KGS-2422-B

Web Management Interface

User's Manual

DOC.160811

TRADEMARKS

Ethernet is a registered trademark of Xerox Corp.

Vitesse Switch Software. Copyright (c) 2002-2009
Vitesse Semiconductor Corporation "Vitesse". All Rights Reserved.
Unpublished rights reserved under the copyright laws of the United States of America, other countries and international treaties. Permission to use, copy, store and modify, the software and its source code is granted. Permission to integrate into other products, disclose, transmit and distribute the software in an absolute machine readable format (e.g. HEX file) is also granted. The software may only be used in products utilizing the Vitesse switch products.

(C) 2015 KTI Networks Inc. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any directive work (such as translation or transformation) without permission from KTI Networks Inc.

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:

United States KTI Networks Inc.
P.O. BOX 631008
Houston, Texas 77263-1008

Phone: 713-2663891
Fax: 713-2663893
E-mail: kti@ktinet.com
URL: http://www.ktinet.com/

International 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*

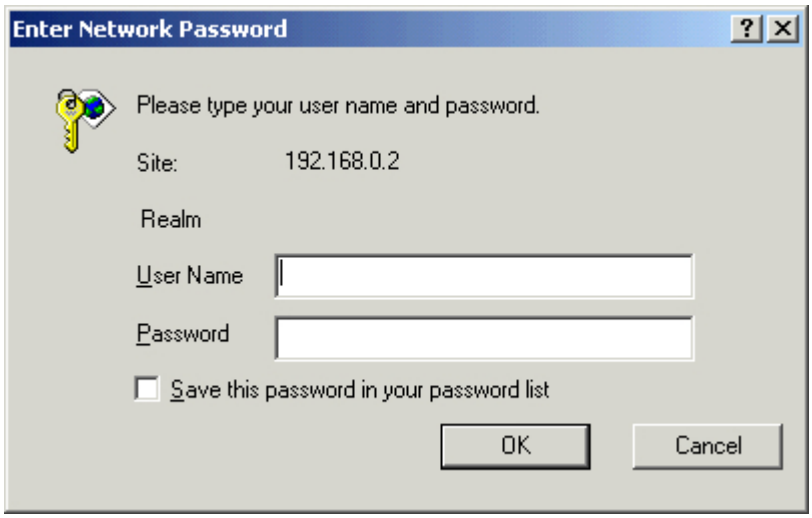
Factory default username: *admin*

Factory default password: ↵

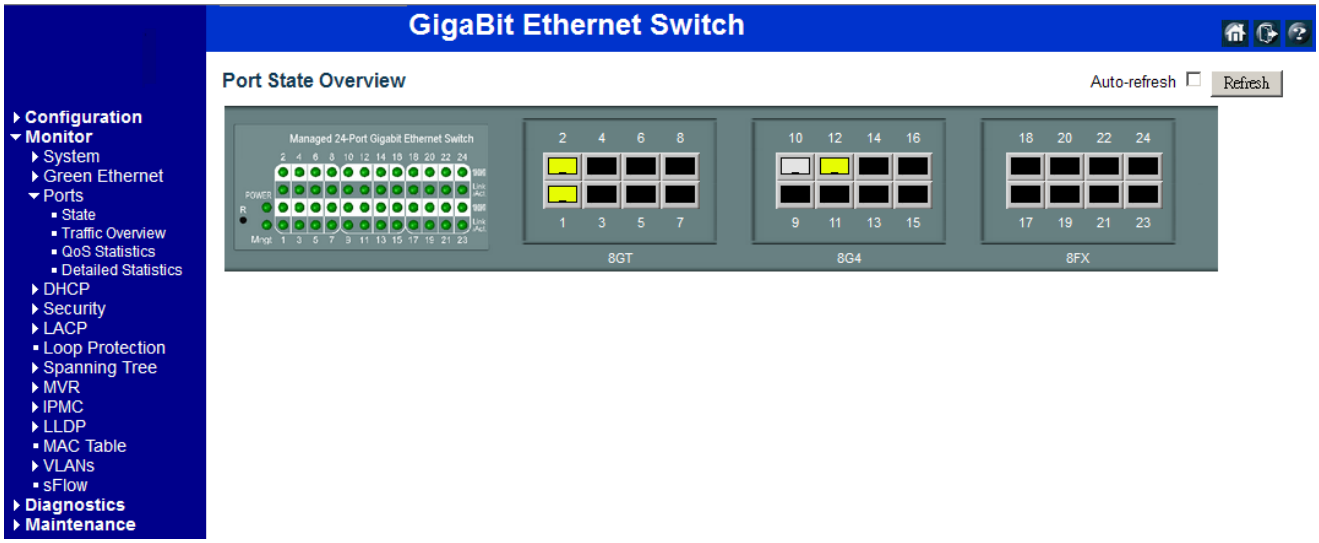
Note: no password with factory defaults

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.



[Home] [Logout] 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.

<<

Click to move to the top of the table.

Click to move to the last entry of the currently displayed table page.

Port state icons are:

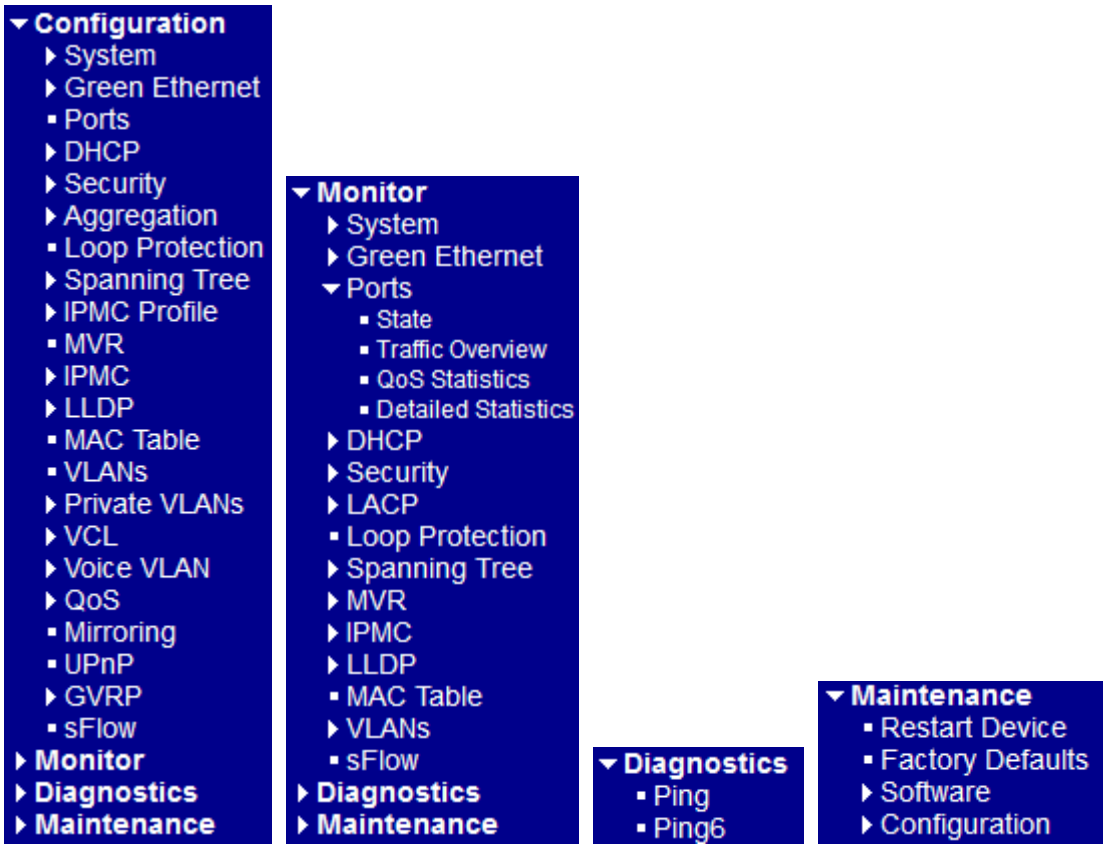
Status	Description
	Port disabled
	Port link down
	Port link up

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
Green Ethernet	
Ports	Port operation related configuration, frame size, and power saving control
DHCP	
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
IPMC Profile	IP Multicast Profile
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
VCL	Configuration for MAC-based, Protocol-based, and IP-based VLANs
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
GVRP	Configuration for GVRP (Generic VLAN Registration Protocol) feature
sFlow	sFlow is an industry standard technology for monitoring switched networks.

Monitor

System	Switch information, IP configuration, SNTP setting, and Password setting
Green Ethernet	
Ports	Port operation related configuration, frame size, and power saving control
DHCP	
Security	Switch & UI authentication configuration, Port access security control
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
sFlow	sFlow is an industry standard technology for monitoring switched networks.

Diagnostics

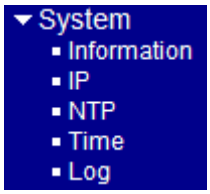
Ping	ICMP ping utility
Ping6	Ping utility for IPv6 devices

Maintenance

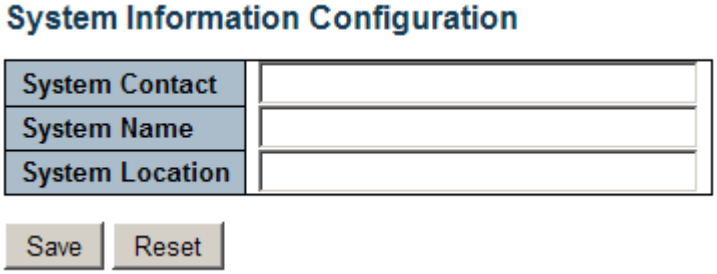
Restart Device	Command to reboot the switch
Factory Defaults	Command to restore the switch with factory default settings
Software	Command to update the switch firmware
Configuration	Command to save or upload the system configuration

2. Configuration

2.1 System



2.1.1 Information

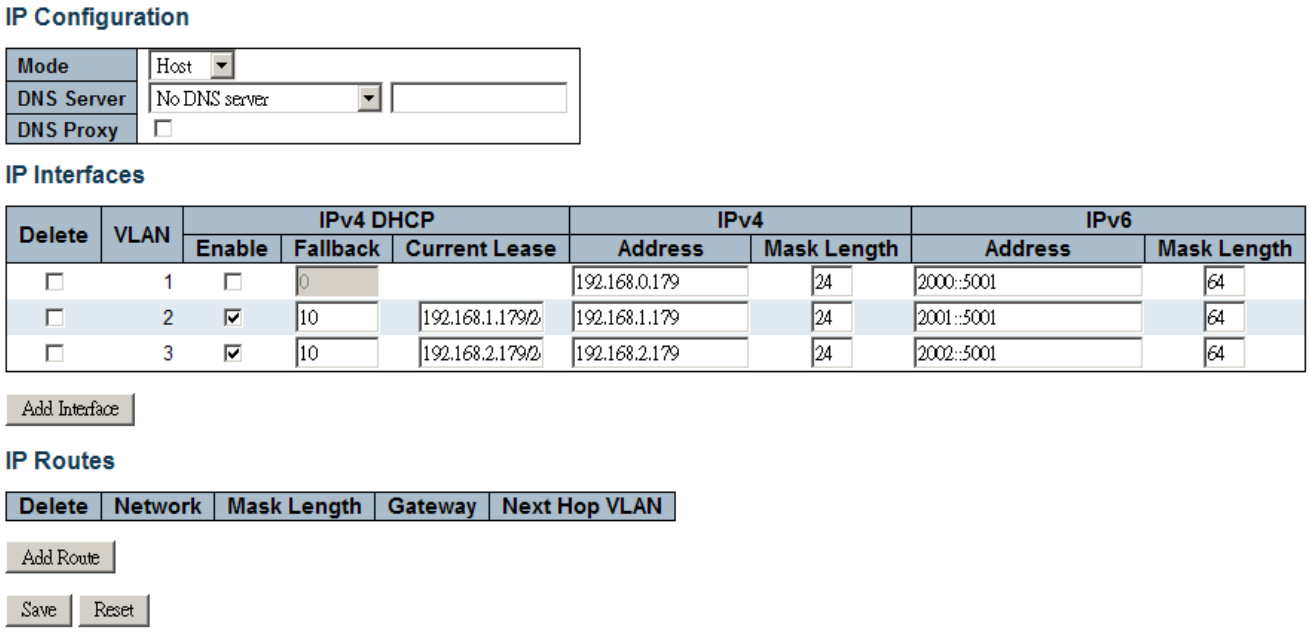


Configuration	Description
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is *0* to *255*, and the allowed content is the ASCII characters from *32* to *126*.
System Name	An administratively 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



IP Configuration	Description
Mode	Configure whether the IP stack should act as a *Host* or a *Router*. In *Host* mode, IP traffic between interfaces will not be routed. In *Router* mode traffic is routed between all interfaces.
DNS Server	This setting controls the DNS name resolution done by the switch. The following modes are supported: *From any DHCP interfaces:* The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used. *No DNS server:* No DNS server will be used. *Configured:* Explicitly provide the IP address of the DNS Server in dotted decimal notation. *From this DHCP interface:* Specify from which DHCP-enabled interface a provided DNS server should be preferred.
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.

IP Interfaces	Description
Delete	Select this option to delete an existing IP interface.
VLAN	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating an new interface.

