephony device by OUI address. *LLDP*: Detect telephony device by LLDP. *Both*: Both OUI and LLDP.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.15.2 OUI

Voice VLAN OUI Table

Delete	Telephony OUI	Description
☐	00-01-e3	Siemens AG phones
☐	00-03-6b	Cisco phones
☐	00-0f-e2	H3C phones
☐	00-60-b9	Philips and NEC AG phones
☐	00-d0-1e	Pingtel phones
☐	00-e0-75	Polycom phones
☐	00-e0-bb	3Com phones

Add New Entry

Save Reset

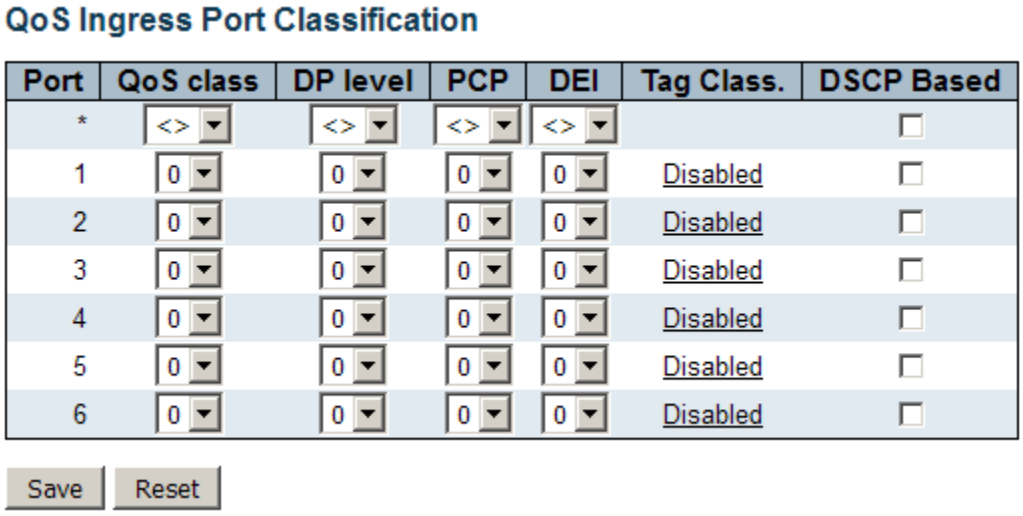
Configuration	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Telephony OUI	Telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
Description	The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.
Add New Entry	Click to add a new entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click Add New Entry :

Delete	Telephony OUI	Description
☐	00-01-e3	Siemens AG phones
☐	00-03-6b	Cisco phones
☐	00-0f-e2	H3C phones
☐	00-60-b9	Philips and NEC AG phones
☐	00-d0-1e	Pingtel phones
☐	00-e0-75	Polycom phones
☐	00-e0-bb	3Com phones
Delete		

2.16 QoS

2.16.1 Port Classification

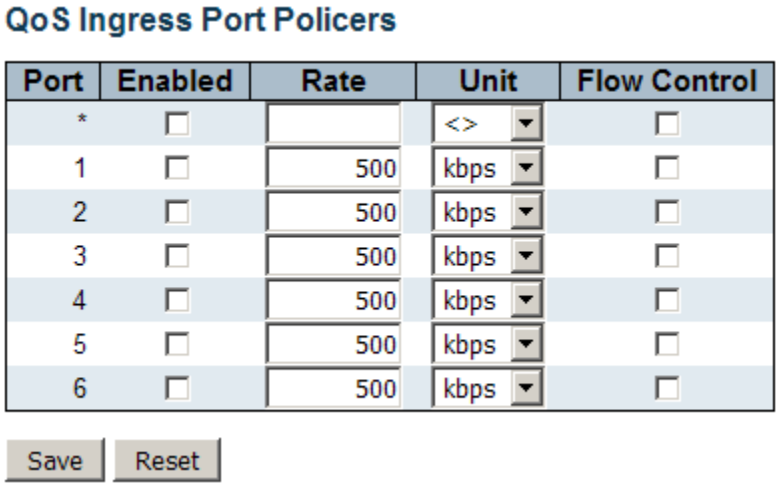


Configuration	Description
Port	The port number for which the configuration below applies.
QoS class	Controls the default QoS class. All frames are classified to a QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority. If the port 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 in order to configure the mode and/or mapping. *Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default QoS class and DP level.*
DSCP Based	Click to Enable DSCP Based QoS Ingress Port Classification.

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

2.16.2 Port Policing



Configuration	Description
Port	The port number for which the configuration below applies.
Enabled	Controls whether the policer is enabled on this switch port.
Rate	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps".
Unit	Controls the unit of measure for the policer rate as *kbps*, *Mbps*, *fps* or *kfps* . The default value is "*kbps*".
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.16.3 Scheduler

QoS Egress Port Schedulers

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

Configuration	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.
Mode	Shows the scheduling mode for this port.
Qn	Shows the weight for this queue and port.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

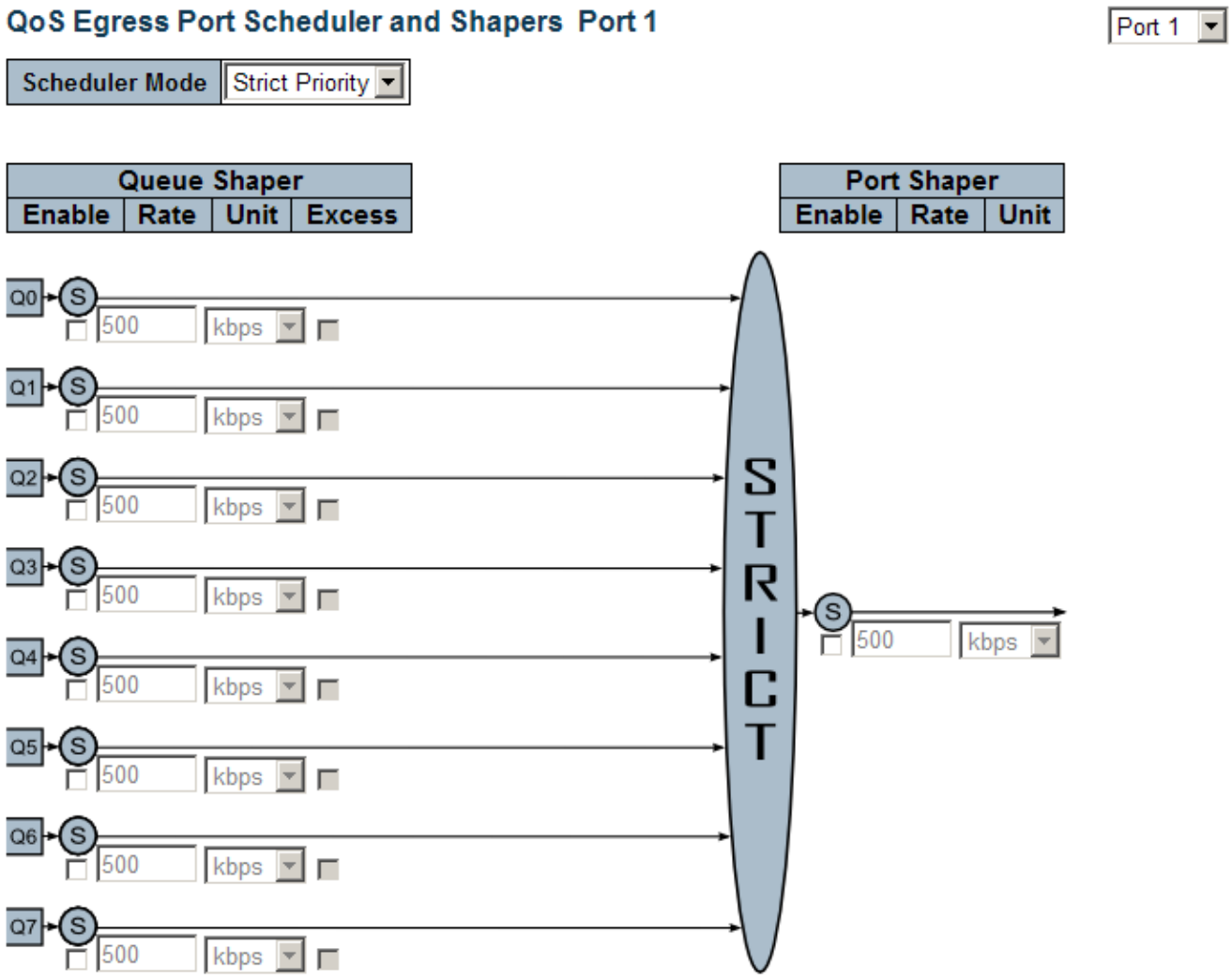
2.16.4 Shaping

QoS Egress Port Shapers

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

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

Click Port 1 icon as an example:

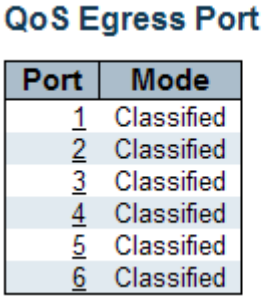


Configuration	Description
Scheduler Mode	Controls whether the scheduler mode is "*Strict Priority*" or "*Weighted*" on this switch port.
Queue Shaper Enable	Controls whether the queue shaper is enabled for this queue on this switch port.
Queue Shaper Rate	Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Queue Shaper Unit	Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".
Queue Shaper Excess	Controls whether the queue is allowed to use excess bandwidth.
Queue Scheduler Weight	Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent	
	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
Port Shaper Enable	Controls whether the port shaper is enabled for this switch port.
Port Shaper Rate	Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Port Shaper Unit	Controls the unit of measure for the port shaper rate as "*kbps*" or "*Mbps*". The default value is "*kbps*".

Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Cancel	Click to undo any changes made locally and revert to previously page.

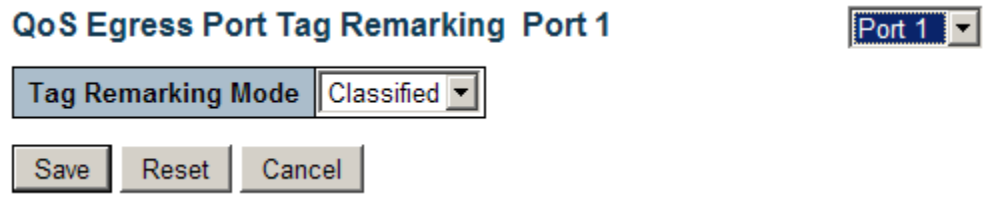
2.16.5 Tag Remarking



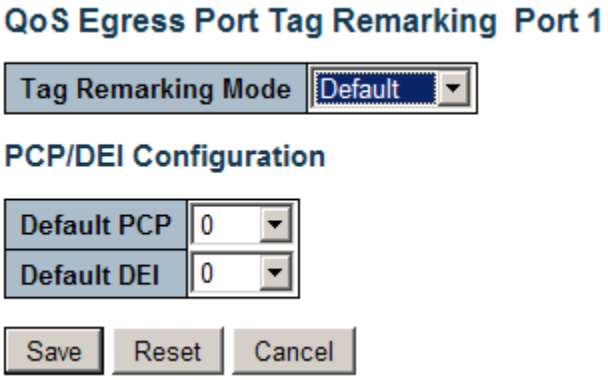
Configuration	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.
Mode	Shows the tag remarking mode for this port. ***Classified***: Use classified PCP/DEI values. ***Default***: Use default PCP/DEI values. ***Mapped***: Use mapped versions of QoS class and DP level.

Click Port 1 icon as an example:

Mode = *Classified*



Mode = *Default*



Mode = *Mapped*

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode	Mapped

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

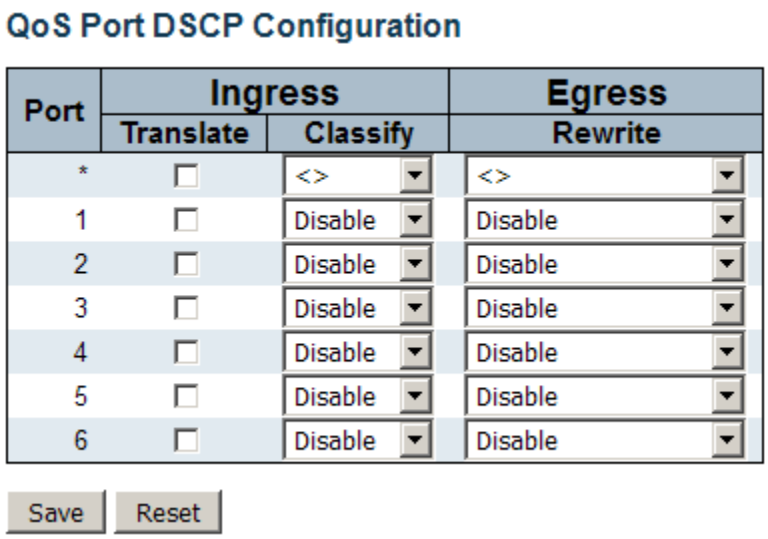
QoS class	DP level	PCP	DEI
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

Save Reset Cancel

Configuration	Description
Mode	Controls the tag remarking mode for this port. Classified: Use classified PCP/DEI values. Default: Use default PCP/DEI values. Mapped: Use mapped versions of QoS class and DP level.
PCP/DEI Configuration	Controls the default PCP and DEI values used when the mode is set to Default.
DP level Configuration	Controls the Drop Precedence level translation table when the mode is set to Mapped. The purpose of this table is to reduce the 2 bit classified DP level to a 1 bit DP level used in the (QoS class, DP level) to (PCP, DEI) mapping process.
(QoS class, DP level) to (PCP, DEI) Mapping	Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.

Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Cancel	Click to undo any changes made locally and revert to previously page.