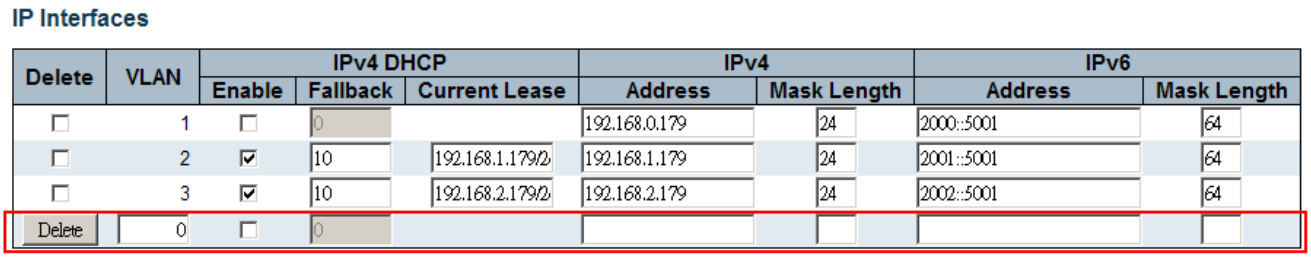
IPv4 DHCP	
Enable	Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
Fallback	The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.
Current Lease	For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.
IPv4 Address	The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
IPv4 Mask Length	The IPv4 network mask, in number of bits (*prefix length*). Valid values are between 0 and 30 bits for a IPv4 address. If *DHCP* is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
IPv6 Address	The IPv6 address of the interface. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol "::" is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address. The field may be left blank if IPv6 operation on the interface is not desired.
IPv6 Mask Length	The IPv6 network mask, in number of bits (*prefix length*). Valid values are between 1 and 128 bits for a IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.
Add Interface	Click to add a new IP interface. A maximum of 128 interfaces is supported.

IP Routers	**Description**
Delete	Select this option to delete an existing IP route.
Network	The destination IP network or host address of this route. Valid format is dotted decimal notationor a valid IPv6 notation. A default route can use the value 0.0.0.0or

	IPv6 : : notation.
Mask Length	The destination IP network or host mask, in number of bits (*prefix length*). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).
Gateway	The IP address of the IP gateway. Valid format is dotted decimal notationor a valid IPv6 notation. Gateway and Network must be of the same type.
Next Hop VLAN	The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway. If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.
Add Router	Click to add a new IP route. A maximum of 32 routes is supported.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.1.2.1 Add Interface

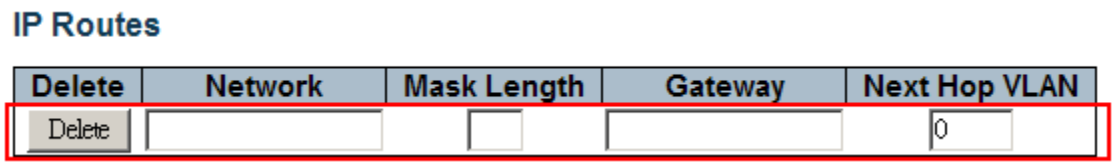
Click button.



Click Delete to cancel the added interface.

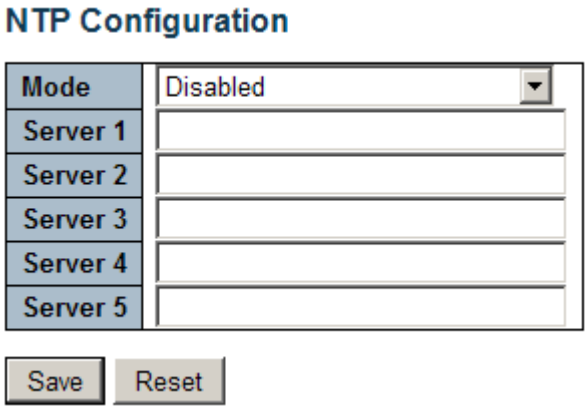
2.1.2.2 Add Router

Click button.



Click Delete to cancel the added router.

2.1.3 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.

2.1.4 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.

to add during Daylight Saving Time. (Range: 1 to

ıade locally and revert to previously saved values.

EEE Configuration

		EEE Urgent Queues							
Port	Enabled	1	2	3	4	5	6	7	8
*	☐	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐	☐

Save Reset

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

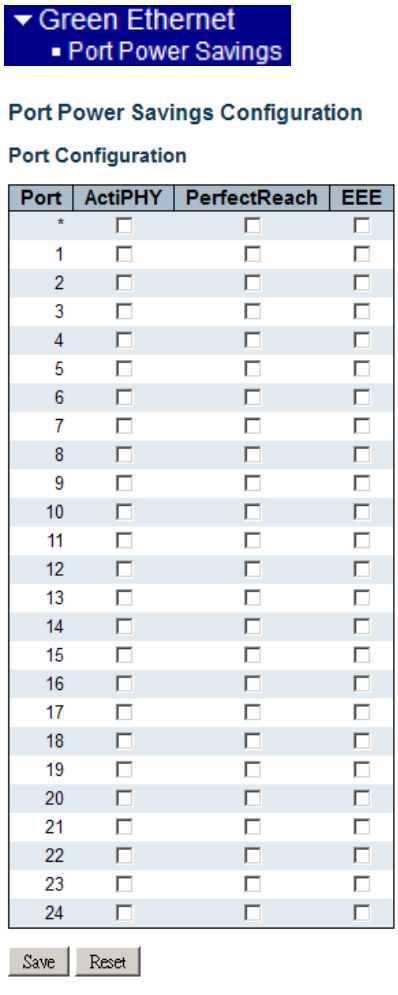
	also can be a host name.
Syslog Level	Indicates what kind of message will send to syslog server. Possible modes are: *Info*: Send information, warnings and errors. *Warning*: Send warnings and errors. *Error*: Send errors.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.2 Green Ethernet

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol. EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode.

For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for. When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.

2.2.1 Port Power Saving



Configuration	Description
Port	The switch port number of the logical EEE port.
ActiPHY	Link down power savings enabled. ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted.
PerfectReach	Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables.
EEE	Controls whether EEE is enabled for this switch port.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3 Ports

Port Configuration Refresh

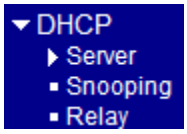
Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*						☐		<>
1	●	100fdx	Auto	✗	✗	☐	10056	Discard
2	●	1Gfdx	Auto	✗	✗	☐	10056	Discard
3	●	Down	Auto	✗	✗	☐	10056	Discard
4	●	Down	Auto	✗	✗	☐	10056	Discard
5	●	Down	Auto	✗	✗	☐	10056	Discard
6	●	Down	1Gbps FDX	✗	✗	☐	10056	Discard
7	●	Down	100Mbps FDX	✗	✗	☐	10056	Discard
8	●	Down	10Mbps FDX	✗	✗	☐	10056	Discard
9	●	Down	Auto	✗	✗	☐	10056	Discard
10	●	Down	Disabled	✗	✗	☐	10056	
11	●	Down	Auto	✗	✗	☐	10056	Discard
12	●	1Gfdx Fiber	1000-X Auto	✗	✗	☐	10056	
13	●	Down	Auto	✗	✗	☐	10056	Discard
14	●	Down	100-FX	✗	✗	☐	10056	
15	●	Down	Auto	✗	✗	☐	10056	Discard
16	●	Down	1000-X	✗	✗	☐	10056	
17	●	Down	100-FX	✗	✗	☐	10056	
18	●	Down	100-FX	✗	✗	☐	10056	
19	●	Down	100-FX	✗	✗	☐	10056	
20	●	Down	100-FX	✗	✗	☐	10056	
21	●	Down	100-FX	✗	✗	☐	10056	
22	●	Down	100-FX	✗	✗	☐	10056	
23	●	Down	100-FX	✗	✗	☐	10056	
24	●	Down	100-FX	✗	✗	☐	10056	

Save Reset

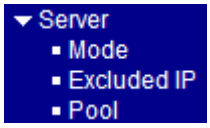
Configuration	Description
Port	The port number associated to this configuration row
Link	The current link status is displayed graphically. Green indicates the link is up and red that it is down.
Speed - Current	Provide the current link speed of the port.
Speed - Configured	Select any available link speed for the given switch port. **Options for 10/100/1000M Copper port type:** *Disabled*: disables the switch port operation. *Auto*: selects the highest speed that is compatible with the link partner. *1Gbps FDX*: Auto-negotiation 1000Mbps and full duplex *100Mbps FDX*: Fixed 100Mbps and full duplex *100Mbps HDX*: Fixed 100Mbps and half duplex *10Mbps FDX*: Fixed 10Mbps and full duplex

	10Mbps HDX: Fixed 10Mbps and half duplex **Options for 100/1000M SFP port type:** *Disabled*: disables the switch port operation. *1000-X Auto*: Auto-negotiation, 1000M and full duplex *1000-X*: Fixed 1000M and full duplex *100-FX*: Fixed 100Mbps and full duplex **Options for Fixed 100M Fiber port type (ST, SC, BiDi, VF-45):** *Disabled*: disables the switch port operation. *100-FX*: Fixed 100Mbps 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 *10056* bytes.
Excessive Collision Mode	Configure port transmission collision behavior. *Discard*: Discard frame after 16 collisions (default). *Restart*: Restart back-off algorithm after 16 collisions.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

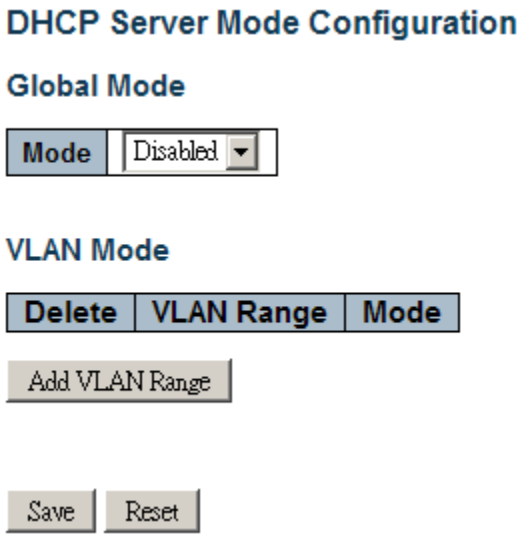
2.4 DHCP



2.4.1 Server



2.4.1.1 Mode

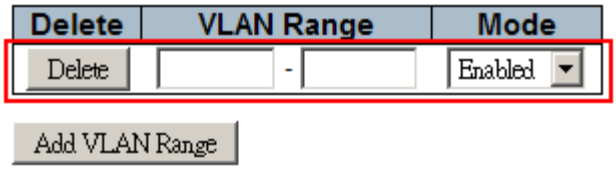


Configuration	Description
Mode	Configure the operation mode per system. Possible modes are: *Enabled:* Enable DHCP server per system. *Disabled:* Disable DHCP server per system.
Delete	Check to delete the entry.
VLAN Range	Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both. On the other hand, if you want to disable existed VLAN range, then you can follow the steps. 1. press to add a new VLAN range. 2. input the VLAN range that you want to disable. 3. choose Mode to be Disabled.

	4. press to apply the change. Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.
Mode	Indicate the the operation mode per VLAN. Possible modes are: *Enabled:* Enable DHCP server per VLAN. *Disabled:* Disable DHCP server pre VLAN.

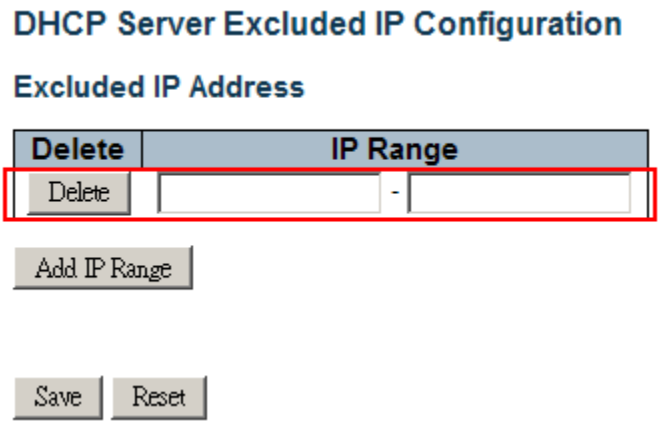
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click Add VLAN Range to add a VLAN Range entry.



2.4.1.2 Excluded IP

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



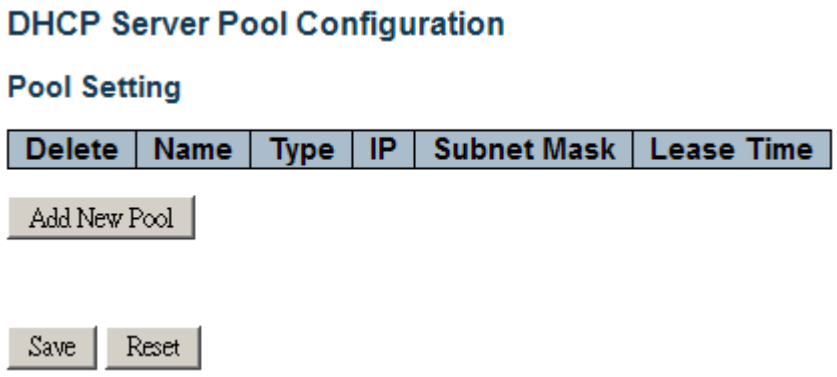
Configuration	**Description**
Delete	Check to delete the entry.
IP Range	Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first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

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

Click Add IP Range to add an IP Range entry.

2.4.1.3 Pool

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



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

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

Click Add New Pool to add a Pool entry.

Pool Setting

Delete	Name	Type	IP	Subnet Mask	Lease Time
Delete		-	-	-	1 days 0 hours 0 minutes

Add New Pool

2.4.2 Snooping

DHCP Snooping Configuration

Snooping Mode	Disabled

Port Mode Configuration

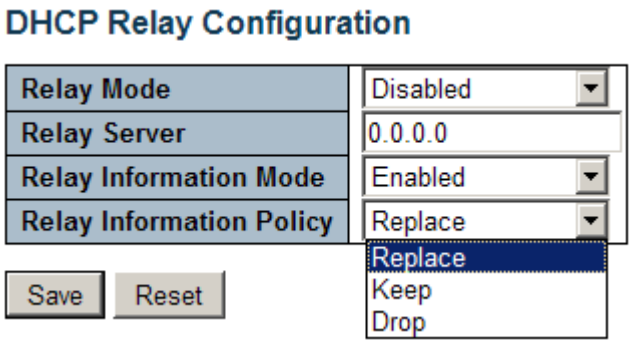
Port	Mode
*	<>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted
9	Trusted
10	Trusted

Save Reset

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.

2.4.3 Relay

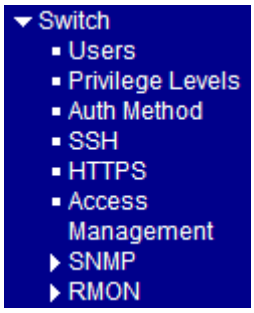


Configuration	Description
Relay Mode	Indicates the DHCP relay mode operation. Possible modes are: ***Enabled:*** Enable DHCP relay mode operation. When enable DHCP relay mode operation, the agent forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet 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

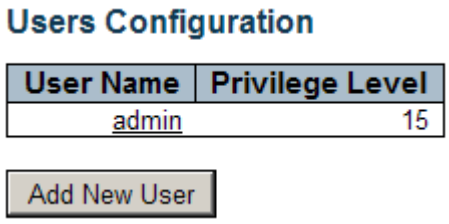
	relay information operation mode enabled. Possible policies are: ***Replace:*** Replace the original relay information when receive a DHCP message that already contains it. ***Keep:*** Keep the original relay information when receive a DHCP message that already contains it. ***Drop:*** Drop the package 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 Security

2.5.1 Switch

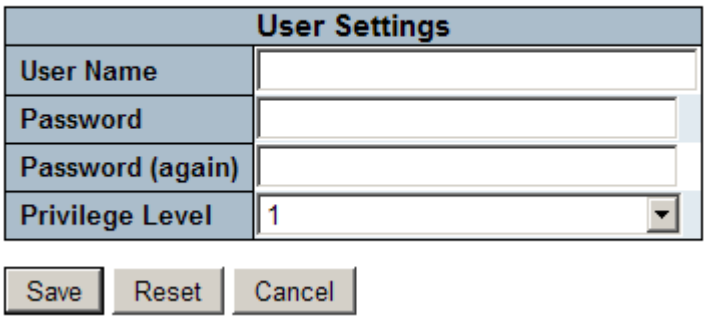


2.5.1.1 Users



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

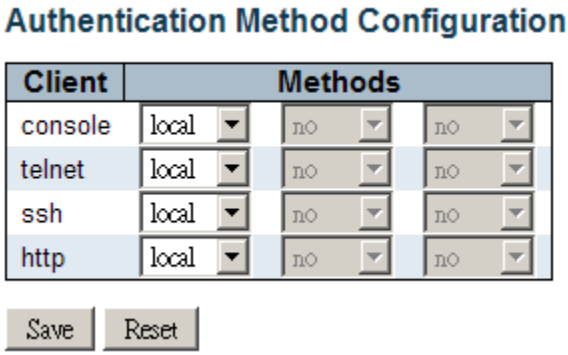
Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
DHCP	5	10	5	10
Dhcp_Client	5	10	5	10
Diagnostics	5	10	5	10
EEE	5	10	5	10
Green_Ethernet	5	10	5	10
IP2	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
Mirroring	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
RPC	5	10	5	10
Security	5	10	5	10
sFlow	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
XXRP	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.

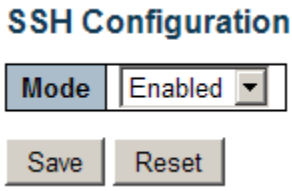
2.5.1.3 Auth Method



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.
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. Methods that involve remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

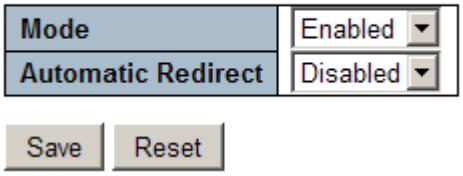
2.5.1.4 SSH



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.

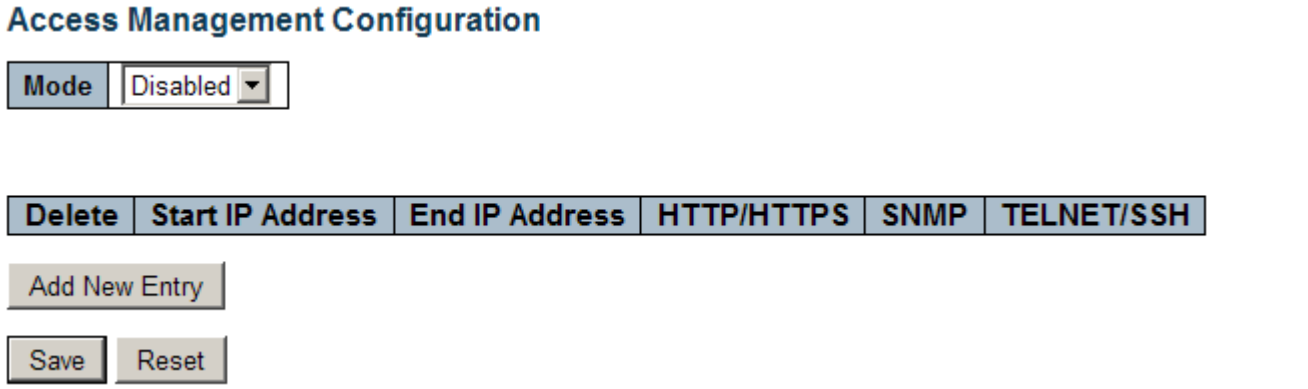
2.5.1.5 HTTPS

HTTPS Configuration

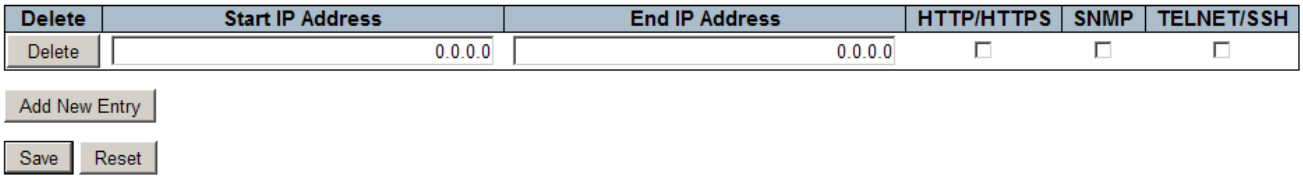


Configuration	Description
Mode	Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are: *Enabled*: Enable HTTPS mode operation. *Disabled*: Disable HTTPS mode operation.
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

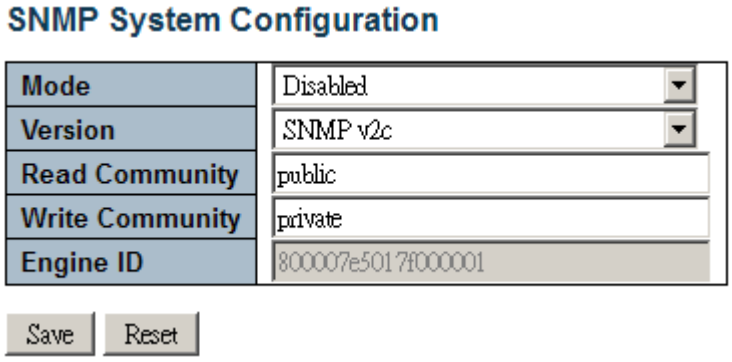


Configure access management table on this page. The maximum number of entries is 16. If the application's type match any one of the access management entries, it will allow access to the switch.

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



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.

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

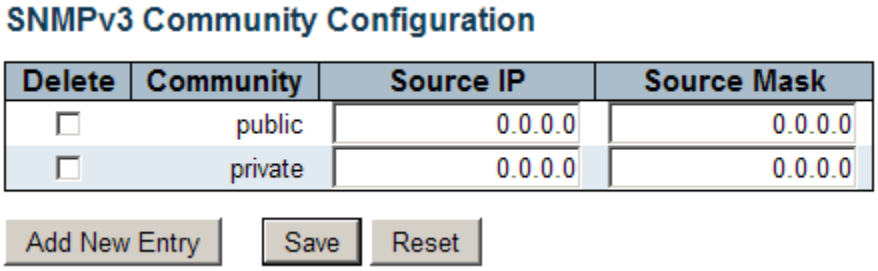
2.5.1.7.2 Traps

Trap Configuration	**Description**
Global Mode	Indicates the SNMP trap mode operation. Possible modes are: ***Enabled:*** Enable SNMP trap mode operation. ***Disabled:*** Disable SNMP trap mode operation.
Delete	Check to delete a trap server entry.
Name	Indicates the trap Configuration's name.
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.
Destination Address	Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allow a valid hostname. A valid hostname is

	a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
Destination Port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

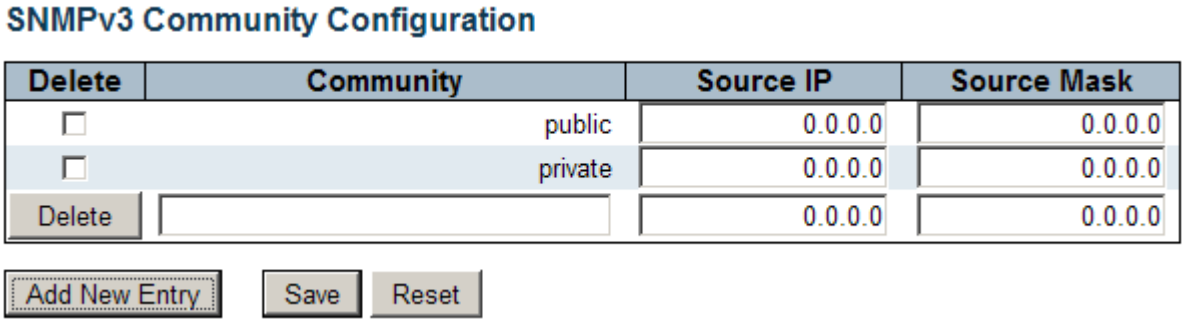
Add New Entry	Click to add en entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.5.1.7.3 Communities



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:



2.5.1.7.4 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	

2.5.1.7.5 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

2.5.1.7.6 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

2.5.1.7.7 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.

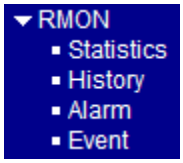
Click Add New Entry:

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

RMON Statistics Configuration

Delete	ID	Data Source

Add New Entry Save Reset

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:

RMON Statistics Configuration

Delete	ID	Data Source
Delete		.1.3.6.1.2.1.2.2.1.1. 0

Add New Entry Save Reset

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:

RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index
Delete		30	.1.3.6.1.2.1.2.2.1.0.0	Delta	0	RisingOrFalling	0	0

Add New Entry Save Reset

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.

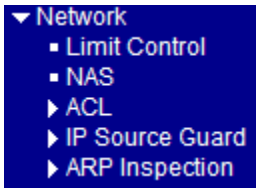
Click Add New Entry:

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

Port Security Limit Control Configuration

System Configuration

Mode	Disabled
Aging Enabled	☐
Aging Period	3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<>		<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen
13	Disabled	4	None	Disabled	Reopen
14	Disabled	4	None	Disabled	Reopen
15	Disabled	4	None	Disabled	Reopen
16	Disabled	4	None	Disabled	Reopen
17	Disabled	4	None	Disabled	Reopen
18	Disabled	4	None	Disabled	Reopen
19	Disabled	4	None	Disabled	Reopen
20	Disabled	4	None	Disabled	Reopen
21	Disabled	4	None	Disabled	Reopen
22	Disabled	4	None	Disabled	Reopen
23	Disabled	4	None	Disabled	Reopen
24	Disabled	4	None	Disabled	Reopen

Save Reset

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*.
Re-open	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
7	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
11	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
12	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
13	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
14	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
15	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
16	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
17	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
18	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
19	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
20	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
21	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
22	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
23	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
24	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.

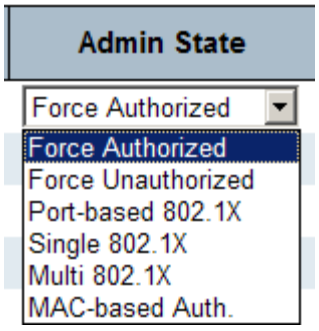
RADIUS-Assigned VLAN Enabled

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.