2.16.6 Port DSCP



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

	remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

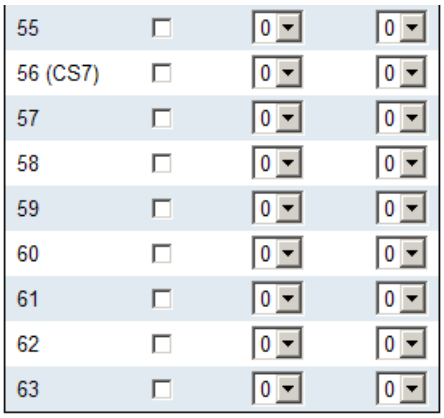
2.16.7 DSCP-Based QoS

DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	☐	<>	<>
0 (BE)	☐	0	0
1	☐	0	0
2	☐	0	0
3	☐	0	0
4	☐	0	0
5	☐	0	0
6	☐	0	0
7	☐	0	0
8 (CS1)	☐	0	0
9	☐	0	0
10 (AF11)	☐	0	0
11	☐	0	0
12 (AF12)	☐	0	0
13	☐	0	0
14 (AF13)	☐	0	0
15	☐	0	0
16 (CS2)	☐	0	0
17	☐	0	0

18 (AF21)	☐	0	0
19	☐	0	0
20 (AF22)	☐	0	0
21	☐	0	0
22 (AF23)	☐	0	0
23	☐	0	0
24 (CS3)	☐	0	0
25	☐	0	0
26 (AF31)	☐	0	0
27	☐	0	0
28 (AF32)	☐	0	0
29	☐	0	0
30 (AF33)	☐	0	0
31	☐	0	0
32 (CS4)	☐	0	0
33	☐	0	0
34 (AF41)	☐	0	0
35	☐	0	0

36 (AF42)	☐	0	0
37	☐	0	0
38 (AF43)	☐	0	0
39	☐	0	0
40 (CS5)	☐	0	0
41	☐	0	0
42	☐	0	0
43	☐	0	0
44	☐	0	0
45	☐	0	0
46 (EF)	☐	0	0
47	☐	0	0
48 (CS6)	☐	0	0
49	☐	0	0
50	☐	0	0
51	☐	0	0
52	☐	0	0
53	☐	0	0
54	☐	0	0



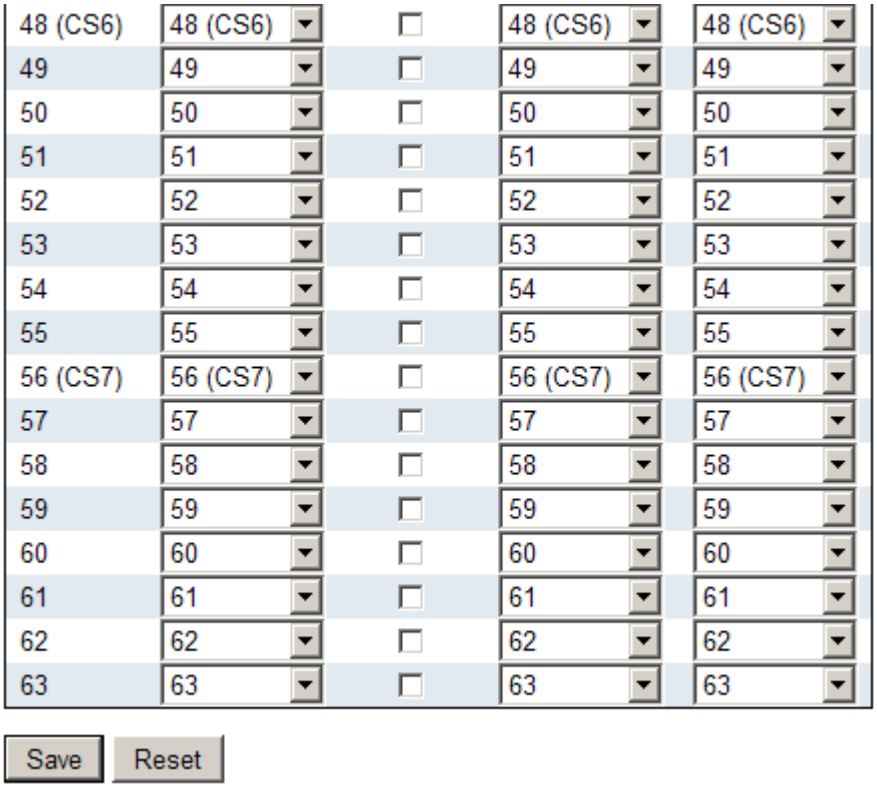
Configuration	Description
DSCP	Maximum number of supported DSCP values are 64.
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS Class	QoS class value can be any of (0-7)
DPL	Drop Precedence Level (0-1)
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.16.8 DSCP Translation

DSCP Translation

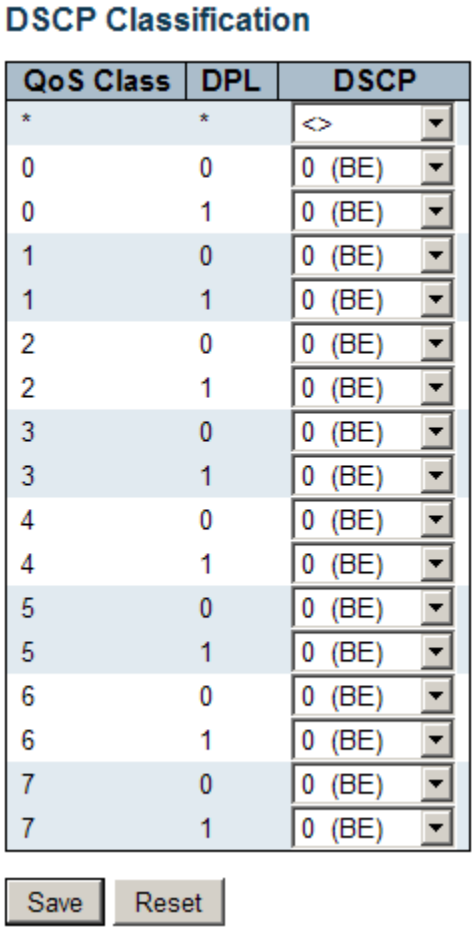
DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	☐	<>	<>
0 (BE)	0 (BE)	☐	0 (BE)	0 (BE)
1	1	☐	1	1
2	2	☐	2	2
3	3	☐	3	3
4	4	☐	4	4
5	5	☐	5	5
6	6	☐	6	6
7	7	☐	7	7
8 (CS1)	8 (CS1)	☐	8 (CS1)	8 (CS1)
9	9	☐	9	9
10 (AF11)	10 (AF11)	☐	10 (AF11)	10 (AF11)
11	11	☐	11	11
12 (AF12)	12 (AF12)	☐	12 (AF12)	12 (AF12)
13	13	☐	13	13
14 (AF13)	14 (AF13)	☐	14 (AF13)	14 (AF13)
15	15	☐	15	15
16 (CS2)	16 (CS2)	☐	16 (CS2)	16 (CS2)
17	17	☐	17	17
18 (AF21)	18 (AF21)	☐	18 (AF21)	18 (AF21)
19	19	☐	19	19
20 (AF22)	20 (AF22)	☐	20 (AF22)	20 (AF22)
21	21	☐	21	21

22 (AF23)	22 (AF23)	☐	22 (AF23)	22 (AF23)
23	23	☐	23	23
24 (CS3)	24 (CS3)	☐	24 (CS3)	24 (CS3)
25	25	☐	25	25
26 (AF31)	26 (AF31)	☐	26 (AF31)	26 (AF31)
27	27	☐	27	27
28 (AF32)	28 (AF32)	☐	28 (AF32)	28 (AF32)
29	29	☐	29	29
30 (AF33)	30 (AF33)	☐	30 (AF33)	30 (AF33)
31	31	☐	31	31
32 (CS4)	32 (CS4)	☐	32 (CS4)	32 (CS4)
33	33	☐	33	33
34 (AF41)	34 (AF41)	☐	34 (AF41)	34 (AF41)
35	35	☐	35	35
36 (AF42)	36 (AF42)	☐	36 (AF42)	36 (AF42)
37	37	☐	37	37
38 (AF43)	38 (AF43)	☐	38 (AF43)	38 (AF43)
39	39	☐	39	39
40 (CS5)	40 (CS5)	☐	40 (CS5)	40 (CS5)
41	41	☐	41	41
42	42	☐	42	42
43	43	☐	43	43
44	44	☐	44	44
45	45	☐	45	45
46 (EF)	46 (EF)	☐	46 (EF)	46 (EF)
47	47	☐	47	47



Configuration	Description
DSCP	Maximal number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
Ingress	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation – Translate & Classify.
Translate	DSCP at Ingress side can be translated to any of (0-63) DSCP values.
Classify	Click to enable Classification at Ingress side.
Egress	There are the following configurable parameters for Egress side - 1. Remap DP0 Controls the remapping for frames with DP level 0. 2. Remap DP1 Controls the remapping for frames with DP level 1.
Remap DP0	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
Remap DP1	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.16.9 DSCP Classification



Configuration	Description
QoS Class	Actual QoS class.
DPL	Actual Drop Precedence Level
DSCP	Select the classified DSCP value (0-63).
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.16.10 QoS Control List

QoS Control List Configuration

QCE#	Port	Frame Type	SMAC	DMAC	VID	PCP	DEI	Action			
								Class	DPL	DSCP	
											⊕

Click ⊕ :

QCE Configuration

Port Members					
1	2	3	4	5	6
☑	☑	☑	☑	☑	☑

Key Parameters

Tag	Any
VID	Any
PCP	Any
DEI	Any
SMAC	Any
DMAC Type	Any
Frame Type	Any

Action Parameters

Class	0
DPL	Default
DSCP	Default

Save Reset Cancel

Configuration	Description
Port Members	Check the checkbox button to include the port in the QCL entry. By default all ports are included.
Key Parameters	Key configuration is described as below:
Tag	Value of Tag field can be *'Any'*, *'Untag'* or *'Tag'*.
VID	Valid value of VLAN ID can be any value in the range 1-4095 or *'Any'*; user can enter either a specific value or a range of VIDs.
PCP	Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or '*Any*'.
DEI	Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or '*Any*'.
SMAC	Source MAC address: 24 MS bits (OUI) or '*Any*'.
DMAC Type	Destination MAC type: possible values are unicast(*UC*), multicast(*MC*), broadcast(*BC*) or '*Any*'.
Frame Type	Frame Type can have any of the following values:

Any, Ethernet, LLC, SNAP, IPv4, IPv6

Note: All frame types are explained below.

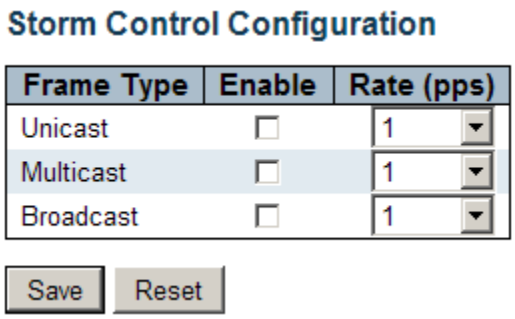
1. *Any: Allow all types of frames.*
2. *Ethernet: Ethernet Type Valid ethernet type can have a value within 0x600-0xFFFF or 'Any' but excluding 0x800(IPv4) and 0x86DD(IPv6), default value is 'Any'.*
3. *LLC: SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'.*
   DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'.
   Control Valid Control field can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'.
4. *SNAP: PID Valid PID(a.k.a ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'.*
5. *IPv4: Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'.*
   Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.
   DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
   IP Fragment IPv4 frame fragmented option: yes|no|any.
   Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
   Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
6. *IPv6: Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'.*
   Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits.
   DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
   Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
   Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Parameters

Class	QoS class: (0-7) or *'Default'*.
DPL	Valid Drop Precedence Level can be (0-1) or *'Default'*.
DSCP	Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or *'Default'*. *'Default'* means that the default classified value is not modified by this QCE.

Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Cancel	Click to undo any changes made locally and revert to previously page.

2.16.11 Storm Control

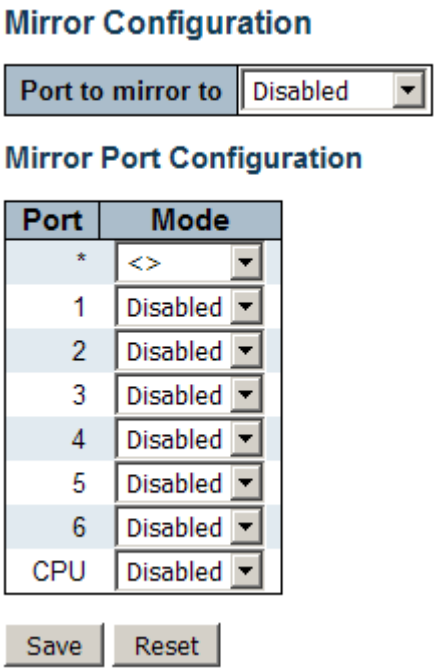


There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

Configuration	**Description**
Frame Type	The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.
Enable	Enable or disable the storm control status for the given frame type.
Rate	The rate unit is packets per second (pps). Valid values are: *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.

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

2.17 Mirroring



To debug network problems, selected traffic can be copied, or mirrored, on a **mirror port** where a frame analyzer can be attached to analyze the frame flow. The traffic to be copied on the **mirror port** is selected as follows:

1. All frames received on a given port (also known as ingress or source mirroring).
2. All frames transmitted on a given port (also known as egress or destination mirroring).

Configuration	Description
Port to mirror to	Port to mirror also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.
Port	The logical port for the settings contained in the same row.
Mode	Select mirror mode. *Rx only*: Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored. *Tx only:* Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored. *Disabled:* Neither frames transmitted nor frames received are mirrored. *Enabled*: Frames received and frames transmitted are mirrored on the mirror port. *Note: For a given port, a frame is only transmitted once. It is therefore not possible*

	to mirror mirror port Tx frames. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.18 UPnP

UPnP Configuration

Mode	Disabled
TTL	4
Advertising Duration	100

Save Reset

Configuration	**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 a 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
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.19 sFlow

sFlow Configuration

Receiver Configuration

Owner	<none>	Release
IP Address/Hostname	0.0.0.0	
UDP Port	6343	
Timeout	0	seconds
Max. Datagram Size	1400	bytes

Port Configuration

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	☐			☐	
1	☐	0	128	☐	0
2	☐	0	128	☐	0
3	☐	0	128	☐	0
4	☐	0	128	☐	0
5	☐	0	128	☐	0
6	☐	0	128	☐	0

Save Reset

Receiver Configuration Description

Owner	Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows: • If sFlow is currently unconfigured/unclaimed, Owner contains <none>. • If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>. • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration. The button allows for releasing the current owner and disable sFlow sampling.
Release	The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).
IP Address/Hostname	The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

UDP Port	The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
Timeout	The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.
Max. Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

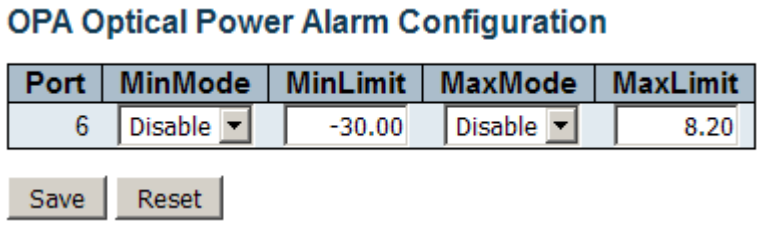
Port Configuration

Port	The port number for which the configuration below applies.
Flow Sampler	
Enabled	Enables/disables flow sampling on this port.
Sampling Rate	The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.
Max. Header	The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.
Counter Poller	
Enabled	Enables/disables counter polling on this port.
Interval	With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

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

2.20 OPA (Optical Power Alarm) Configuration

OPA function allows to set lower and upper alarm thresholds for the optical power of the fiber ports. The alarm is sent via relay alarm output and SNMP trap. The optical power is monitored once every second. Note that if no SFP transceiver is installed or no DDM is supported in the SFP transceiver, OPA function is dsiabled automatically.