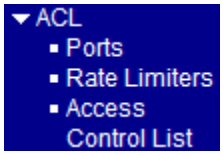
Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

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

ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Logging	Shutdown	State	Counter
*		<>	<>	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
11	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
12	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	34053
13	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
14	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
15	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
16	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
17	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
18	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
19	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
20	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
21	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
22	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
23	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
24	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0

Save Reset

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

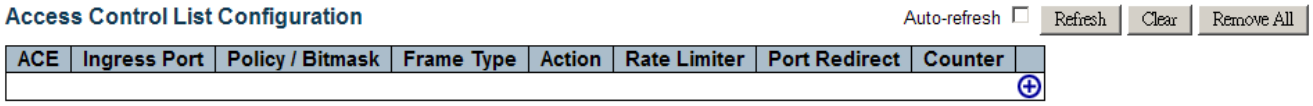
ACL Rate Limiter Configuration

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

Save Reset

Configuration	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate (pps)	The rate range is located 0-131071 in pps.
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



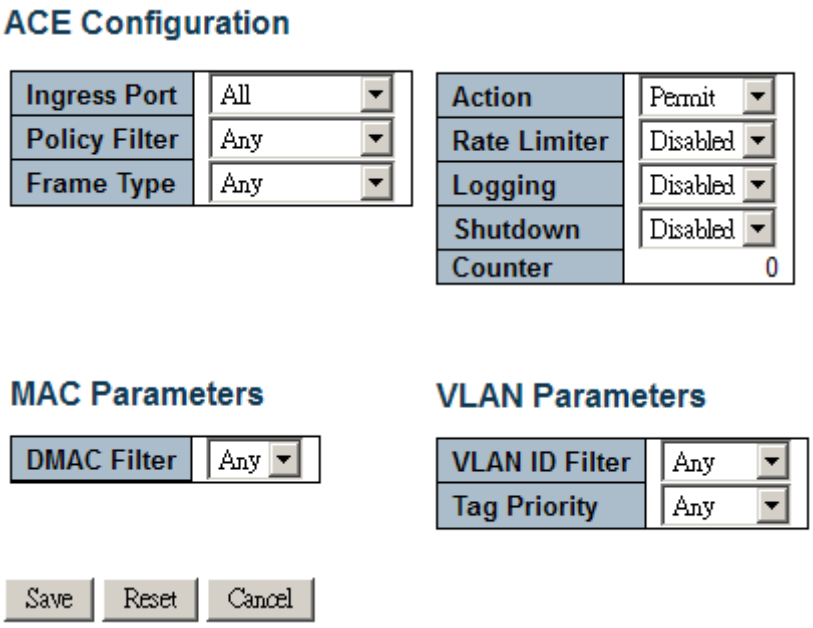
Configuration	Description
ACE	ACE ID
Ingress Port	Indicates the ingress port of the ACE. Possible values are: *All*: The ACE will match all ingress port. *Port*: The ACE will match a specific ingress port.
Policy/Bitmask	Indicates the policy number and bitmask of the ACE.
Frame Type	Indicates the frame 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:



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 Filter	Specify the policy number filter for this ACE. *Any:* No policy filter is specified. (policy filter status is "don't-care".) *Specific*: If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.
Frame Type	Indicates the frame type of the ACE.
Action	Indicates the forwarding action of the ACE.

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.
Logging	Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are: *Enabled*: Frames matching the ACE are stored in the System Log. *Disabled*: Frames matching the ACE are not logged. Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of the ACE. The allowed values are: *Enabled*: If a frame matches the ACE, the ingress port will be disabled. *Disabled*: Port shut down is disabled for the ACE. Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).
Counter	The counter indicates the number of times the ACE was hit by a frame.
SMAC Filter	(Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE. *Any*: No SMAC filter is specified. (SMAC filter status is "don't-care".) *Specific*: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.
SMAC Value	When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.
DMAC Filter	Specify the destination MAC filter for this ACE. Any: No DMAC filter is specified. (DMAC filter status is "don't-care".) *MC*: Frame must be multicast. *BC*: Frame must be broadcast. *UC*: Frame must be unicast. *Specific*: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.
DMAC Value	When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.
VLAN ID Filter	Specify the VLAN ID filter for this ACE. *Any*: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)

	Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.
VLAN ID	When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
Tag Priority	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

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.

ARP Parameters

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

ARP/RARP	Specify the available ARP/RARP opcode (OP) flag for this ACE. *Any*: No ARP/RARP OP flag is specified. (OP is "don't-care".) *ARP*: Frame must have ARP opcode set to ARP. *RARP*: Frame must have RARP opcode set to RARP. Other: Frame has unknown ARP/RARP Opcode flag.
Request/Reply	Specify the available Request/Reply opcode (OP) flag for this ACE. *Any*: No Request/Reply OP flag is specified. (OP is "don't-care".) *Request*: Frame must have ARP Request or RARP Request OP flag set. *Reply*: Frame must have ARP Reply or RARP Reply OP flag.
Sender IP Filter	Specify the sender IP filter for this ACE. *Any*: No sender IP filter is specified. (Sender IP filter is "don't-care".) *Host*: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears. Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.
Sender IP Address	When "*Host*" or "*Network*" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.
Sender IP Mask	When "*Network*" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
Target IP Filter	Specify the target IP filter for this specific ACE.

	Any: No target IP filter is specified. (Target IP filter is "don't-care".) *Host*: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.
Target IP Address	When "*Host*" or "*Network*" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.
Target IP Mask	When "*Network*" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
ARP Sender MAC Match	
	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. *0*: ARP frames where SHA is not equal to the SMAC address. *1*: ARP frames where SHA is equal to the SMAC address. *Any*: Any value is allowed ("don't-care").
RARP Target MAC Match	
	Specify whether frames can hit the action according to their target hardware address field (THA) settings. 0: RARP frames where THA is not equal to the target MAC address. *1*: RARP frames where THA is equal to the target MAC address. *Any*: Any value is allowed ("don't-care").
IP/Ethernet Length	Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings. *0*: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04). *1*: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04). *Any*: Any value is allowed ("don't-care").
IP	Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings. *0*: ARP/RARP frames where the HLD is not equal to Ethernet (1). *1*: ARP/RARP frames where the HLD is equal to Ethernet (1). *Any*: Any value is allowed ("don't-care").
Ethernet	Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

0: ARP/RARP frames where the PRO is not equal to IP (0x800).

1: ARP/RARP frames where the PRO is equal to IP (0x800).

Any: Any value is allowed ("don't-care").

IP Parameters

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

IP Protocol Filter	Specify the IP protocol filter for this ACE. *Any*: No IP protocol filter is specified ("don't-care"). *Specific*: If you want to filter a specific IP protocol filter with this ACE, choose this *value*. A field for entering an IP protocol filter appears. ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file. UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file. TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.
IP Protocol Value	When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.
IP TTL	Specify the Time-to-Live settings for this ACE. *zero*: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry. *non-zero*: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry. *Any*: Any value is allowed ("don't-care").
IP Fragment	Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. *No*: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. *Yes*: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. *Any*: Any value is allowed ("don't-care").
IP Option	Specify the options flag setting for this ACE. *No*: IPv4 frames where the options flag is set must not be able to match this entry. *Yes*: IPv4 frames where the options flag is set must be able to match this entry. *Any*: Any value is allowed ("don't-care").
SIP Filter	Specify the source IP filter for this ACE.

	Any: No source IP filter is specified. (Source IP filter is "don't-care".) *Host*: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears. *Network*: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.
SIP Address	When "*Host*" or "*Network*" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.
SIP Mask	When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
DIP Filter	Specify the destination IP filter for this ACE. *Any*: No destination IP filter is specified. (Destination IP filter is "don't-care".) *Host*: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. *Network*: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.
DIP Address	When "*Host*" or "*Network*" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.
DIP Mask	When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

IPv6 Parameters

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

Next Header Filter	Specify the IPv6 next header filter for this ACE. *Any*: No IPv6 next header filter is specified ("don't-care"). *Specific*: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears. *ICMP*: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file. *UDP*: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file. *TCP*: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.
Next Header Value	When "*Specific*" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IPv6

	protocol value.
SIP Filter	Specify the source IPv6 filter for this ACE. *Any*: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".) *Specific*: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.
SIP Address	When "*Specific*" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.
SIP BitMask	When "*Specific*" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.
Hop Limit	Specify the hop limit settings for this ACE. *zero*: IPv6 frames with a hop limit field greater than zero must not be able to match this entry. *non-zero*: IPv6 frames with a hop limit field greater than zero must be able to match this entry. *Any*: Any value is allowed ("don't-care").
ICMP Parameters	
ICMP Type Filter	Specify the ICMP filter for this ACE. *Any*: No ICMP filter is specified (ICMP filter status is "don't-care"). *Specific*: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.
ICMP Type Value	When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.
ICMP Code Filter	Specify the ICMP code filter for this ACE. *Any*: No ICMP code filter is specified (ICMP code filter status is "don't-care"). *Specific*: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.
ICMP Code Value	When "*Specific*" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.
TCP/UDP Parameters	
TCP/UDP Source Filter	Specify the TCP/UDP source filter for this ACE. *Any*: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").

Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.

Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

TCP/UDP Source No. When "*Specific*" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Source Range

When "*Range*" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Destination Filter

Specify the TCP/UDP destination filter for this ACE.

Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").

Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.

Range: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

TCP/UDP Destination Number

When "*Specific*" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP/UDP Destination Range

When "*Range*" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

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

0: TCP frames where the FIN field is set must not be able to match this entry.

1: TCP frames where the FIN field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

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

0: TCP frames where the SYN field is set must not be able to match this entry.

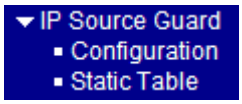
	1: TCP frames where the SYN field is set must be able to match this entry.
	Any: Any value is allowed ("don't-care").
TCP RST	Specify the TCP "Reset the connection" (RST) value for this ACE.
	0: TCP frames where the RST field is set must not be able to match this entry.
	1: TCP frames where the RST field is set must be able to match this entry.
	Any: Any value is allowed ("don't-care").
TCP PSH	Specify the TCP "Push Function" (PSH) value for this ACE.
	0: TCP frames where the PSH field is set must not be able to match this entry.
	1: TCP frames where the PSH field is set must be able to match this entry.
	Any: Any value is allowed ("don't-care").
TCP ACK	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.
	0: TCP frames where the ACK field is set must not be able to match this entry.
	1: TCP frames where the ACK field is set must be able to match this entry.
	Any: Any value is allowed ("don't-care").
TCP URG	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.
	0: TCP frames where the URG field is set must not be able to match this entry.
	1: TCP frames where the URG field is set must be able to match this entry.
	Any: Any value is allowed ("don't-care").

Ethernet Type Parameters

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

EtherType Filter	Specify the Ethernet type filter for this ACE.
	Any: No EtherType filter is specified (EtherType filter status is "don't-care").
	Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.
Ethernet Type Value	When "*Specific*" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

2.5.2.4 IP Source Guard



2.5.2.4.1 Configuration

IP Source Guard Configuration

Mode	Disabled

Translate dynamic to static

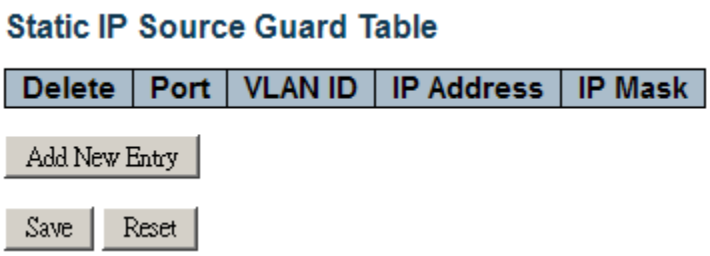
Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9	Disabled	Unlimited
10	Disabled	Unlimited
11	Disabled	Unlimited
12	Disabled	Unlimited
13	Disabled	Unlimited
14	Disabled	Unlimited
15	Disabled	Unlimited
16	Disabled	Unlimited
17	Disabled	Unlimited
18	Disabled	Unlimited
19	Disabled	Unlimited
20	Disabled	Unlimited
21	Disabled	Unlimited
22	Disabled	Unlimited
23	Disabled	Unlimited
24	Disabled	Unlimited

Save | Reset

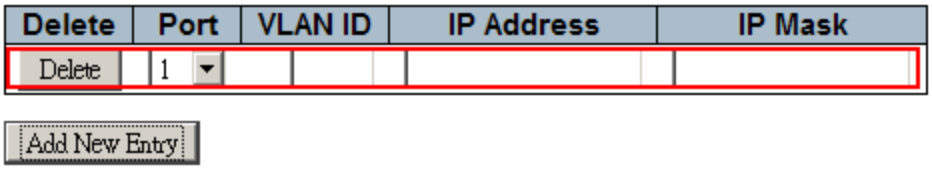
Configuration	Description
Mode of IP Source Guard Configuration	
	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
Port Mode Configuration	Specify IP Source Guard is enabled on which ports. Only when both Global Mode and 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.