Configuration	Description
Port	The fiber optical port number
MinMode	enable alarm if power is less than the lower threshold
MinLimit	set lower threshold limit, unit dBm
ManMode	enable alarm if power is higher than the upper threshold
ManLimit	set upper threshold limit, unit dBm
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Note:

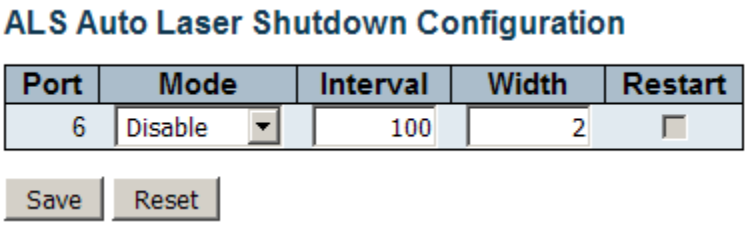
The alarm can be via relay alarm output and SNP trap. The alarm via SNMP trap can be disabled. Refer to ***Configuration > Security > Switch > SNMP > System*** *page for SNMP Trap Configuration.*

2.21 ALS (Auto Laser Shutdown) Configuration

ALS function is supported for the SFP transceiver and used to automatically shut down the output power of the transmitter in case of fiber break. ALS is provisioned on both ends of the fiber pair. “Auto” mode is set to turn on transmitter automatically if the broken fiber is believed to have been repaired.

The method is to turn on transmitter at the near end for a test pulse period every interval time. This pulse causes LOS cleared at the far end if the cable has been repaired. The transmitter is turned on at the far end. At the same time LOS cleared is also detected at the near end. Transmitters of both ends are turned on and LOS alarm is cleared.

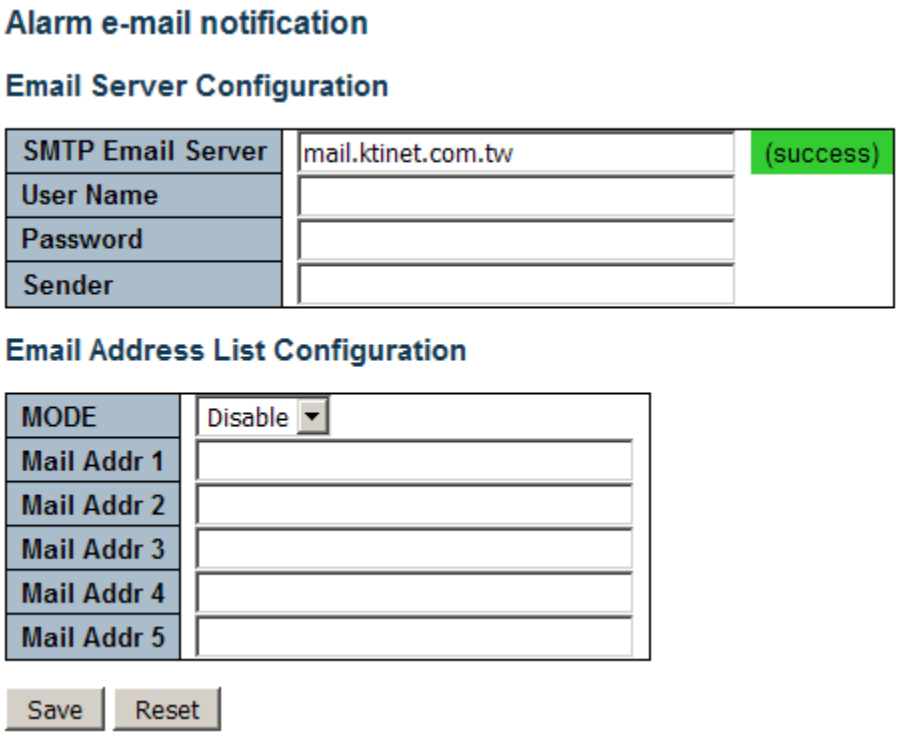
LOS set for 500ms up is confirmed as an optical loss and indicates a possible cable break. The laser transmitter is turned off immediately. The transmitter is restarted if LOS is cleared for 100ms up.



Configuration	Description
Port	The fiber optical port number
Mode	ALS mode for the port
	Disable – disable ALS function
	Manual – restart the transmitter for one test pulse period
	Automatic – restart the transmitter for a test pulse period every one interval time
Interval	Set interval time for *Automatic* mode, unit second
Width	The width of the test pulse, unit second, default 2
Restart	Check to turn transmitter on for one test pulse, used in *Manual* mode
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

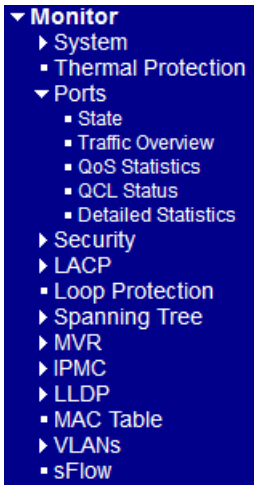
2.22 Alarm e-mail

When alarm event occurs the notification can be sent over SMTP Email. The configuration is:



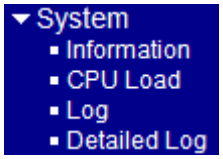
Configuration	Description
SMTP Email Server	Name of the SMTP Email server (Note: TLS encryption is not supported.)
User Name	Enter user account
Password	Enter user password
Sender	Sender Email address
Mode	Enabled/Disabled alarm e-mail function
Mail Addr 1~5	Email address accounts (Up to 5 accounts)
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

3. Monitor



Icon	Function
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Updates the system log entries, starting from the current entry ID.
Clear	Flushes the selected log entries.
|<<	Updates the system log entries, starting from the first available entry ID.
<<	Updates the system log entries, ending at the last entry currently displayed.
>>	Updates the system log entries, starting from the last entry currently displayed.
>>|	Updates the system log entries, ending at the last available entry ID.
Port 1	Selects port number to display the associated status.

3.1 System



3.1.1 Information

System Information

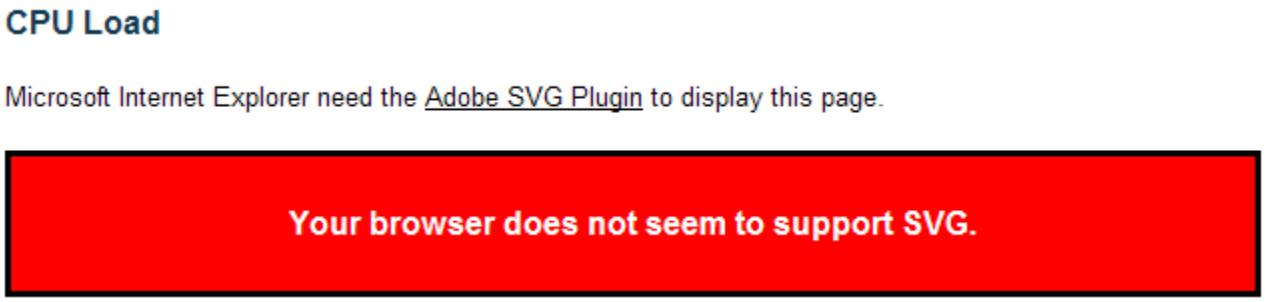
System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-40-f3-ff-06-00
Chip ID	VSC7424
Time	
System Date	2016-09-02T07:51:42+00:00
System Uptime	4d 05:16:14
Software	
Software Version	v1.0_beta_2016082910
Software Date	2016-08-29T10:28:10+08:00
Acknowledgments	Details

Status	Description
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person.
System Name	An administratively assigned name for this managed node.
System Location	The physical location of this node (e.g., telephone closet, 3rd floor)
MAC Address	The MAC Address of this switch.
Chip ID	The Chip ID of this switch.
System Date	The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.
System Uptime	The period of time the device has been operational.
Chip ID	The Chip ID of this switch.
Software Version	The software version of this switch
Software Date	The date when the switch software was produced.
Acknowledgments	Contribution of some open source code components

3.1.2 CPU Load

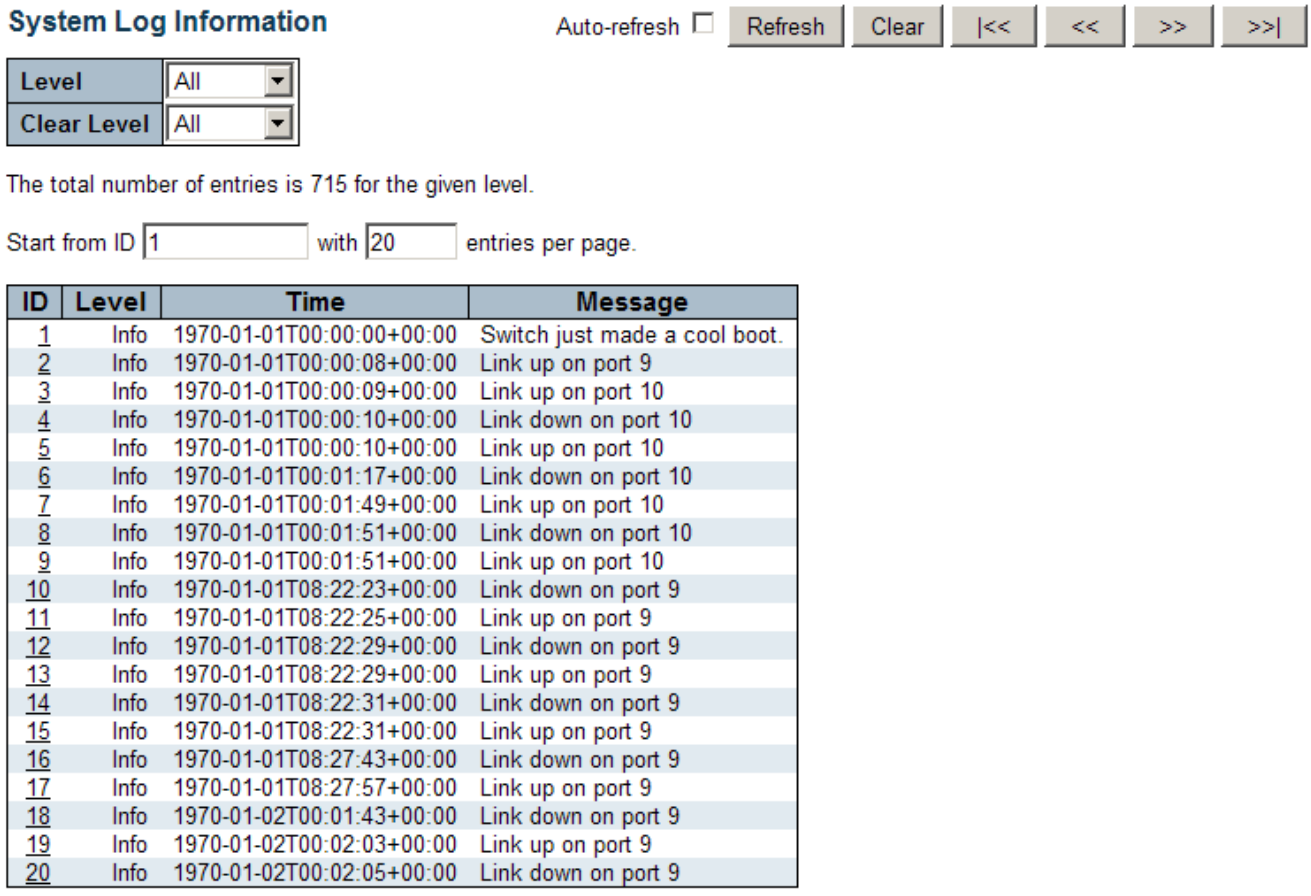
This page displays the CPU load, using an SVG graph. The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

In order to display the SVG graph, your browser must support the SVG format. The system needs Adobe SVG Plugin software to support this page; otherwise a message displayed as:



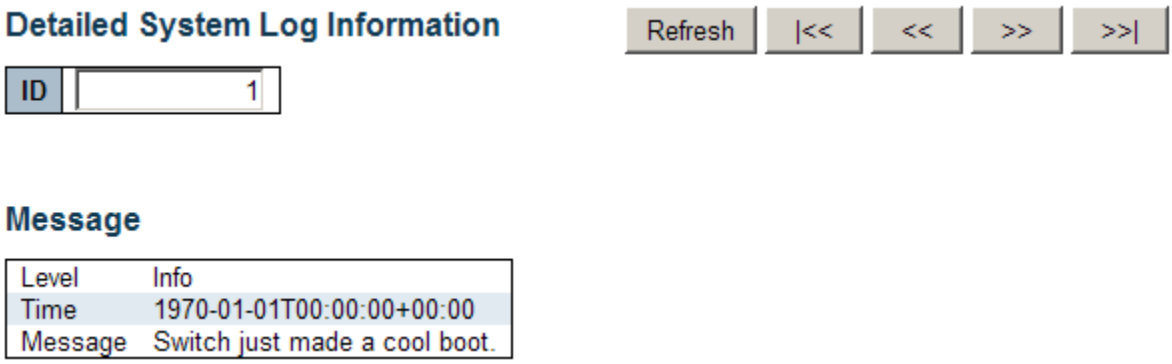
Normal Display

3.1.3 Log



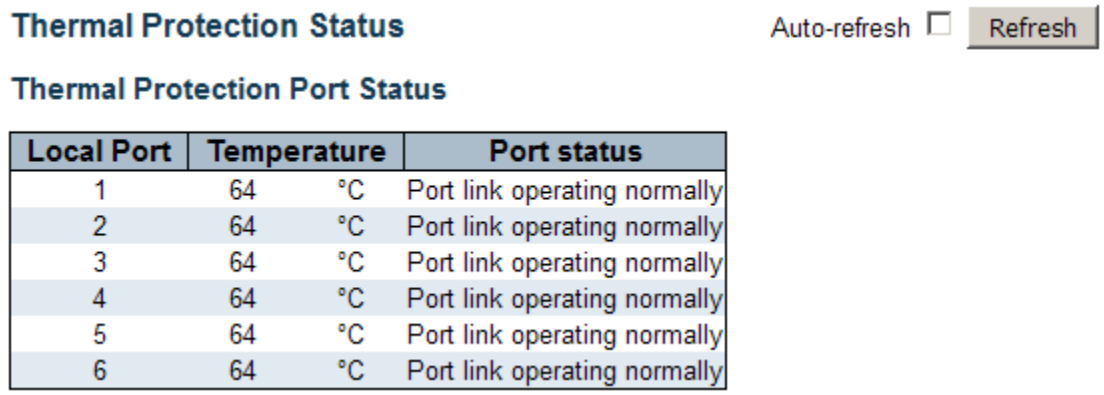
Status	Description
System Log	
Level	Specify the level of log entries for display and refresh.
Clear Level	Specify the level of log entries for Clear button.
ID	The ID (>= 1) of the system log entry.
Level	The level of the system log entry. The following level types are supported: ***Info***: Information level of the system log. ***Warning***: Warning level of the system log. ***Error***: Error level of the system log. ***All***: All levels.
Time	The time of the system log entry.
Message	The message of the system log entry.