2.5.2.4.2 Static Table

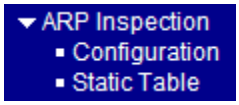


Configuration	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings
VLAN ID	The VLAN ID for the settings
IP Address	Allowed Source IP address
Add New Entry	Click to add a new entry to the Static IP Source Guard table.
Save	Click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

Click Add New Entry:


Delete
Port
VLAN ID
IP Address
IP Mask
Delete
1
Add New Entry

2.5.2.5 ARP Inspection



2.5.2.5.1 Port Configuration

ARP Inspection Configuration

Mode	Disabled

Translate dynamic to static

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None
7	Disabled	Disabled	None
8	Disabled	Disabled	None
9	Disabled	Disabled	None
10	Disabled	Disabled	None
11	Disabled	Disabled	None
12	Disabled	Disabled	None
13	Disabled	Disabled	None
14	Disabled	Disabled	None
15	Disabled	Disabled	None
16	Disabled	Disabled	None
17	Disabled	Disabled	None
18	Disabled	Disabled	None
19	Disabled	Disabled	None
20	Disabled	Disabled	None
21	Disabled	Disabled	None
22	Disabled	Disabled	None
23	Disabled	Disabled	None
24	Disabled	Disabled	None

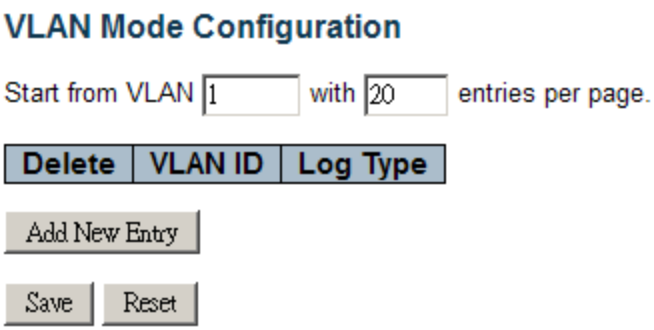
Save Reset

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

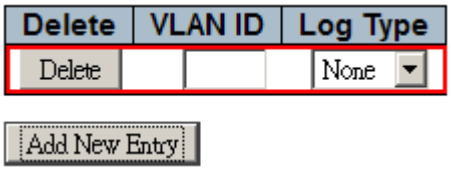
Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

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

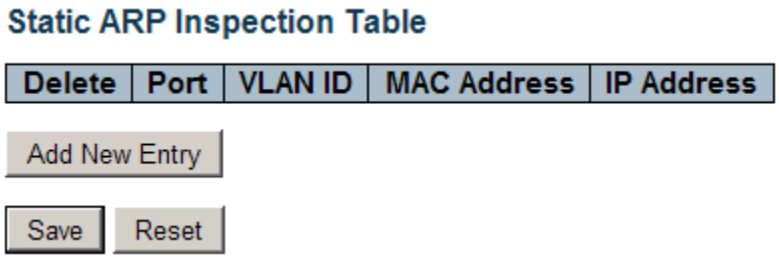


Configuration	Description
Delete	Check to delete the entry.
VLAN ID	Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.
Log Type	Possible types are: *None*: Log nothing. *Deny*: Log denied entries. *Permit*: Log permitted entries. *ALL*: Log all entries.
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 button to add a new entry.

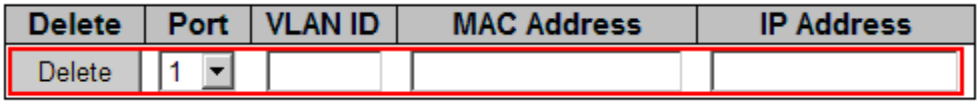


2.5.2.5.3 Static Table



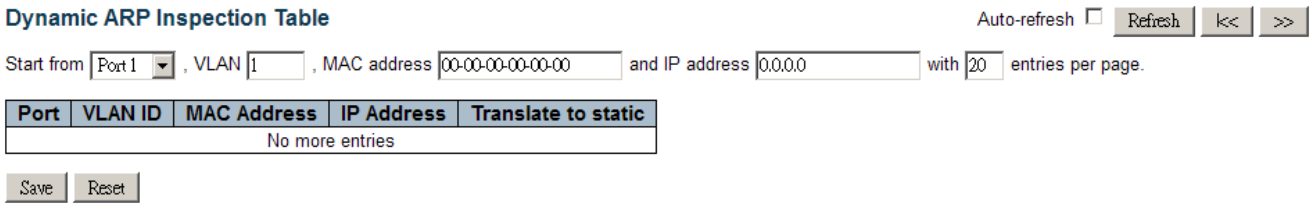
Configuration	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings
VLAN ID	The VLAN ID for the settings
MAC Address	Allowed MAC address
IP Address	Allowed Source IP address
Add new entry	Click to add a new entry.
Save	Click to save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

Click Add New Entry:



2.5.2.5.4 Dynamic Table

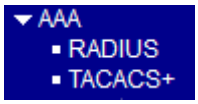
Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.



Configuration	Description
Port	Switch Port Number for which the entries are displayed.
VLAN ID	VLAN ID in which the ARP traffic is permitted.
MAC Address	User MAC address of the entry.
IP Address	User IP address of the entry.
Translate to static	Select the checkbox to translate the entry to static entry.
Save	Click to save the changes.

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

2.5.3 AAA



2.5.3.1 RADIUS

RADIUS Server Configuration

Global Configuration

Timeout	5 seconds
Retransmit	3 times
Deadtime	0 minutes
Key	
NAS-IP-Address	
NAS-IPv6-Address	
NAS-Identifier	

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key

Add New Server

Save Reset

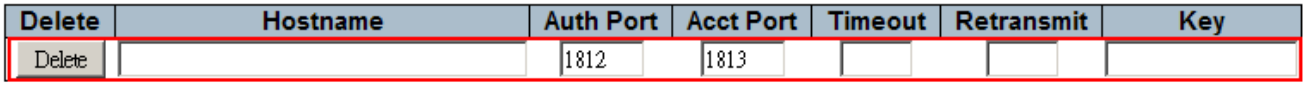
Global Configuration	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
Retransmit	Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.
Deadtime	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Key	The secret key - up to 63 characters long - shared between the RADIUS server and the switch.
NAS-IP-Address	The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this

	field is left blank, the IP address of the outgoing interface is used.
NAS-IPv6-Address	The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
NAS-Identifier	The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

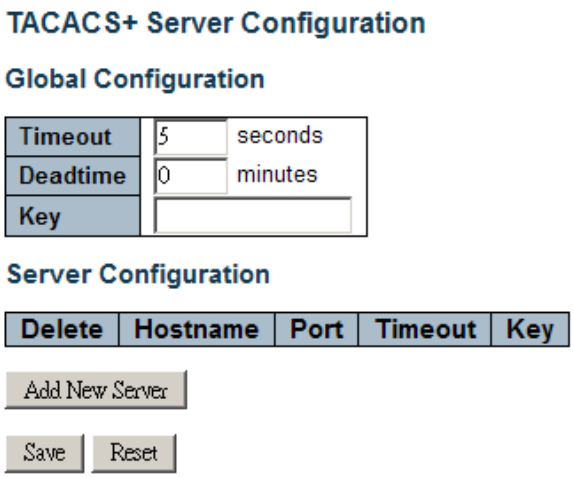
Server Entry	**Description**
Delete	To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IP address or hostname of the RADIUS server.
Auth Port	The UDP port to use on the RADIUS server for authentication.
Acct Port	The UDP port to use on the RADIUS server for accounting.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Retransmit	This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.

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:



2.5.3.2 TACACS+



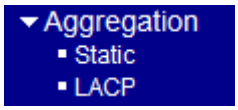
Global Configuration	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.
Deadtime	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Key	The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Entry	Description
Delete	To delete a server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IP address or hostname of the server.
Port	The TCP port to use on the TACACS+ server for authentication.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.

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.

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

Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	☐
IP Address	☑
TCP/UDP Port Number	☑

Aggregation Group Configuration

	Port Members																							
Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Normal	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
9	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
10	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
11	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
12	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Save Reset

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
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768
9	☐	Auto		Active	Fast	32768
10	☐	Auto		Active	Fast	32768
11	☐	Auto		Active	Fast	32768
12	☐	Auto		Active	Fast	32768
13	☐	Auto		Active	Fast	32768
14	☐	Auto		Active	Fast	32768
15	☐	Auto		Active	Fast	32768
16	☐	Auto		Active	Fast	32768
17	☐	Auto		Active	Fast	32768
18	☐	Auto		Active	Fast	32768
19	☐	Auto		Active	Fast	32768
20	☐	Auto		Active	Fast	32768
21	☐	Auto		Active	Fast	32768
22	☐	Auto		Active	Fast	32768
23	☐	Auto		Active	Fast	32768
24	☐	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

Loop Protection Configuration

General Settings

Global Configuration		
Enable Loop Protection	Disable	
Transmission Time	5	seconds
Shutdown Time	180	seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	☐	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable
7	☑	Shutdown Port	Enable
8	☑	Shutdown Port	Enable
9	☑	Shutdown Port	Enable
10	☑	Shutdown Port	Enable
11	☑	Shutdown Port	Enable
12	☑	Shutdown Port	Enable
13	☑	Shutdown Port	Enable
14	☑	Shutdown Port	Enable
15	☑	Shutdown Port	Enable
16	☑	Shutdown Port	Enable
17	☑	Shutdown Port	Enable
18	☑	Shutdown Port	Enable
19	☑	Shutdown Port	Enable
20	☑	Shutdown Port	Enable
21	☑	Shutdown Port	Enable
22	☑	Shutdown Port	Enable
23	☑	Shutdown Port	Enable
24	☑	Shutdown Port	Enable

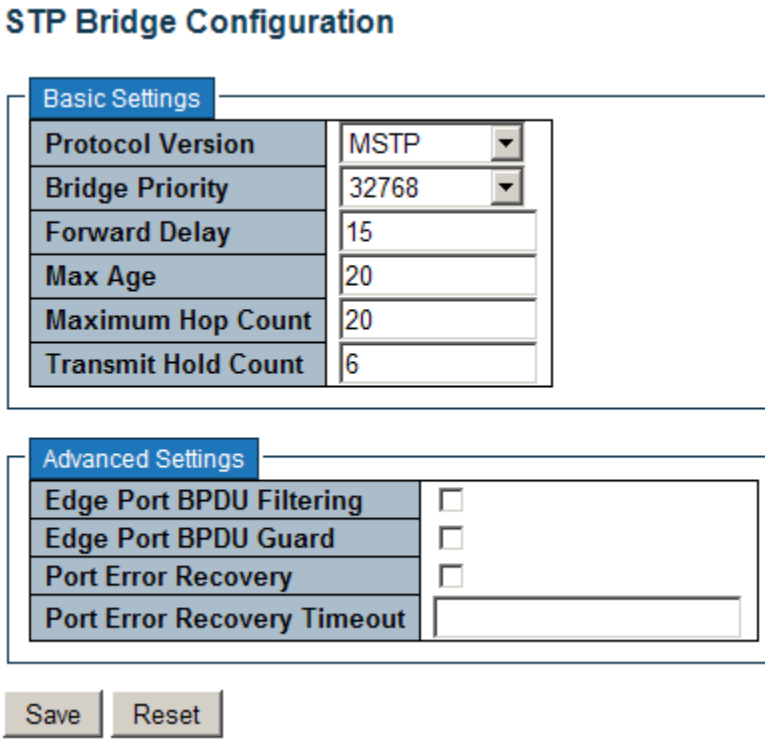
Save Reset

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).

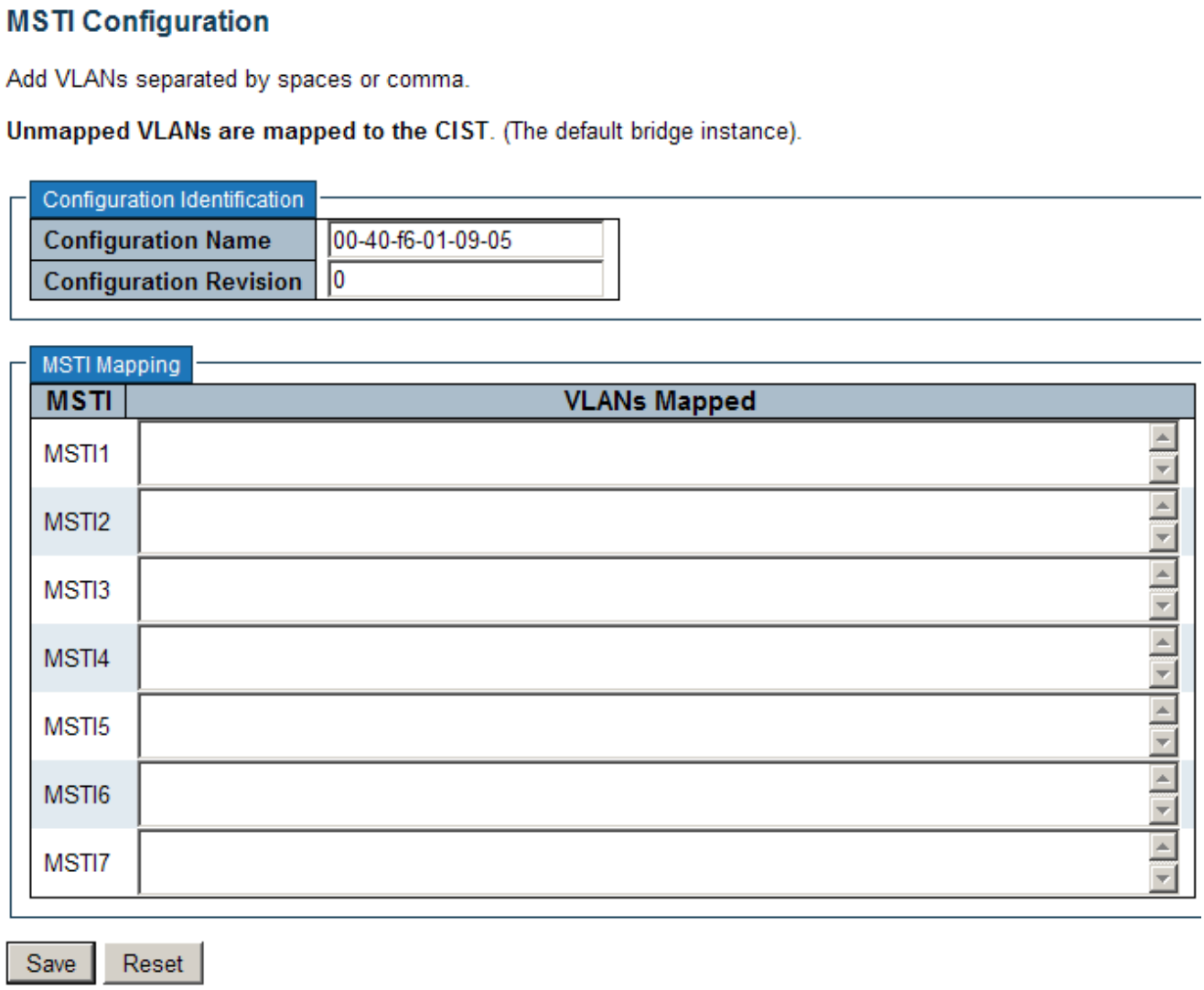
	Valid values: *4 ~ 30 seconds*
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge Valid values: *6 ~ 40 seconds (Max Age must be <= (FwdDelay-1)*2)*
Maximum Hop Count	It defines how many bridges a root bridge can distribute its BPDU information. This defines 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.

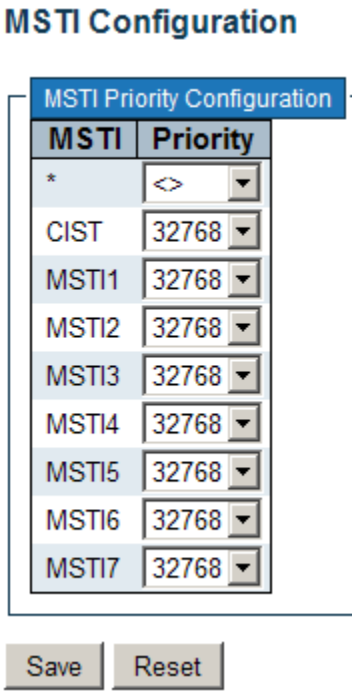
2.8.2 MSTI Mapping



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

STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
-	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
*	☐	<>	<>	<>	☐	☐	☐	☐	<>
1	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
2	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
3	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
4	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
5	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
6	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
7	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
8	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
9	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
10	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
11	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
12	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
13	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
14	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
15	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
16	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
17	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
18	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
19	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
20	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
21	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
22	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
23	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
24	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto

Save Reset

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

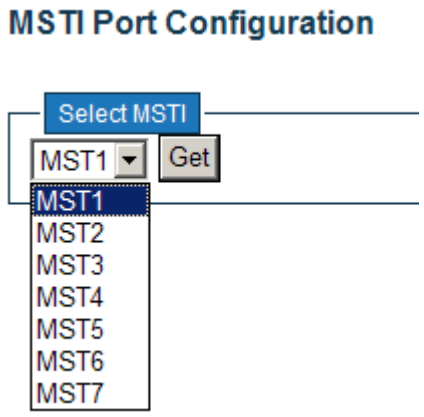
	establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values: *1 to 200000000*
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
AdminEdge	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.

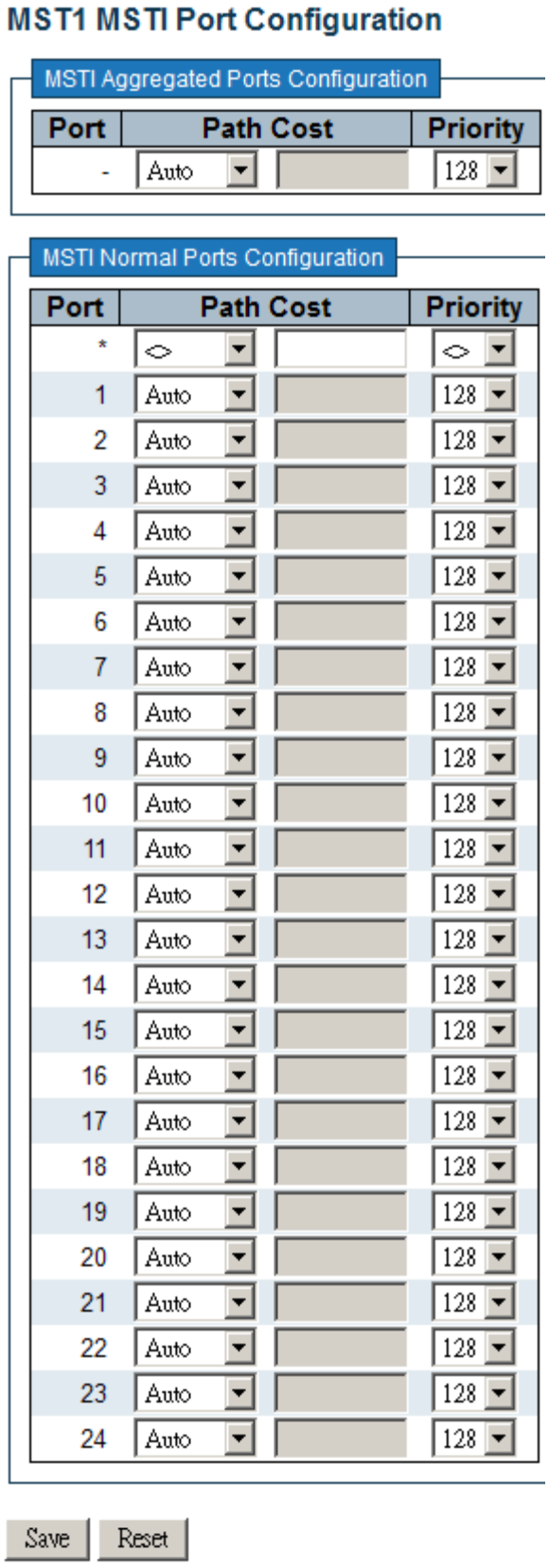
2.8.5 MSTI Ports

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 :

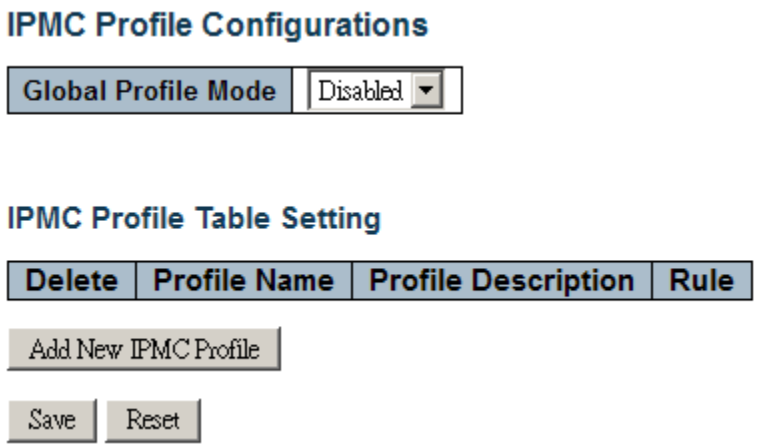

MST1 MSTI Port Configuration
MSTI Aggregated Ports Configuration
Port
Path Cost
Priority
-
Auto
128
MSTI Normal Ports Configuration
Port
Path Cost
Priority
*
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
Save
Reset

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 IPMC Profile

The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.

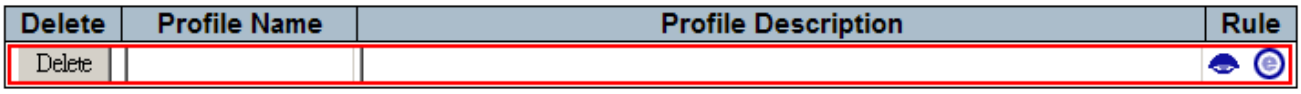
2.9.1 Profile Table



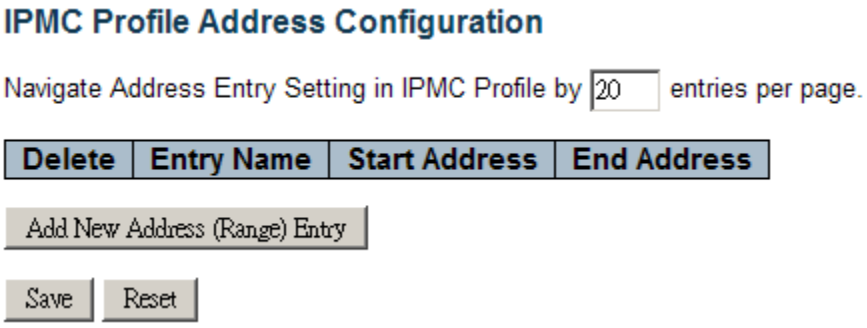
Configuration	Description
Global Mode	Enable/Disable the Global IPMC Profile. System starts to do filtering based on profile settings only when the global profile mode is enabled.
Delete	Check to delete the entry.
Profile Name	The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and

	numeric characters. At least one alphabet must be present.
Profile Description	Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.
Rule	When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons: : List the rules associated with the designated profile. : Adjust the rules associated with the designated profile.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click Add New IPMC Profile:



2.9.2 Address Entry



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

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

Click Add New Address (Range) Entry:

Delete	Entry Name	Start Address	End Address
Delete			

2.10 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.

MVR Configurations

MVR Mode	Disabled

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile

Add New MVR VLAN

Immediate Leave Setting

Port	Immediate Leave
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled

Save Reset

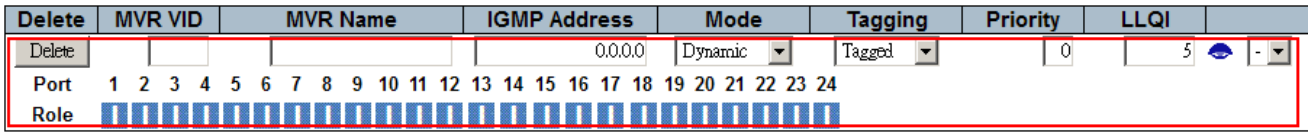
Configuration	Description (Example with MSTI1)
MVR Mode	Enable/Disable the Global MVR.

	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.
IGMP Address	Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.
Mode	Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.
Tagging	Specify whether the traversed IGMP/MLD control frames will be sent as *Untagged* or *Tagged* with MVR VID. The default is *Tagged*.
Priority	Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.
LLQI	Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.
Interface Channel Profile	
	You can inspect the rules of the designated profile by using the following button:  : List the rules associated with the designated profile.
Port	The logical port for the settings
Port Role	Configure an MVR port of the designated MVR VLAN as one of the following roles. *Inactive*: The designated port does not participate MVR operations. *Source*: Configure uplink ports that receive and send multicast data as source ports.

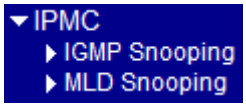
	Subscribers cannot be directly connected to source ports. *Receiver*: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages. *Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.* Select the port role by clicking the Role symbol to switch the setting. *I:* indicates Inactive; *S:* indicates Source; R indicates Receiver The default Role is Inactive.
Immediate Leave	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.

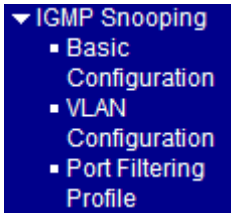
Click Add New MVR VLAN:



2.11 IPMC



2.11.1 IGMP Snooping



2.11.1.1 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

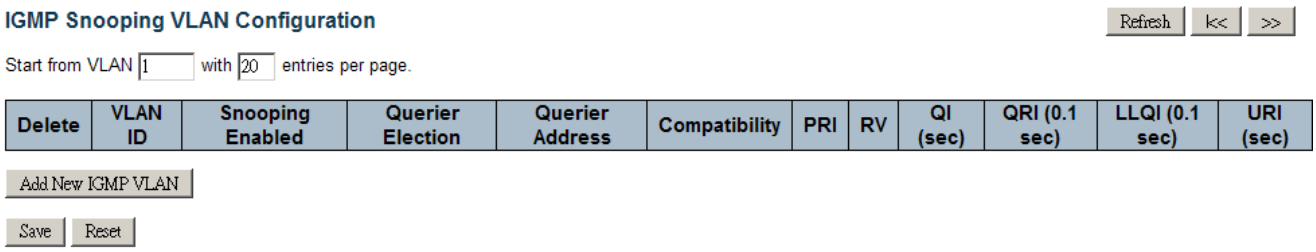
Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☐	☐	unlimited
7	☐	☐	unlimited
8	☐	☐	unlimited
9	☐	☐	unlimited
10	☐	☐	unlimited
11	☐	☐	unlimited
12	☐	☐	unlimited
13	☐	☐	unlimited
14	☐	☐	unlimited
15	☐	☐	unlimited
16	☐	☐	unlimited
17	☐	☐	unlimited
18	☐	☐	unlimited
19	☐	☐	unlimited
20	☐	☐	unlimited
21	☐	☐	unlimited
22	☐	☐	unlimited
23	☐	☐	unlimited
24	☐	☐	unlimited

Save Reset

Configuration	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMCv4 Flooding Enabled	Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.
IGMP SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
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.