3.1.4 Detailed Log



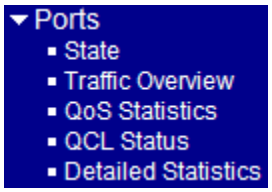
Status	Description
ID	The ID (>= 1) of the system log entry.
Message	The detailed message of the system log entry.

3.2 Thermal Protection



Status	Description
Thermal Protection	
Port Status	Shows if the port is thermally protected (link is down) or if the port is operating normally.
Chip Temperature	Shows the current chip temperature in degrees Celsius

3.3 Ports



3.3.1 State

Status	Description
	RJ-45 port disabled
	RJ-45 port link down
	RJ-45 port link up
	SFP port disabled
	SFP port link down
	SFP port link in 1G full duplex
	SFP port link in 100M full duplex

3.3.2 Traffic Overview

Port Statistics Overview

Auto-refresh ☐ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	3259877	406864	600504314	30821196	0	0	0	0	891920
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

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

3.3.3 QoS Statistics

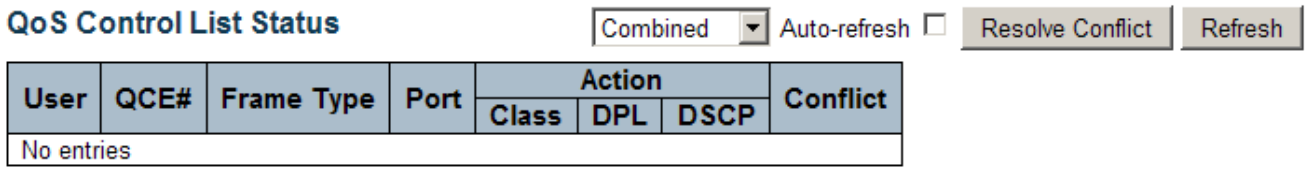
Queuing Counters

Auto-refresh ☐ Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	3260344	0	0	0	0	0	0	0	0	0	0	0	0	0	0	406984
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

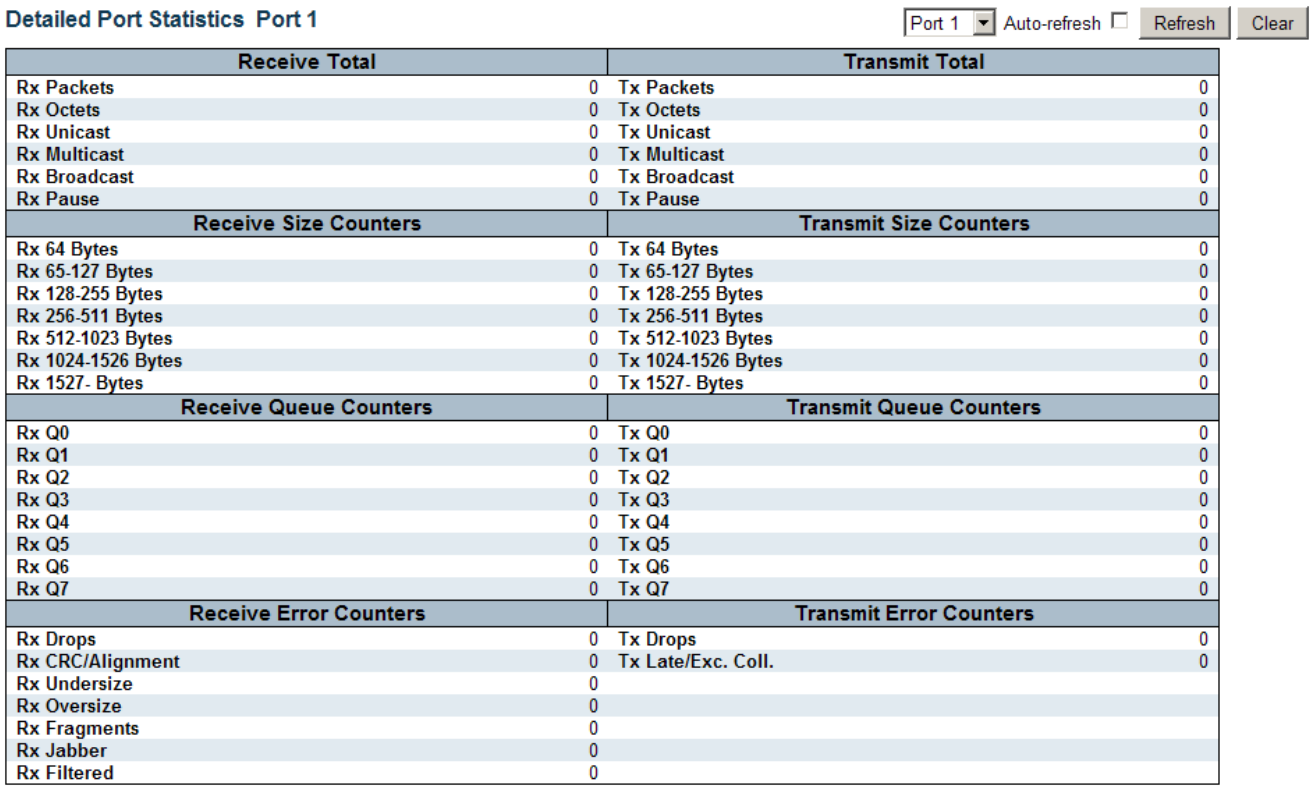
Status	Description
Port	The logical port for the settings contained in the same row.
Qn	There are 8 QoS queues per port. Q0 is the lowest priority queue.
Rx/Tx	The number of received and transmitted packets per queue

3.3.4 QCL Status



Status	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 class; if a frame matches the QCE it will be put in the queue. *DPL*: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column. *DSCP*: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.
Conflict	Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.
Resolve Conflict	Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

3.3.5 Detailed Statistics



Status	Description
Receive Total and Transmit Total	
Rx and Tx Packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Receive and Transmit Size Counters	
Rx and Tx xxxx Bytes	The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.
Receive and Transmit Queue Counters	
Rx and Tx Qn	The number of received and transmitted packets per input and output queue
Receive Error Counters	
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.

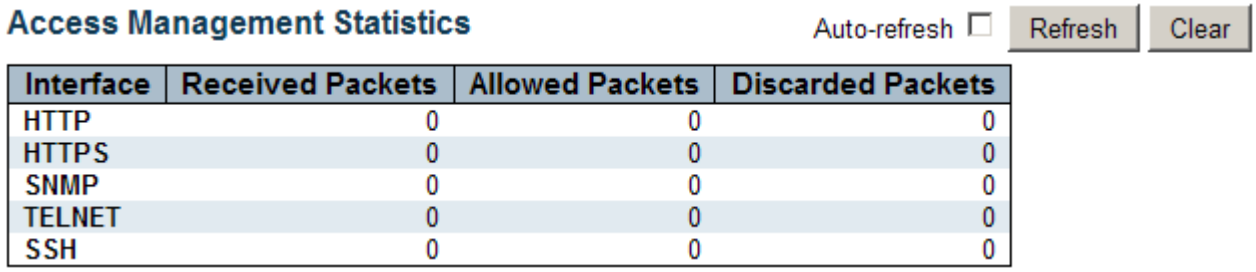
Rx Undersize	The number of short 1 frames received with valid CRC.
Rx Oversize	The number of long 2 frames received with valid CRC.
Rx Fragments	The number of short 1 frames received with invalid CRC.
Rx Jabber	The number of long 2 frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.
	1 Short frames are frames that are smaller than 64 bytes.
	2 Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late/Exc. Coll.	The number of frames dropped due to excessive or late collisions.

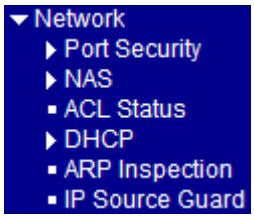
3.4 Security

3.4.1 Access Management Statistics



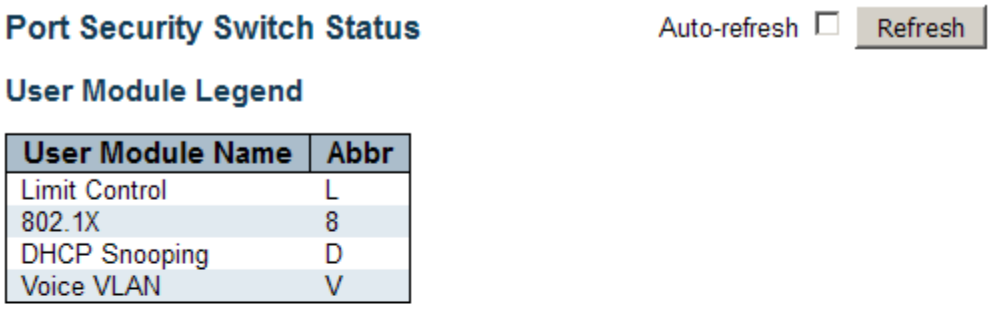
Status	Description
Interface	The interface type through which the remote host can access the switch.
Received Packets	Number of received packets from the interface when access management mode is enabled
Allowed Packets	Number of allowed packets from the interface when access management mode is enabled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

3.4.2 Network



3.4.2.1 Port Security

3.4.2.1.1 Switch



Status	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.
Port Status	The table has one row for each port on the selected switch in the stack and a number of columns, which are:
Port	The port number for which the status applies. Click the port number to see the status for this particular port.
Users	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.
State	Shows the current state of the port. It can take one of four values: *Disabled*: No user modules are currently using the Port Security service. *Ready*: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. *Limit Reached*: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. *Shutdown*: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses

can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

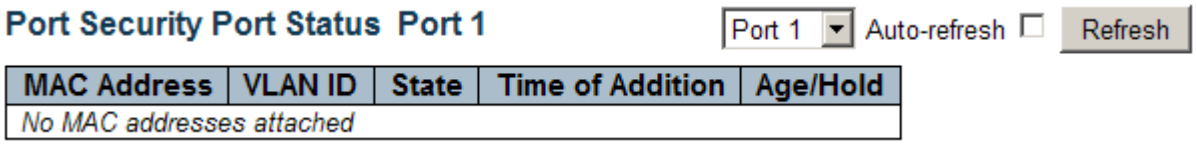
MAC Count (Current, Limit)

The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

If no user modules are enabled on the port, the Current column will show a dash (-).

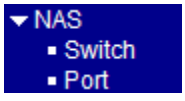
If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

3.4.2.1.2 Port

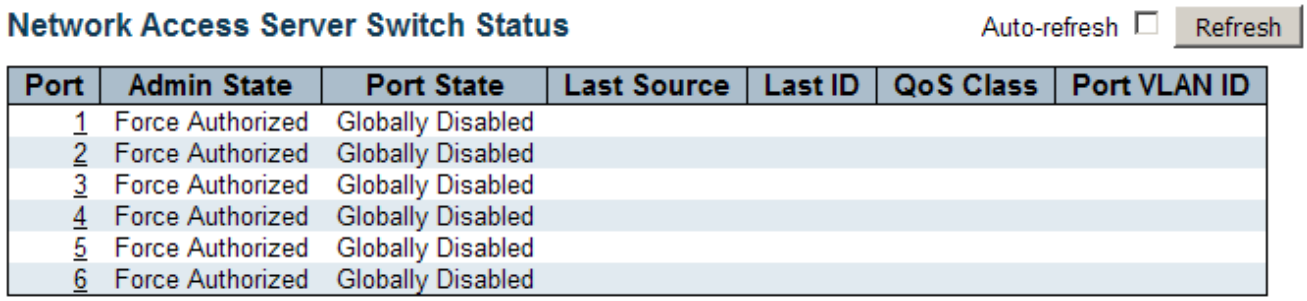


Status	Description
MAC Address & VLAN ID	The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.
State	Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
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.

3.4.2.2 NAS

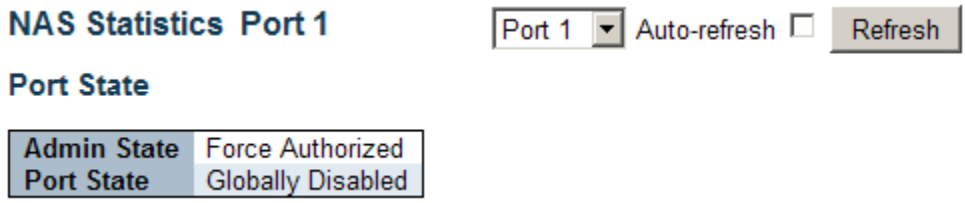


3.4.2.2.1 Switch



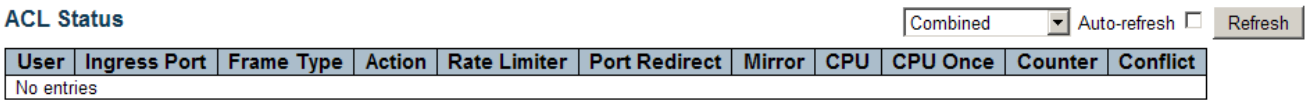
Status	Description
Port	The switch port number. Click to navigate to detailed NAS statistics for this port.
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description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

3.4.2.2.2 Port



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

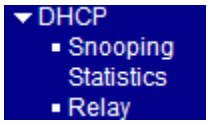
3.4.2.3 ACL Status



Status	Description
User	Indicates the ACL user.
Ingress Port	Indicates the ingress port of the ACE. Possible values are: *All*: The ACE will match all ingress port. *Port*: The ACE will match a specific ingress port.
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.
Port Copy	Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
Mirror	Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled".
CPU	Forward packet that matched the specific ACE to CPU
CPU Once	Forward first 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.