2.11.1.2 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.
Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier Election	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier Address	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.
Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is *IGMP-Auto*, *Forced IGMPv1*, *Forced IGMPv2*, *Forced IGMPv3*, default compatibility value is *IGMP-Auto*.
PRI	Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2.
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125

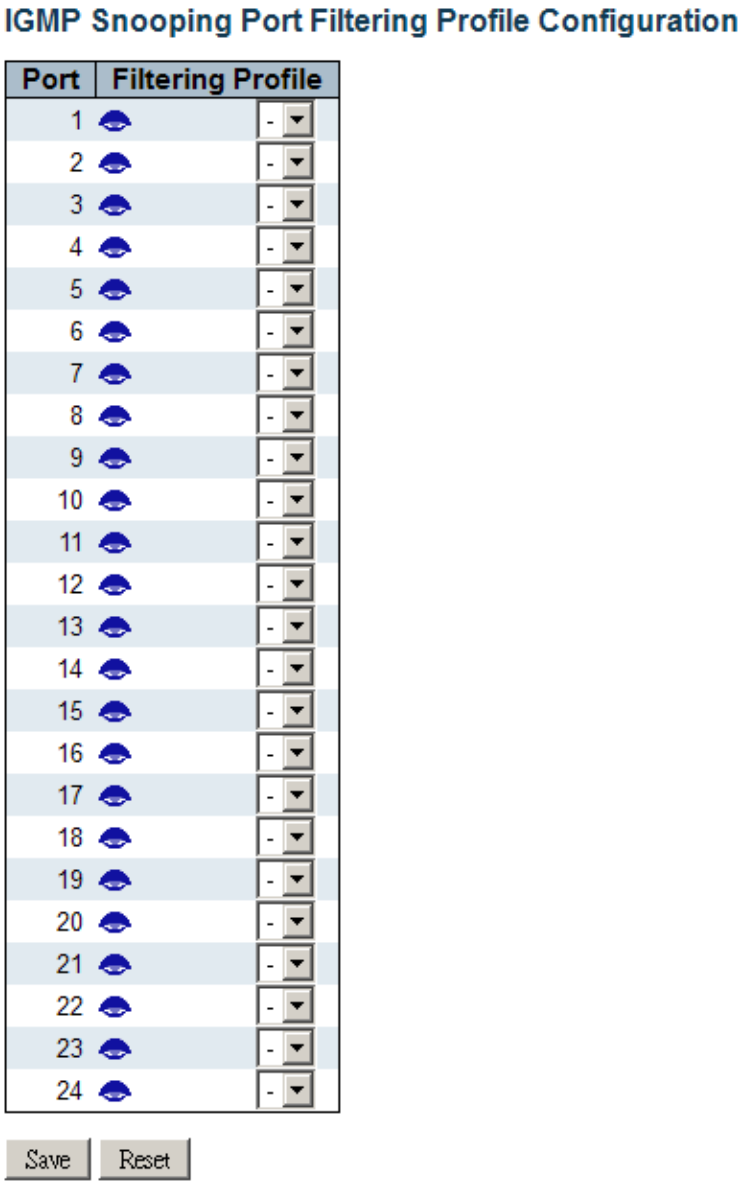
	seconds.
QRI	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
LLQI (LMQI for IGMP)	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).
URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

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 :

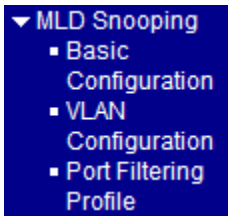
Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Delete		☐	☑	0.0.0.0	IGMP-Auto	0	2	125	100	10	1

2.11.1.3 Port Group Profile



Configuration	Description (Example with MSTI1)
Port	The logical port for the settings.
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.
	Profile Management Button You can inspect the rules of the designated profile by using the following button: List the rules associated with the designated profile.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.11.2 MLD Snooping



2.11.2.1 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

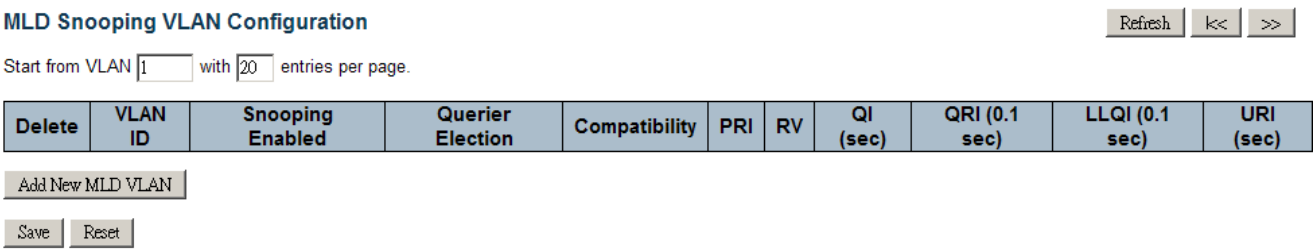
Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☐	☐	unlimited
7	☐	☐	unlimited
8	☐	☐	unlimited
9	☐	☐	unlimited
10	☐	☐	unlimited
11	☐	☐	unlimited
12	☐	☐	unlimited
13	☐	☐	unlimited
14	☐	☐	unlimited
15	☐	☐	unlimited
16	☐	☐	unlimited
17	☐	☐	unlimited
18	☐	☐	unlimited
19	☐	☐	unlimited
20	☐	☐	unlimited
21	☐	☐	unlimited
22	☐	☐	unlimited
23	☐	☐	unlimited
24	☐	☐	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.

2.11.2.2 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.
Snooping Enabled	Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.
Querier Election	Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.
Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is *MLD-Auto*, *Forced MLDv1*, *Forced MLDv2*, default compatibility value is *MLD-Auto*.
PRI	Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2.
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.
QRI	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
LLQI	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	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Delete		☐	☑	MLD-Auto	0	2	125	100	10	1

2.11.2.3 Port Group Profile

MLD Snooping Port Filtering Profile Configuration

Port	Filtering Profile
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-
21	-
22	-
23	-
24	-

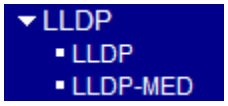
Save Reset

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 Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.
	Profile Management Button You can inspect the rules of the designated profile by using the following button: List the rules associated with the designated profile.

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

2.12 LLDP



2.12.1 LLDP

LLDP Configuration

LLDP Parameters

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

LLDP Port Configuration

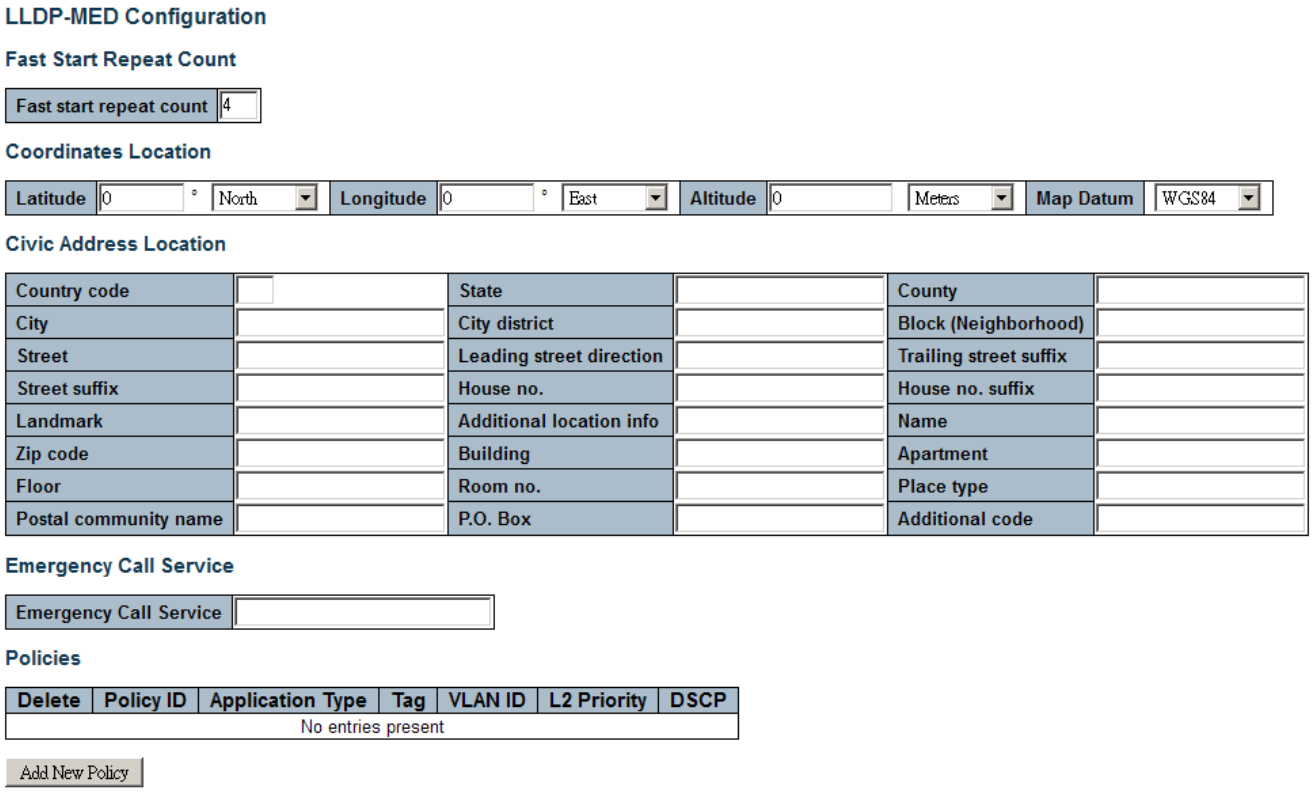
			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☐	☐	☐	☐	☐
1	Disabled	☐	☑	☑	☑	☑	☑
2	Disabled	☐	☑	☑	☑	☑	☑
3	Disabled	☐	☑	☑	☑	☑	☑
4	Disabled	☐	☑	☑	☑	☑	☑
5	Disabled	☐	☑	☑	☑	☑	☑
6	Disabled	☐	☑	☑	☑	☑	☑
7	Disabled	☐	☑	☑	☑	☑	☑
8	Disabled	☐	☑	☑	☑	☑	☑
9	Disabled	☐	☑	☑	☑	☑	☑
10	Disabled	☐	☑	☑	☑	☑	☑
11	Disabled	☐	☑	☑	☑	☑	☑
12	Disabled	☐	☑	☑	☑	☑	☑
13	Disabled	☐	☑	☑	☑	☑	☑
14	Disabled	☐	☑	☑	☑	☑	☑
15	Disabled	☐	☑	☑	☑	☑	☑
16	Disabled	☐	☑	☑	☑	☑	☑
17	Disabled	☐	☑	☑	☑	☑	☑
18	Disabled	☐	☑	☑	☑	☑	☑
19	Disabled	☐	☑	☑	☑	☑	☑
20	Disabled	☐	☑	☑	☑	☑	☑
21	Disabled	☐	☑	☑	☑	☑	☑
22	Disabled	☐	☑	☑	☑	☑	☑
23	Disabled	☐	☑	☑	☑	☑	☑
24	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.

2.12.2 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.

2.13 MAC Table

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	☐
Aging Time	300 seconds

MAC Table Learning

	Port Members																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Auto	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Static MAC Table Configuration

			Port Members																					
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Add New Static Entry

Save Reset

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 :

Delete	VLAN ID	MAC Address	Port Members 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Delete	1	00-00-00-00-00-00	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

2.14 VLANs

- VLANs
  - VLAN Membership
  - Ports

2.14.1 VLAN Membership

Global VLAN Configuration

Allowed Access VLANs	1-4
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tag Insert Rule	Allowed VLANs	Forbidden VLANs
*	<>		<>	☐	<>	<>		
1	Hybrid	2	C-Port	☐	Tagged and Untagged	NO_PVID	2	4
2	Hybrid	2	C-Port	☐	Tagged and Untagged	NO_PVID	2	
3	Hybrid	2	C-Port	☐	Tagged and Untagged	NO_PVID	2	
4	Hybrid	3	C-Port	☐	Tagged and Untagged	NO_PVID	3	2
5	Hybrid	3	C-Port	☐	Tagged and Untagged	NO_PVID	3	
6	Hybrid	3	C-Port	☐	Tagged and Untagged	NO_PVID	3	
7	Hybrid	4	C-Port	☐	Tagged and Untagged	NO_PVID	4	
8	Hybrid	4	C-Port	☐	Tagged and Untagged	NO_PVID	4	
9	Hybrid	4	C-Port	☐	Tagged and Untagged	NO_PVID	4	
10	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
11	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
12	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
13	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
14	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
15	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
16	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
17	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
18	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
19	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
20	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
21	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
22	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
23	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	
24	Hybrid	1	C-Port	☐	Tagged and Untagged	NO_PVID	1	

Save Reset

Global Configuration	Description
Allowed Access VLANs	This field shows the allowed Access VLANs, i.e. it only affects ports configured as *Access ports*. Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.
Ethertype for Custom S-ports	This field specifies the ethertype/TPID (specified in hexadecimal) used for S-Custom -ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port Configuration	Description
Port	This is the logical port number of this row.
Mode	The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out field shows the value of the port will get when the mode is applied. ***Access*:** Access ports are normally used to connect end stations. Access ports have the following characteristics: * Member of only one VLAN, or called the Port VLAN (also called Access VLAN), which by default is 1 * Accepts all frame types including untagged and C-tagged frames * Discards the frames that are not classified to the Access VLAN * On egress the frames classified to the Access VLAN are transmitted untagged. Others are transmitted tagged as Access VLAN ***Trunk*:** Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect other switches. Trunk ports have the following characteristics: * By default, a trunk port is member of all VLANs (1-4095) * A trunk port can be the member of more than one VLAN. The VLAN membership is configured in Allowed VLANs. * On ingress the trunk port must be the member of the classified VLAN. Otherwise, the frame is discarded. * On egress a frame's classified VLAN does not matches the Port VLAN (a.k.a.

	Native VLAN). The frame is tagged with its classified VLAN ID. Otherwise, the frame does not get C-tagged. * Egress tagging configuration can be changed to tag all frames if only tagged frames are accepted on ingress. ***Hybrid*:** Hybrid ports resemble trunk ports in many ways, but given more flexibility of port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities: * Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware * Ingress filtering can be controlled * Ingress acceptance of frames and configuration of egress tagging can be configured independently
Port VLAN	Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1. On ingress, frames get classified to the Port VLAN if one of the following conditions matches: * The port is configured as VLAN unaware * The frame is untagged * VLAN awareness is enabled on the port, but the frame is priority tagged (VID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to *NO_PVID*. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.
Port Type	Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is inserted. ***Unaware:*** On ingress, all frames whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress. ***C-Port:*** On ingress, tagged frames (TPID 0x8100 or 0x88A8) get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. ***S-Port:*** On ingress, tagged frames (TPID 0x8100 or 0x88A8) get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be

tagged with an S-tag.