3.4.2.4 DHCP



3.4.2.4.1 Snooping Statistics

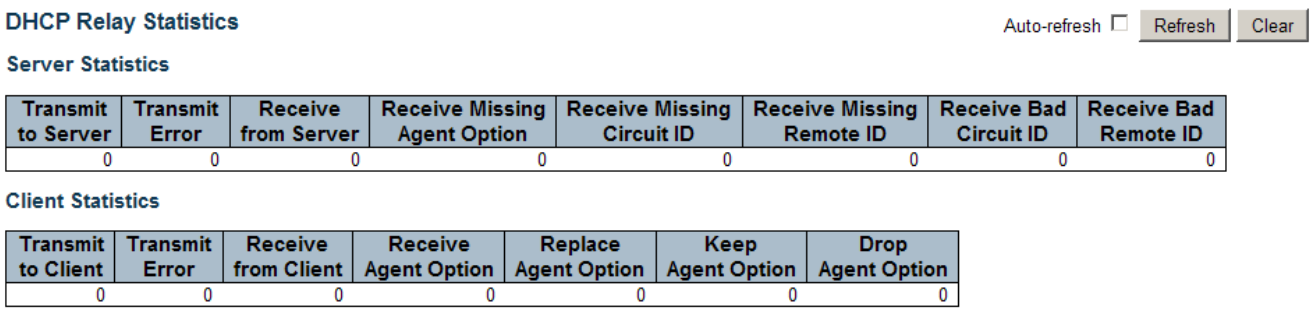
DHCP Snooping Port Statistics Port 1

Port 1 | Auto-refresh | Refresh | Clear

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0

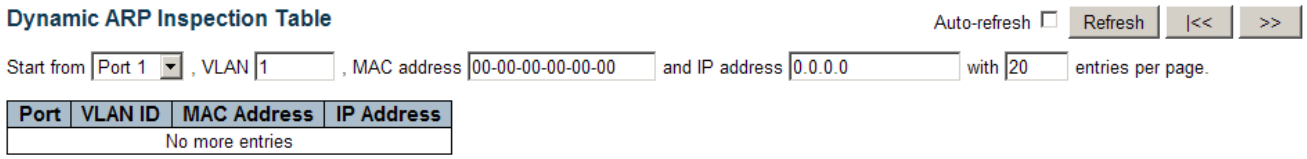
Status	Description
Receive and Transmit Packets	
Rx and Tx Discover	The number of discover (option 53 with value 1) packets received and transmitted.
Rx and Tx Offer	The number of offer (option 53 with value 2) packets received and transmitted.
Rx and Tx Request	The number of request (option 53 with 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

3.4.2.4.2 Relay



Status	Description
Server Statistics	
Transmit to Server	The number of packets that are relayed from client to server.
Transmit Error	The number of packets that resulted in errors while being sent to clients.
Receive from Server	The number of packets received from server.
Receive Missing Agent Option	The number of packets received without agent information options.
Receive Missing Circuit ID	The number of packets received with the Circuit ID option missing.
Receive Missing Remote ID	The number of packets received with the Remote ID option missing.
Receive Bad Circuit ID	The number of packets whose Circuit ID option did not match known circuit ID.
Receive Bad Remote ID	The number of packets whose Remote ID option did not match known Remote ID.
Client Statistics	
Transmit to Client	The number of relayed packets from server to client.
Transmit Error	The number of packets that resulted in error while being sent to servers.
Receive from Client	The number of received packets from server.
Receive Agent Option	The number of received packets with relay agent information option.
Replace Agent Option	The number of packets which were replaced with relay agent information option.
Keep Agent Option	The number of packets whose relay agent information was retained.
Drop Agent Option	The number of packets that were dropped which were received with relay agent information.

3.4.2.5 ARP Inspection

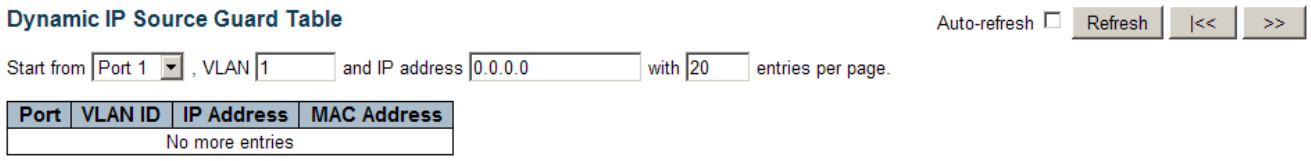


The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table.

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

3.4.2.6 IP Source Guard

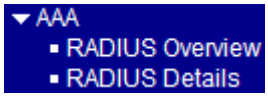


The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table.

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

3.4.3 AAA



3.4.3.1 RADIUS Overview

RADIUS Authentication Server Status Overview

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

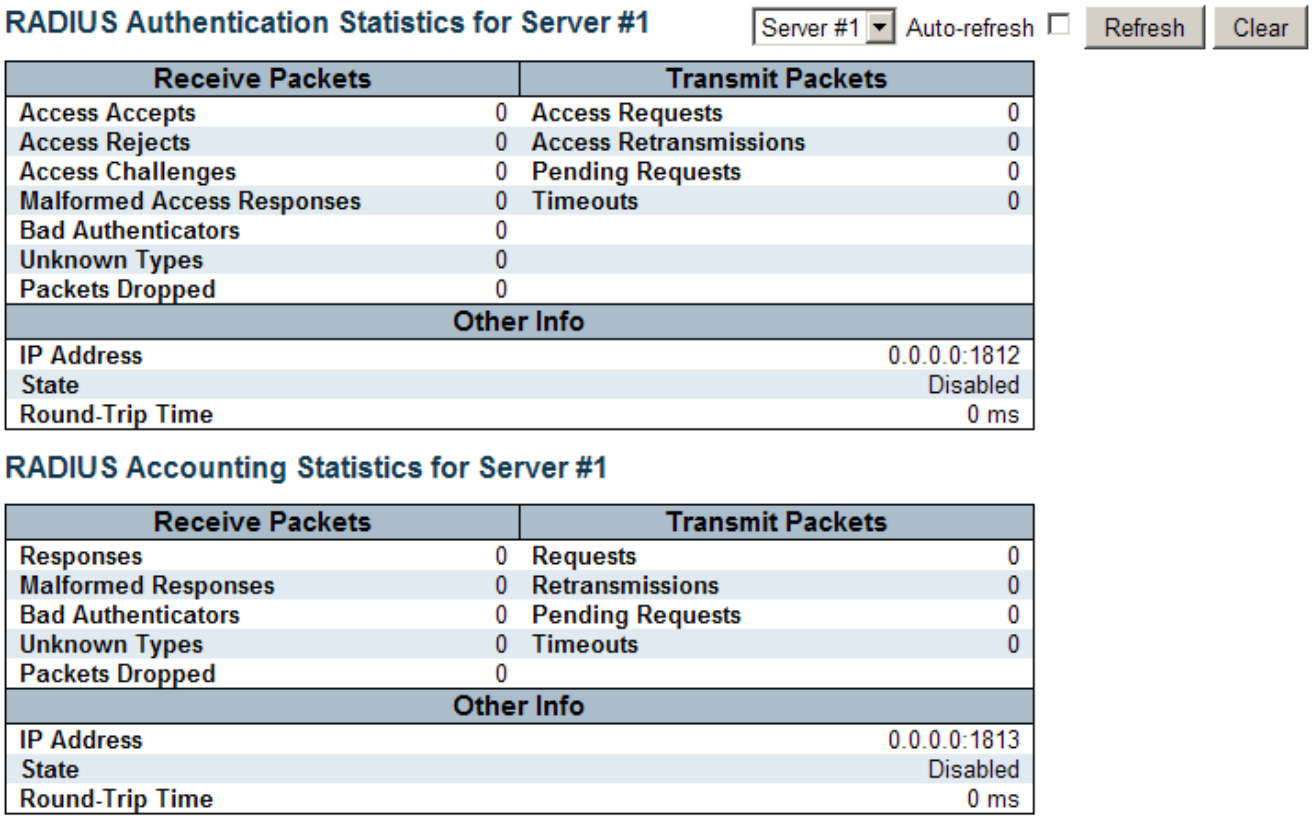
RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

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

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

3.4.3.2 RADIUS Details



Server #1	Selects a RADIUS server to display.

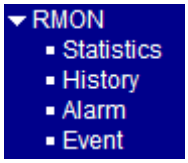
Authentication Server	Description
Server #	Select a RADIUS server number.
Rx Access Accepts	RFC4670 name: radiusAuthClientExtAccessAccepts The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx Access Rejects	RFC4670 name: radiusAuthClientExtAccessRejects The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx Access Challenges	RFC4670 name: radiusAuthClientExtAccessChallenges The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx Malformed Access Responses	RFC4670 name: radiusAuthClientExtMalformedAccessResponses The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Rx Bad Authenticators	RFC4670 name: radiusAuthClientExtBadAuthenticators The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx Unknown Types	RFC4670 name: radiusAuthClientExtUnknownTypes The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Rx Packets Dropped	RFC4670 name: radiusAuthClientExtPacketsDropped The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx Access Requests	RFC4670 name: radiusAuthClientExtAccessRequests The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx Access Retransmissions	RFC4670 name: radiusAuthClientExtAccessRetransmissions The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx Pending Requests	RFC4670 name: radiusAuthClientExtPendingRequests The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an

	Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx Timeouts	RFC4670 name: radiusAuthClientExtTimeouts The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
IP Address	The IP address of the selected server
State	Shows the state of the server. It takes one of the following values: ***Disabled:*** The selected server is disabled. ***Not Ready:*** The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. ***Dead (X seconds left):*** Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	RFC4670 name: radiusAuthClientExtRoundTripTime The time interval (measured in milliseconds) is between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

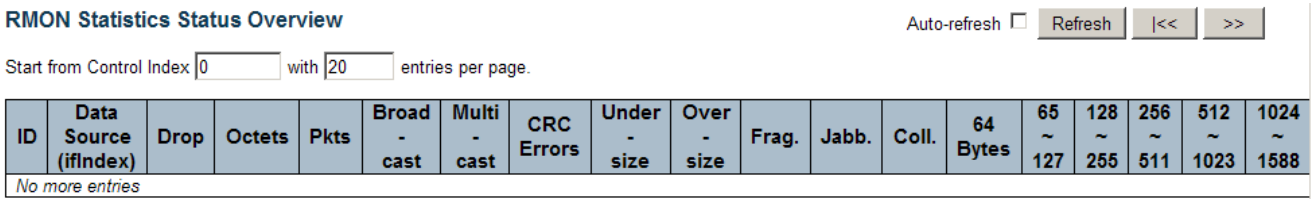
Accounting Server	**Description**
Rx Responses	RFC4670 name: radiusAccClientExtResponses The number of RADIUS packets (valid or invalid) received from the server.
Rx Malformed Responses	RFC4670 name: radiusAccClientExtMalformedResponses The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or or unknown types are not included as malformed access responses.
Rx Bad Authenticators	RFC4670 name: radiusAcctClientExtBadAuthenticators The number of RADIUS packets containing invalid authenticators received from the server.
Rx Unknown Types	RFC4670 name: radiusAccClientExtUnknownTypes The number of RADIUS packets of unknown types that were received from the

	server on the accounting port.
Rx Packets Dropped	RFC4670 name: radiusAccClientExtPacketsDropped The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx Requests	RFC4670 name: radiusAccClientExtRequests The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx Retransmissions	RFC4670 name: radiusAccClientExtRetransmissions The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx Pending Requests	RFC4670 name: radiusAccClientExtPendingRequests The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx Timeouts	RFC4670 name: radiusAccClientExtTimeouts The number of accounting timeouts to the server After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
IP Address	The IP address of the selected server
State	Shows the state of the server. It takes one of the following values: ***Disabled:*** The selected server is disabled. ***Not Ready:*** The server is enabled, but IP communication is not yet up and running. ***Ready:*** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. ***Dead (X seconds left):*** Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAccClientExtRoundTripTime The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

3.4.4 Switch-RMON



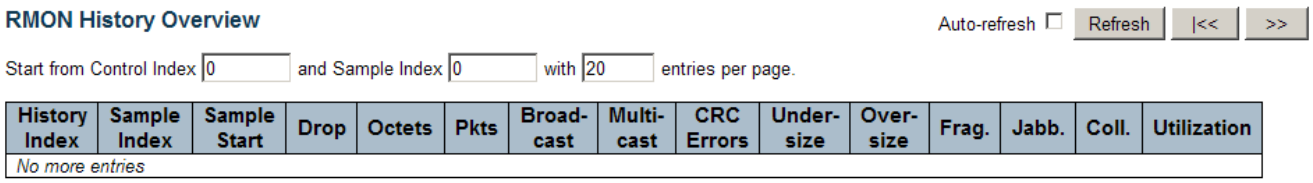
3.4.4.1 Statistics



Status	Description
ID	Indicates the index of Statistics entry.
Data Source(ifIndex)	The port ID which wants to be monitored.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broad-cast	The total number of good packets received that were directed to the broadcast address.
Multi-cast	The total number of good packets received that were directed to a multicast address.
CRC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Under-size	The total number of packets received that were less than 64 octets.
Over-size	The total number of packets received that were longer than 1518 octets.
Frag.	The number of frames which size is less than 64 octets received with invalid CRC.
Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
64	The total number of packets (including bad packets) received that were 64 octets in length.
65~127	The total number of packets (including bad packets) received that were between 65 to

	127 octets in length.
128~255	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
256~511	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
512~1023	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
1024~1588	The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

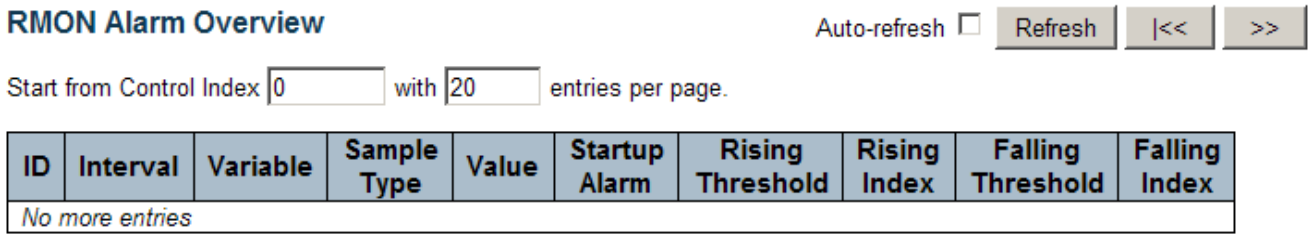
3.4.4.2 History



Status	Description
History Index	Indicates the index of History control entry.
Sample Index	Indicates the index of the data entry associated with the control entry.
Sample Start	The value of sysUpTime at the start of the interval over which this sample was measured.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	The total number of good packets received that were directed to the broadcast address.
Multicast	The total number of good packets received that were directed to a multicast address.
CRCErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	The total number of packets received that were less than 64 octets.
Oversize	The total number of packets received that were longer than 1518 octets.
Frag.	The number of frames which size is less than 64 octets received with invalid CRC.

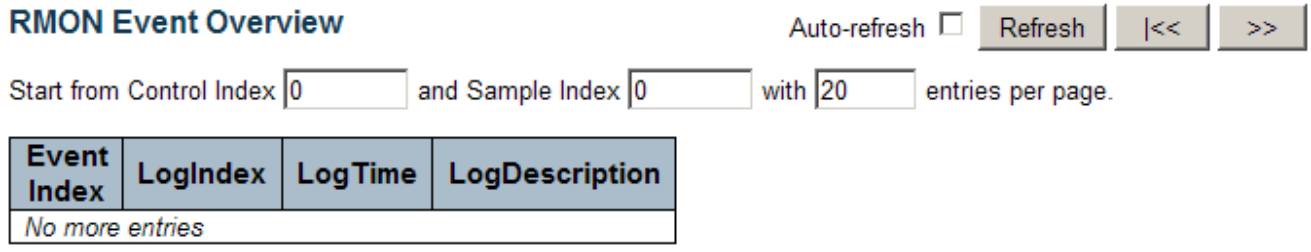
Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

3.4.4.3 Alarm



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

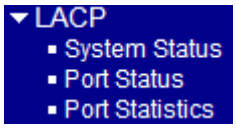
3.4.4.4 Event



Status	Description
Event Index	Indicates the index of the event entry.

Log Index	Indicates the index of the log entry.
LogTIme	Indicates Event log time
LogDescription	Indicates the Event description.

3.5 LACP



3.5.1 System Status

LACP System Status

Auto-refresh ☐ Refresh

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

Status	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The Key that the partner has assigned to this aggregation ID.
Last changed	The time since this aggregation changed.
Local Ports	Shows which ports are a part of this aggregation for this switch. The format is: "Switch ID:Port".

3.5.2 Port Status

LACP Status

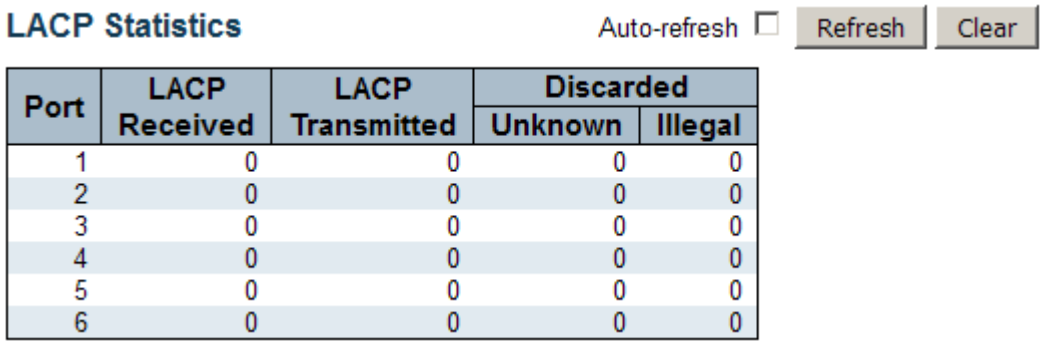
Auto-refresh ☐ Refresh

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

Status	Description
Port	The switch port number.
LACP	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.
Key	The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID	The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.
Partner System ID	The partner's System ID (MAC address).
Partner Port	The partner's port number connected to this port.
Partner Prio	The partner's port priority.

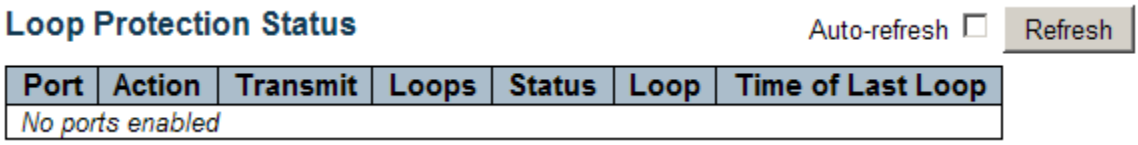
3.5.3 Port Statistics



Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0

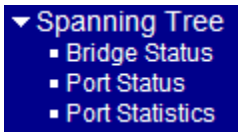
Status	**Description**
Port	The switch port number.
LACP Received	Shows how many LACP frames have been received at each port.
LACP Transmitted	Shows how many LACP frames have been sent from each port.
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.

3.6 Loop Protection



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

3.7 Spanning Tree



3.7.1 Bridge Status

STP Bridges

Auto-refresh ☐ Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-40-F6-01-09-05	32768.00-40-F6-01-09-05	-	0	Steady	-

Status	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 it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Topology Flag	The current state of the Topology Change Flag of this Bridge instance.
Topology Change Last	The time since last Topology Change occurred.

3.7.2 Port Status

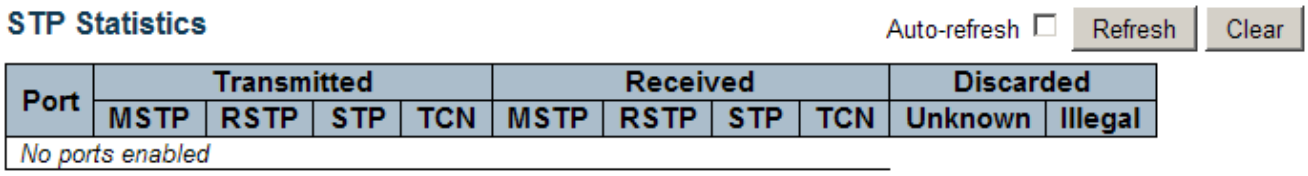
STP Port Status

Auto-refresh ☐ Refresh

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-

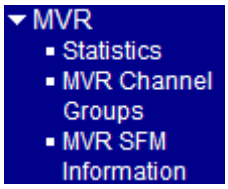
Status	Description
Port	The switch port number of the logical STP port.
CIST Role	The current STP port role of the CIST port. The port role can be one of the following values: *AlternatePort, BackupPort, RootPort, DesignatedPort, Disabled*.
CIST State	The current STP port state of the CIST port. The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

3.7.3 Port Statistics

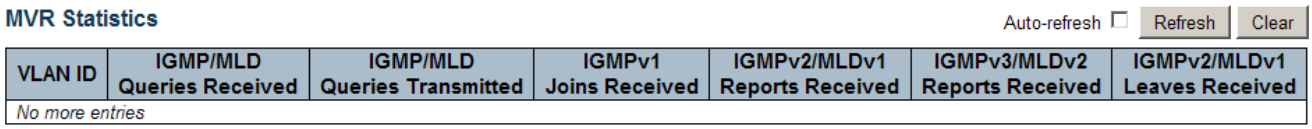


Status	Description
Port	The switch port number of the logical STP port.
MSTP	The number of MSTP BPDU's received/transmitted on the port.
RSTP	The number of RSTP BPDU's received/transmitted on the port.
STP	The number of legacy STP Configuration BPDU's received/transmitted on the port.
TCN	The number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

3.8 MVR



3.8.1 Statistics

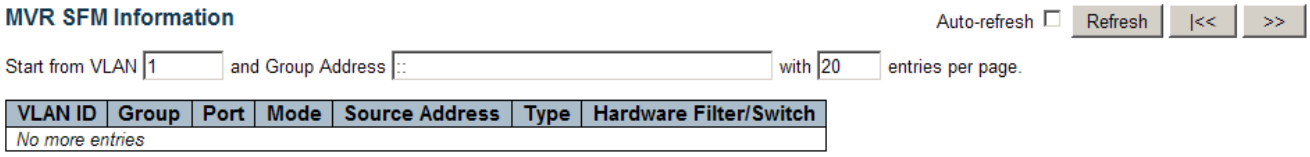


Status	Description
VLAN ID	The Multicast VLAN ID.
IGMP/MLD Queries Received	The number of Received Queries for IGMP and MLD, respectively.
IGMP/MLD Queries Transmitted	The number of Transmitted Queries for IGMP and MLD, respectively.
IGMPv1 Joins Received	The number of Received IGMPv1 Join's.
IGMPv2/MLDv1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

3.8.2 MVR Channel Groups

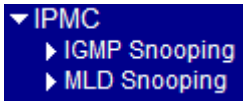
Status	Description
VLAN ID	VLAN ID of the group.
Groups	Group ID of the group displayed.
Port Members	Ports under this group.

3.8.3 MVR SFM Information

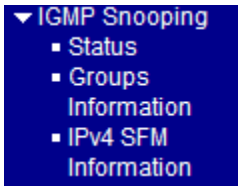


Status	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either ***Include*** or ***Exclude***.
Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.
Type	Indicates the Type. It can be either ***Allow*** or ***Deny***.
Hardware Filter/Switch	Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

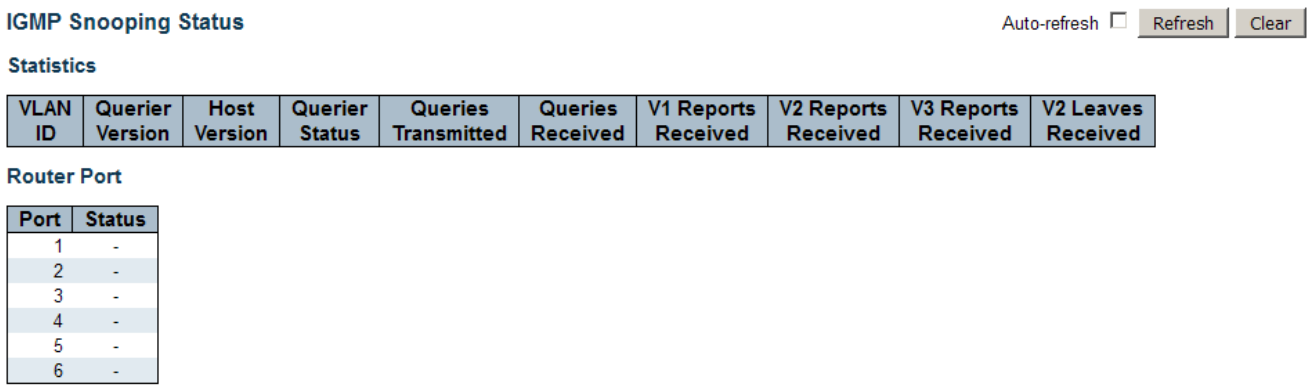
3.9 IPMC



3.9.1 IGMP Snooping



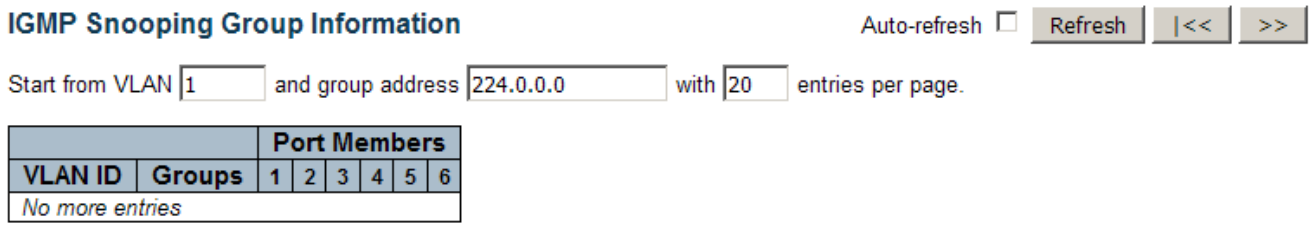
3.9.1.1 Status



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

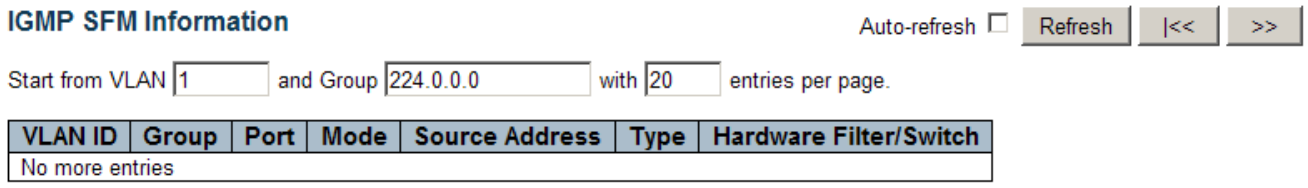
	Both denote the specific port is configured or learnt to be a router port.
Port	Switch port number.
Status	Indicate whether specific port is a router port or not.

3.9.1.2 Groups Information



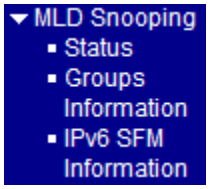
Status	Description
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

3.9.1.3 IPv4 SFM Information

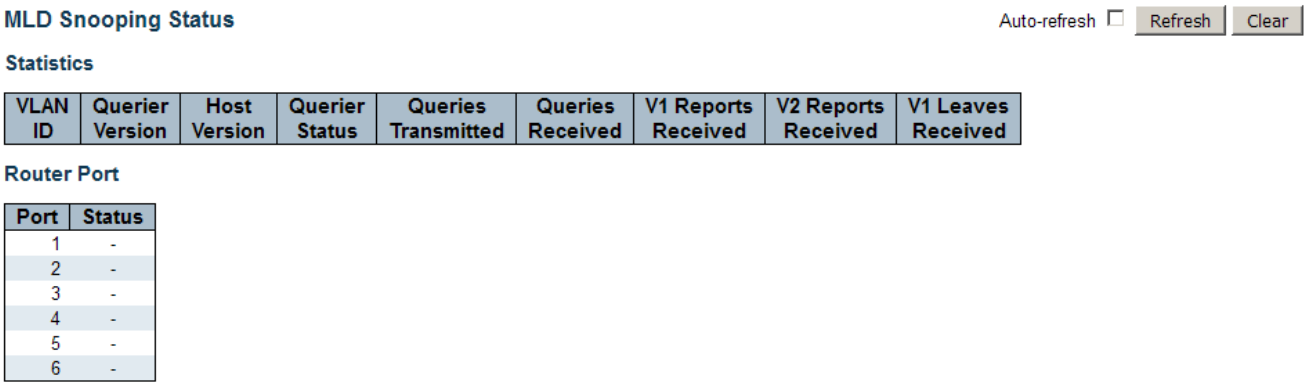


Status	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either ***Include*** or ***Exclude***.
Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
Type	Indicates the Type. It can be either ***Allow*** or ***Deny***.
Hardware Filter/Switch	Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

3.9.2 MLD Snooping



3.9.2.1 Status



Status	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Shows the Querier status is ***ACTIVE*** or ***IDLE***. "***DISABLE***" denotes the specific interface is administratively disabled.
Queries Transmitted	The number of Transmitted Queries.
Queries Received	The number of Received Queries.
V1 Reports Received	The number of Received V1 Reports.
V2 Reports Received	The number of Received V2 Reports.
V1 Leaves Received	The number of Received V1 Leaves.
Router Port	Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.
Port	Switch port number.
Status	Indicate whether specific port is a router port or not.

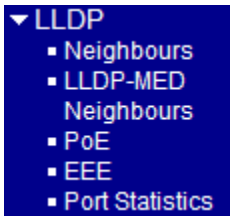
3.9.2.2 Groups Information

Status	Description
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

3.9.2.3 IPv6 SFM Information

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

3.10 LLDP

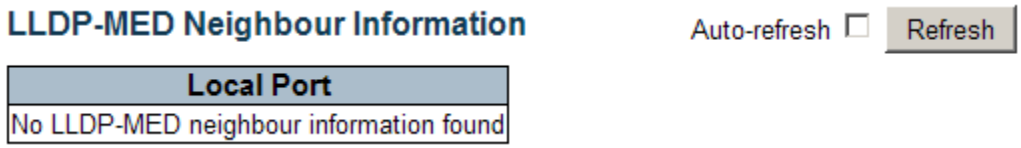


3.10.1 Neighbours

LLDP Remote Device Summary						
Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbour information found						

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

3.10.2 LLDP-MED Neighbours



Status	Description
Port	The port on which the LLDP frame was received.
Device Type	LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices. **LLDP-MED Network Connectivity Device Definition** LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies: 1. LAN Switch/Router 2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method. **LLDP-MED Endpoint Device Definition** LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I). **LLDP-MED Generic Endpoint (Class I)** The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057,

however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

LLDP-MED Capabilities

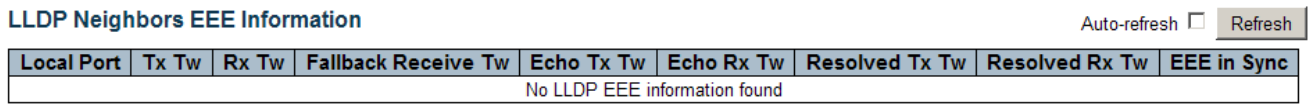
LLDP-MED Capabilities describes the neighbour unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
5. Extended Power via MDI - PD
6. Inventory

	7. Reserved
Application Type	Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below. 1. ***Voice*** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. 2. ***Voice Signaling*** - for use in network topologies that require a different policy for the voice signaling than for the voice media. 3. *Guest Voice* - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. 4. ***Guest Voice Signaling*** - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. 5. ***Softphone Voice*** - for use by softphone applications on typical data centric devices, such as PCs or laptops. 6. ***Video Conferencing*** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. 7. ***Streaming Video*** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. 8. ***Video Signaling*** - for use in network topologies that require a separate policy for the video signaling than for the video media.
Policy	Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown ***Unknown***: The network policy for the specified application type is currently unknown. ***Defined***: The network policy is defined.
TAG	TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged. ***Untagged***: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. ***Tagged***: The device is using the IEEE 802.1Q tagged frame format.
VLAN ID	VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority

	Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
Priority	Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).
DSCP	DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
Auto-negotiation	Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.
Auto-negotiation status	Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.
Auto-negotiation Capabilities	Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

3.10.3 EEE



Status	Description
Local Port	The port on which LLDP frames are received or transmitted.
Tx Tw	The link partner's maximum time that transmit path can hold-off sending data after de-assertion of LPI.
Rx Tw	The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.
Fallback Receive Tw	The link partner's fallback receive Tw. A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.
Echo Tx Tw	The link partner's Echo Tx Tw value. The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its

	echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.
Echo Rx Tw	The link partner's Echo Rx Tw value.
Resolved Tx Tw	The resolved Tx Tw for this link. Note : NOT the link partner The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).
Resolved Rx Tw	The resolved Rx Tw for this link. Note : NOT the link partner The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).
EEE in Sync	Shows whether the switch and the link partner have agreed on wake times. *Red* - Switch and link partner have not agreed on wakeup times. *Green* - Switch and link partner have agreed on wakeup times.

3.10.4 Port Statistics

LLDP Global Counters

Auto-refresh ☐ Refresh Clear

Global Counters	
Neighbour entries were last changed	2016-08-29T02:35:28+00:00 (366222 secs. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

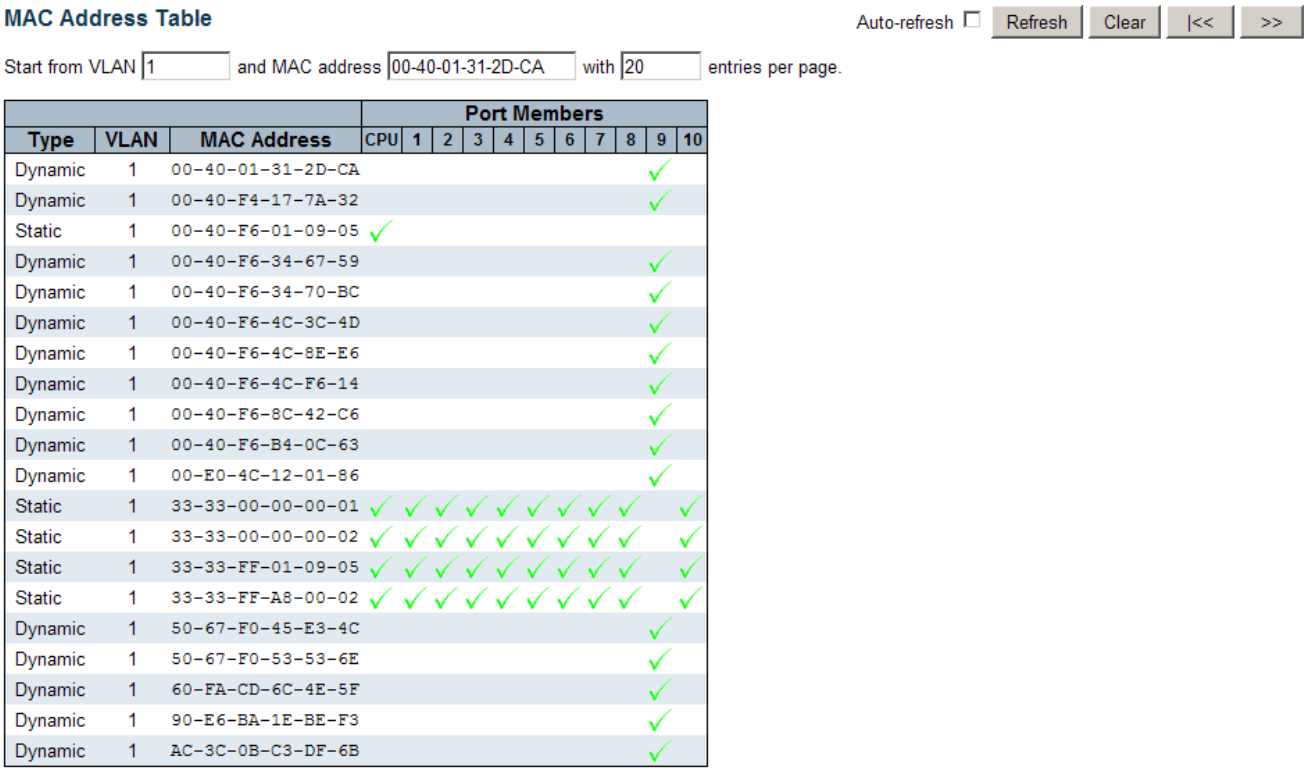
LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0

Status	**Description**
Global Counters	
Neighbour 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 Neighbours Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbours Entries Deleted	Shows the number of new entries deleted since switch reboot.

Total Neighbours Entries Dropped	
	Shows the number of LLDP frames dropped due to the entry table being full.
Total Neighbours Entries Aged Out	
	Shows the number of entries deleted due to Time-To-Live expiring.
Local Counters	The displayed table contains a row for each port. The columns hold the following information:
Local Port	The port on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing some kind of error.
Frames Discarded	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	The number of organizationally received TLVs.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

3.11 MAC Table



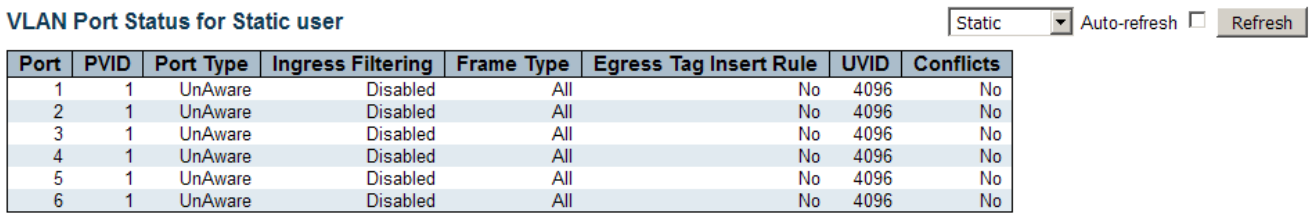
Status	Description
Type	Indicates whether the entry is a static or a dynamic entry.
MAC address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.
Port Members	The ports that are members of the entry.

3.12 VLANs

3.12.1 VLAN Membership

Status	Description
VLAN USER	VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently we support the following VLAN user types: ***Statis***: These is referred to *CLI/Web/SNMP*. ***NAS***: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server. ***Voice VLAN***: Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones. ***MVR***: MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN. ***MSTP***: The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment. ***Combined***: List all types.
VLAN ID	Indicates the ID of this particular VLAN.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. If a port is included in a VLAN, an image ✓ will be displayed. If a port is included in a Forbidden port list, an image ✗ will be displayed. If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as ✗.

3.12.2 VLAN Ports



Port	PVID	Port Type	Ingress Filtering	Frame Type	Egress Tag Insert Rule	UVID	Conflicts
1	1	UnAware	Disabled	All	No	4096	No
2	1	UnAware	Disabled	All	No	4096	No
3	1	UnAware	Disabled	All	No	4096	No
4	1	UnAware	Disabled	All	No	4096	No
5	1	UnAware	Disabled	All	No	4096	No
6	1	UnAware	Disabled	All	No	4096	No

VLAN USER

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN User types:

Statis*:* This is referred to *CLI/Web/SNMP*:.

NAS: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

***MVRP*:** Multiple VLAN Registration Protocol(MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

Voice VLAN: Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

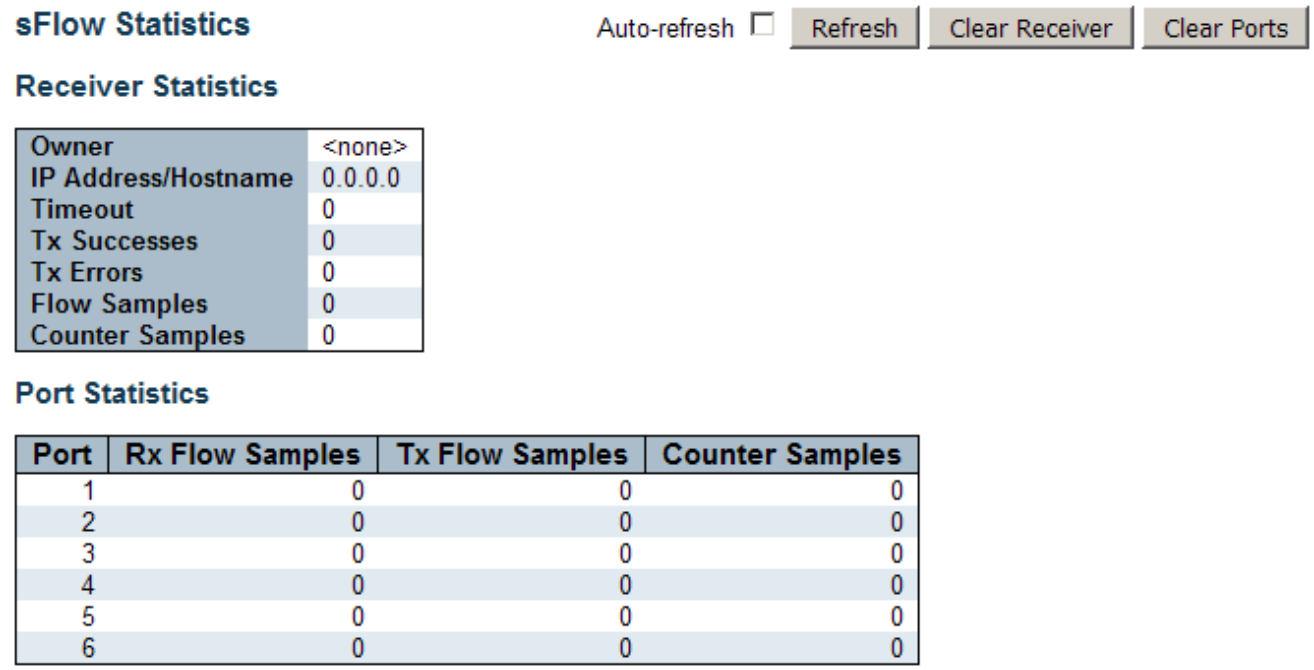
MVR: MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

MSTP: The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

Status	Description
Port	The logical port for the settings contained in the same row.
PVID	Shows the VLAN identifier for that port. The allowed values are 1 through 4095. The default value is 1.
Port Type	Shows the Port Type. Port type can be any of ***Unaware***, ***C-port***, ***S-port***, ***Custom S-port***. If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.
Ingress Filtering	Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.
Frame Type	Shows whether the port accepts all frames or only tagged frames. This parameter

	affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.
Tx Tag	Shows egress filtering frame status whether ***tagged*** or ***untagged***.
UVID	Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behaviour at the egress side.
Conflicts	Shows status of Conflicts whether exists or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur: Functional Conflicts between features. Conflicts due to hardware limitation. Direct conflict between user modules.

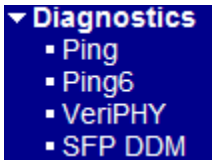
3.13 sFlow



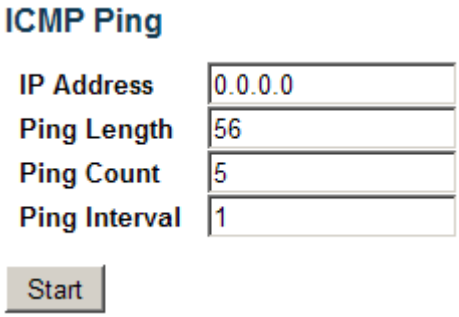
Status	Description
Owner	This field shows the current owner of the sFlow configuration. It assumes one of three values as follows: • If sFlow is currently unconfigured/unclaimed, Owner contains <none>. • If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>. • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
IP Address/Hostname	The IP address or hostname of the sFlow receiver.
Timeout	The number of seconds remaining before sampling stops and the current sFlow owner is released.
Tx Successes	The number of UDP datagrams successfully sent to the sFlow receiver.
Tx Errors	The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6).
Flow Samples	The total number of flow samples sent to the sFlow receiver.
Counter Samples	The total number of counter samples sent to the sFlow receiver.
Port	The port number for which the following statistics applies.
Rx and Tx Flow Samples	

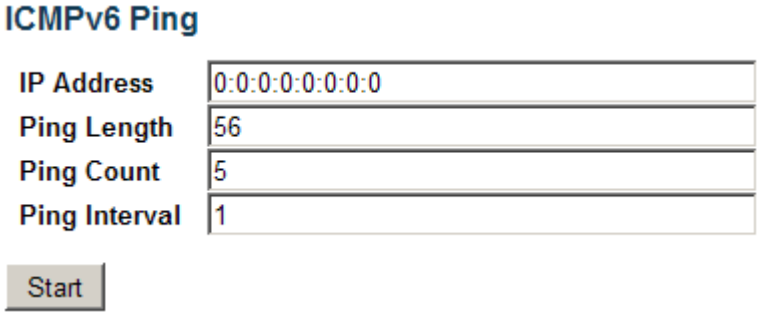
	The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.
Counter Samples	The total number of counter samples sent to the sFlow receiver originating from this port.

4. Diagnostics



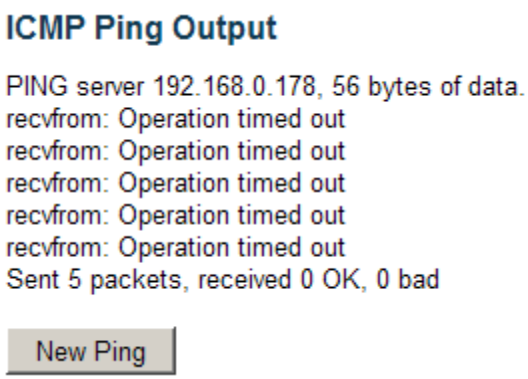
4.1 Ping & Ping6



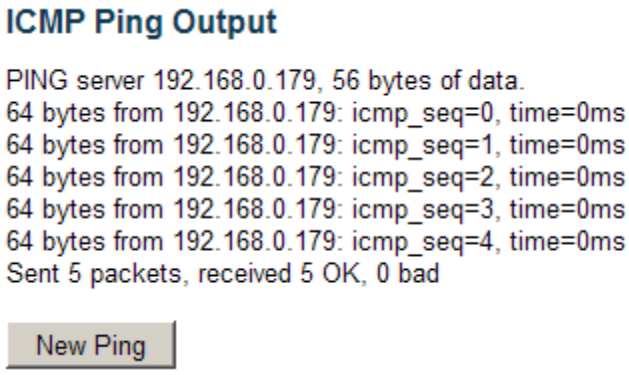


Settings	Description
IP Address	The destination IP Address.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.
Start	After you press button, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space(the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

Result displayed for a failed ping test

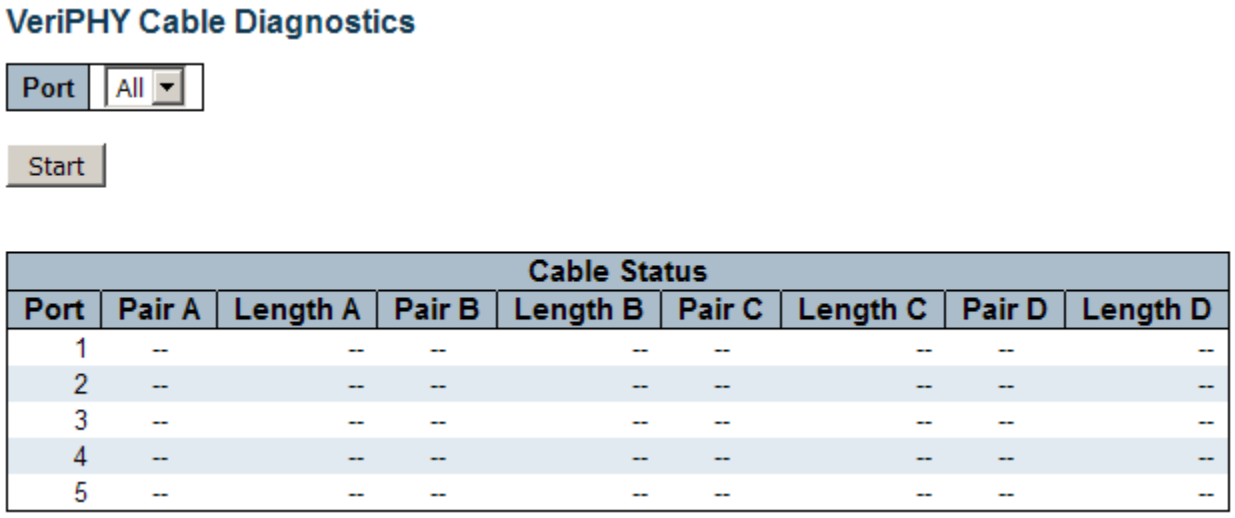


Result displayed for a successful ping test



New Ping	Click to start a new ping test.

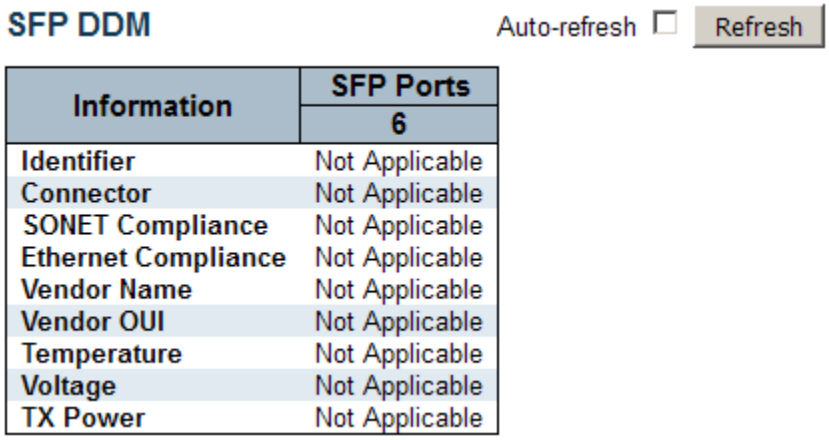
4.2 VeriPHY



Status	Description
Port	The port where you are requesting Copper Cable Diagnostics. ***All:*** select all ports
Cable Status	Port: Port number. Pair: The status of the cable pair. Pair A, B, C, D The status of the cable pair. *OK* - Correctly terminated pair *Open* - Open pair *Short* - Shorted pair *Short A* - Cross-pair short to pair A *Short B* - Cross-pair short to pair B *Short C* - Cross-pair short to pair C *Short D* - Cross-pair short to pair D *Cross A* - Abnormal cross-pair coupling with pair A *Cross B* - Abnormal cross-pair coupling with pair B *Cross C* - Abnormal cross-pair coupling with pair C *Cross D* - Abnormal cross-pair coupling with pair D **Length:** The length (in meters) of the cable pair.
Start	Click to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

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

4.3 SFP DDM



DDM Status	Description
SFP Ports	Port numbers which are equipped with SFP slot.
Identifier	Identification information of the transceiver
Connector	The connector type used on the transceiver
SONET Compliance	The SONET compliance information of the transceiver
GbE Compliance	Gigabit Ethernet compliance information of the transceiver
Vendor Name	The vendor name of the transceiver
Vendor OUI	The vendor OUI of the transceiver
Temperature	The current temperature sensed currently inside the transceiver
Voltage	The working voltage sensed currently inside the transceiver
TX Power	The transmission optical power sensed currently
RX Power	The receiving optical power sensed currently

Note: The TX power and RX power might be reported with deviation of ±3dB. Both can not be expected to be as accurate as professional optical meter provides.

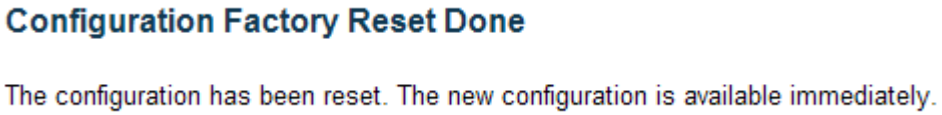
5. Maintenance

5.1 Restart Device

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

Yes — Click to reboot device. The following message is displayed as follows.

5.2 Factory Defaults

Yes	Click to reboot device. “System rebooting” message is displayed as follows. 
No	Click to return to the Port State page without rebooting.

5.3 Software

5.3.1 Upload

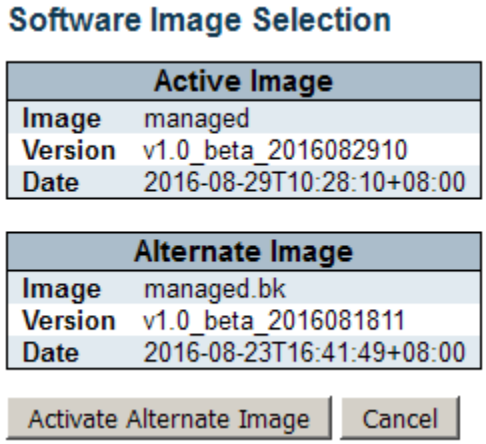
This page facilitates an update of the firmware controlling the switch.

Browse	Click to the location of a software image
Upload	Click to start uploading.

After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the software is updated and the switch reboots.

Warning**: While the software is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10Hz while the software update is in progress.* ***Do not reset or power off the device at this time *or the switch may fail to function afterwards.*

5.3.2 Image Select



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

The web page displays two tables with information about the active and alternate firmware images.

Note:

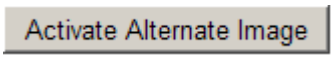
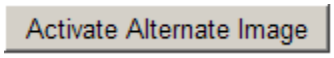
1. *In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the*  *button is also disabled.*
2. *If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.*
3. *The firmware version and date information may be empty for older firmware releases. This does not constitute an error.*

Image Information

Image	The flash index name of the firmware image. The name of primary (preferred) image is “managed”, the alternate image is named “managed.bk”.
Version	The version of the firmware image. *Remark: The version of the image currently used in your switch device might not match the one shown above. Every device was configured with the latest release of the images before being shipped from factory.*
Date	The date where the firmware was produced.

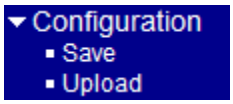


Click to use the alternate image. This button may be disabled depending on system state.

Cancel

Cancel activating the backup image. Navigates away from this page.

5.4 Configuration



5.4.1 Save

You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags:

Header tags: <?xml version="1.0"?> and <configuration>. These tags are mandatory and must be present at the beginning of the file.
Section tags: <platform>, <global> and <switch>. The platform section must be the first section tag and this section must include the correct platform ID and version. The global section is optional and includes configuration which is not related to specific switch ports. The switch section is optional and includes configuration which is related to specific switch ports.
Module tags: <ip>, <mac>, <port> etc. These tags identify a module controlling specific parts of the configuration.
Group tags: <port_table>, <vlan_table> etc. These tags identify a group of parameters, typically a table.
Parameter tags: <mode>, <entry> etc. These tags identify parameters for the specific section, module and group. The <entry> tag is used for table entries.

Configuration parameters are represented as attribute values. When saving the configuration from the switch, the entire configuration including syntax descriptions is included in the file. The file may then be modified using an editor and loaded to a switch.

The example below shows a small configuration file only including configuration of the MAC address age time and the learning mode per port. When loading this file, only the included parameters will be changed. This means that the age time will be set to 200 and the learn mode will be set to automatic.

```
<?xml version="1.0"?>
<configuration>
  <platform>
    <pid val="3"></pid>
    <version val="1"></version>
```

```
  </platform>
  <global>
    <mac>
      <age val="200"></age>>
    </mac>
  </global>
  <switch sid="1">
    <mac>
      <entry port="1-24" learn_mode="auto"></entry>
    </mac>
  </switch>
</configuration>
```

Configuration Save

Save configuration

Save configuration	Click to start download of the configuration.

5.4.2 Upload

Configuration Upload

Browse Upload

Browse	Click to the location of a configuration file
Upload	Click to start uploading configuration.

Glossary

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

ACE

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.
There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.
Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.
ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:
ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.
ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets

past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.
ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS

AMS is an acronym for Auto Media Select. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and cu cables are inserted, the port will select the prefered media.

APS

APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.
(Also *Port Aggregation, Link Aggregation*).

ARP

ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to it's peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for Cisco Discovery Protocol.

CIST

Within MSTP network, ISTs in different regions are interconnected through a common spanning tree (CST). The collection of the ISTs in each MST region, and the common spanning tree that interconnects the MST regions and single spanning trees are called the common and internal spanning tree (CIST).

D

DDM

Modern optical SFP transceivers support digital diagnostics monitoring (DDM) functions according to the industry-standard SFF-8472. This feature is also known as digital optical monitoring (DOM). Modules with this capability give the end user the ability to monitor parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage, in real time.

DEI

DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is

assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

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

DNS

DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at

network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.

An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

Drop Precedence Level

Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 or higher corresponds to 'Discard Eligible' (Yellow) frames.

DSCP

DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP

FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

This processing applies to IGMP and MLD.

H

HTTP

HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports

can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for IP MultiCast.

IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

LLC

The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The Link Layer Discovery Protocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LLQI

LLQI (Last Listener Query Interval) is the maximun response time used to calculate the Maximun Respse Code inserted into Specific Queries. It is used to detect the departure of the

last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC

LOC is an acronym for Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M

MAC Table

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

MEP

MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)
Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MSTP

In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated

in IEEE 802.1D-2005.

MSTI

It may be necessary to have different topologies for different VLANs, for load-sharing or other purposes. MSTP enables the grouping of multiple VLANs with the same topology requirements into one MST instance (MSTI). Instances are not supported in STP or RSTP, so those two versions have the same spanning-tree in common for all of the VLANs.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.
The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them(Wikipedia).

N

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).
The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.
NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM

OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier ethernet functionality. MEP functionality like CC and RDI is based on this

Optional TLVs.

A LLDP frame contains multiple TLVs

For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for Powered Device. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

PING is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

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.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress

queue.

POP3

POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for Point-to-Point Protocol over Ethernet.

It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a private VLAN, PVLANs provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

PTP

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

Q

QCE

QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

R

RARP

RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same

time being backwards-compatible with STP.

S

SAMBA

Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

SFP

The small form-factor pluggable (SFP) is a compact, hot-pluggable transceiver used for both telecommunication and data communications applications. The form factor and electrical interface are specified by a multi-source agreement (MSA). It interfaces a network device motherboard (for a switch, router, media converter or similar device) to a fiber optic or copper networking cable. It is a popular industry format jointly developed and supported by many network component vendors. SFP transceivers are designed to support SONET, Gigabit Ethernet, Fibre Channel, and other communications standards.

sFlow

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.

Additional information can be found at http://sflow.org.

SHA

SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file

transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack Protocol using ROUting Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

Switch ID

Switch IDs (1-?) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for Terminal Acess Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the

network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS

ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

TKIP is an acronym for Temporal Key Integrity Protocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

U

UDP

UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

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

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

W

WEP

WEP is an acronym for Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network

(Wikipedia).

WiFi

WiFi is an acronym for Wireless Fidelity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system , Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

WPA-PSK is an acronym for Wi-Fi Protected Access - Pre Shared Key. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

WPA-Radius is an acronym for Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPS

WPS is an acronym for Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WRED

WRED is an acronym for Weighted Random Early Detection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP

level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR

WTR is an acronym for Wait To Restore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.