S-Custom-Port: On ingress, tagged frames (TPID 0x8100 or TPID equal to the value configured in "Ethertype for Custom S-ports") get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the S-Custom-tag.

Mode	**Port type options**
Access	*C-Port (fixed)*
Trunk	*C-Port (fixed)*
Hybrid	*Unaware, C-Port, S-Port, S-Custom-Port*

Ingress Filtering

Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.

If ingress filtering is enabled (checkbox is checked), the frames classified to a VLAN of which the port is not a member get discarded. Otherwise, the frames are accepted and forwarded to the switch engine.

Mode	**Ingress Filtering options**
Access	*Enabled*
Trunk	*Enabled*
Hybrid	*Enabled, Disabled*

Ingress Acceptance

Hybrid ports allow for changing the type of frames that are accepted on ingress.

Tagged and Untagged Both tagged and untagged frames are accepted.

Tagged Only Only tagged frames are accepted on ingress. Untagged frames are discarded.

Untagged Only Only untagged frames are accepted on ingress. Tagged frames are discarded.

Port Type	**Tagged frames** are defined:
C-Port	*Frames tagged with C-tag (TPID 0x8100)*
S-Port	*Frames tagged with S-tag (TPID 0x88a8)*
S-Custom-Port	*Frames tagged with Custom S-tag (Custom TPID configured in "Ethertype for Custom S-ports".)*

Egress Tag Insert Rule — Set egress tagging of the port.

NO_PVID No classified tag insertion if egress PVID matches the classified VID.

Yes Insert the classified tag for each frame.

No No tag insertion for all frames.

Mode	Ingress Acceptance options	Egress Tag Insert Rule options
Access	*Tagged and Untagged*	*NO_PVID*
Trunk	*Tagged and Untagged*	*NO_PVID*
	Tagged Only	*Yes*
Hybrid	*Free for configuration except "Unaware" port type*	*Free for configuration*

Note:

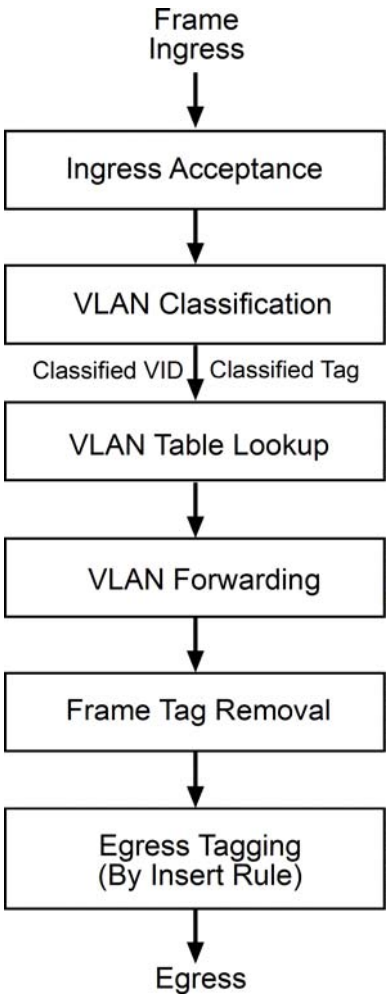
Mode	Port Type	Frame's tag removal before tag insertion
Access	*C-Port*	*1 (Outer tag if doubled tagged)*
Trunk	*C-Port*	*1 (Outer tag if doubled tagged)*
Hybrid	*Unaware*	*0 (No removal)*
	C-Port, S-Port, S-Custom-Port	*1 (Outer tag if doubled tagged)*

Allowed VLANs — Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095. The field may be left empty, which means that the port will not become member of any VLANs.

Forbidden VLANs — A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.

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

Remarks:



Each incoming frame on the ingress port passes “Ingress Acceptance” process first for filtering accepted frames and discarding others. Then, the frame gets into “VLAN Classification” process for getting Classified VLAN and classified tag. The “Classified VLAN” is used for VLAN table lookup and VLAN bridging operation. The “Classified tag” is used for tag insertion for egress tagging is required.

Ingress Port Type	Frame type	Classified VLAN	Classified TPID
Unaware	All frame types	PVID	0x8100
C-Port	Untagged	PVID	0x8100
	Priority C-tagged	PVID	Frame's TPID
	C-tagged	Frame's VID	Frame's TPID
	Priority S-tagged	PVID	Frame's TPID
	S-tagged	Frame's VID	Frame's TPID
	Priority S-Custom-tagged	PVID	0x8100
	S-Custom-tagged	PVID	0x8100
S-Port	Untagged	PVID	0x88a8
	Priority C-tagged	PVID	Frame's TPID
	C-tagged	Frame's VID	Frame's TPID
	Priority S-tagged	PVID	Frame's TPID
	S-tagged	Frame's VID	Frame's TPID
	Priority S-Custom-tagged	PVID	0x88a8
	S-Custom-tagged	PVID	0x88a8
S-Custom-Port	Untagged	PVID	Custom TPID
	Priority C-tagged	PVID	Frame's TPID
	C-tagged	Frame's VID	Frame's TPID
	Priority S-tagged	PVID	Custom TPID
	S-tagged	PVID	Custom TPID
	Priority S-Custom-tagged	PVID	Frame's TPID
	S-Custom-tagged	Frame's VID	Frame's TPID

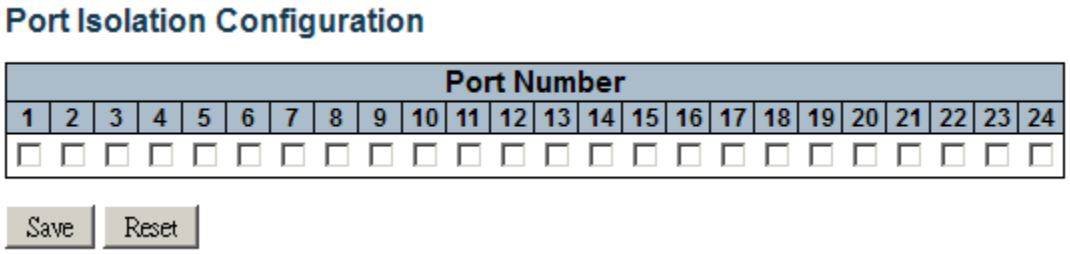
Custom TPID: The value configured in "Ethertype for Custom S-ports" setting.

2.15 Private VLANs

This page is used for enabling or disabling port isolation on ports in a Private VLAN.

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

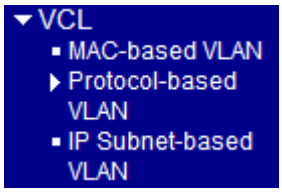
2.15.1 Port Isolation



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.

2.16 VCL



2.16.1 MAC-based VLAN

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

MAC-based VLAN Membership Configuration

			Port Members																						
Delete	MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Currently no entries present																										

Add New Entry

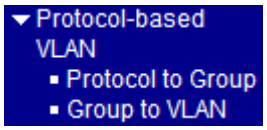
Save Reset

Configuration	Description
Delete	To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.
MAC Address	Indicates the MAC address.
VLAN ID	Indicates the VLAN ID.
Port Members	A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Add New Entry	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.

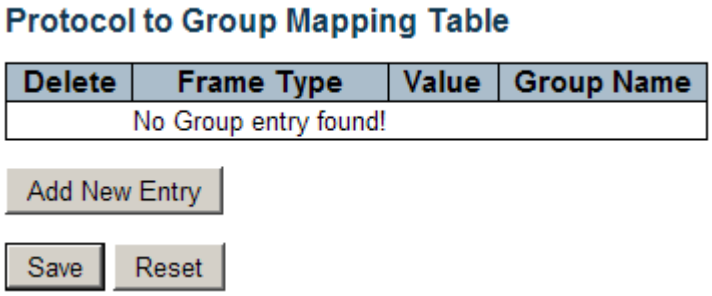
Click Add New Entry :

			Port Members																						
Delete	MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Delete	00-00-00-00-00-00	1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

2.16.2 Protocol-based VLAN



2.16.2.1 Protocol to Group



Configuration	Description
Delete	To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.
Frame Type	Frame Type can have one of the following values: *Ethernet*, *LLC*, *SNAP* *Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.*
Value	Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. Below are the criteria for three different Frame Types: For *Ethernet*: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff For *LLC*: Valid value in this case is comprised of two different sub-values. a. DSAP: 1-byte long string (0x00-0xff) b. SSAP: 1-byte long string (0x00-0xff) For *SNAP*: Valid value in this case also is comprised of two different sub-values. a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff. b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

	In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.
Group Name	A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9). Note: special character and underscore (_) are not allowed.

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	Frame Type	Value	Group Name
Delete	Ethernet	Etype: 0x 0800	

2.16.2.2 Group to VLAN

Group Name to VLAN mapping Table

			Port Members																						
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
No Group entries																										

Add New Entry

Save Reset

Configuration	Description
Group Name	A valid Group Name is a string at the most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers (0-9). No special character is allowed. Whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.
VLAN ID	Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.
Port Members	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

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 :

			Port Members																						
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Delete			☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

2.16.3 IP Subnet-based VLAN

IP Subnet-based VLAN Membership Configuration

					Port Members																				
Delete	VCE ID	IP Address	Mask Length	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Currently no entries present																												

Add New Entry

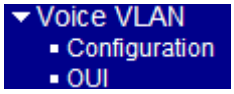
Save Reset

Configuration	Description
Delete	To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.
VCE ID	Indicates the index of the entry. It is user configurable. The value range is from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.
IP Address	Indicates the IP address.
Mask Length	Indicates the network mask length.
VLAN ID	Indicates the VLAN ID. VLAN ID can be changed for the existing entries.
Port Members	A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
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	VCE ID	IP Address	Mask Length	VLAN ID	Port Members																				
					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Delete	0	0.0.0.0	24	1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

2.17 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.

2.17.1 Configuration

Voice VLAN Configuration

Mode	Disabled
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High)

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9	Disabled	Disabled	OUI
10	Disabled	Disabled	OUI
11	Disabled	Disabled	OUI
12	Disabled	Disabled	OUI
13	Disabled	Disabled	OUI
14	Disabled	Disabled	OUI
15	Disabled	Disabled	OUI
16	Disabled	Disabled	OUI
17	Disabled	Disabled	OUI
18	Disabled	Disabled	OUI
19	Disabled	Disabled	OUI
20	Disabled	Disabled	OUI
21	Disabled	Disabled	OUI
22	Disabled	Disabled	OUI
23	Disabled	Disabled	OUI
24	Disabled	Disabled	OUI

Save Reset

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.

2.17.2 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

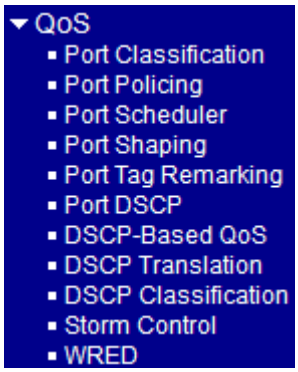
Save Reset

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		

2.18 QoS



2.18.1 Port Classification

QoS Ingress Port Classification

Port	CoS	DPL	DSCP Based
*	<>	<>	☐
1	0	0	☐
2	0	0	☐
3	0	0	☐
4	0	0	☐
5	0	0	☐
6	0	0	☐
7	0	0	☐
8	0	0	☐
9	0	0	☐
10	0	0	☐
11	0	0	☐
12	0	0	☐
13	0	0	☐
14	0	0	☐
15	0	0	☐
16	0	0	☐
17	0	0	☐
18	0	0	☐
19	0	0	☐
20	0	0	☐
21	0	0	☐
22	0	0	☐
23	0	0	☐
24	0	0	☐

Save Reset

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.*
DPL	Controls the default Drop Precedence Level. All frames are classified to a DPL. If the port is VLAN aware and the frame is tagged, then the frame is classified to a DPL that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DPL. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL. The classified DPL can be overruled by a QCL entry.
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.

2.18.2 Port Policing

QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	☐		<>	☐
1	☐	500	kbps	☐
2	☐	500	kbps	☐
3	☐	500	kbps	☐
4	☐	500	kbps	☐
5	☐	500	kbps	☐
6	☐	500	kbps	☐
7	☐	500	kbps	☐
8	☐	500	kbps	☐
9	☐	500	kbps	☐
10	☐	500	kbps	☐
11	☐	500	kbps	☐
12	☐	500	kbps	☐
13	☐	500	kbps	☐
14	☐	500	kbps	☐
15	☐	500	kbps	☐
16	☐	500	kbps	☐
17	☐	500	kbps	☐
18	☐	500	kbps	☐
19	☐	500	kbps	☐
20	☐	500	kbps	☐
21	☐	500	kbps	☐
22	☐	500	kbps	☐
23	☐	500	kbps	☐
24	☐	500	kbps	☐

Save Reset

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.

2.18.3 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	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-
13	Strict Priority	-	-	-	-	-	-
14	Strict Priority	-	-	-	-	-	-
15	Strict Priority	-	-	-	-	-	-
16	Strict Priority	-	-	-	-	-	-
17	Strict Priority	-	-	-	-	-	-
18	Strict Priority	-	-	-	-	-	-
19	Strict Priority	-	-	-	-	-	-
20	Strict Priority	-	-	-	-	-	-
21	Strict Priority	-	-	-	-	-	-
22	Strict Priority	-	-	-	-	-	-
23	Strict Priority	-	-	-	-	-	-
24	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.

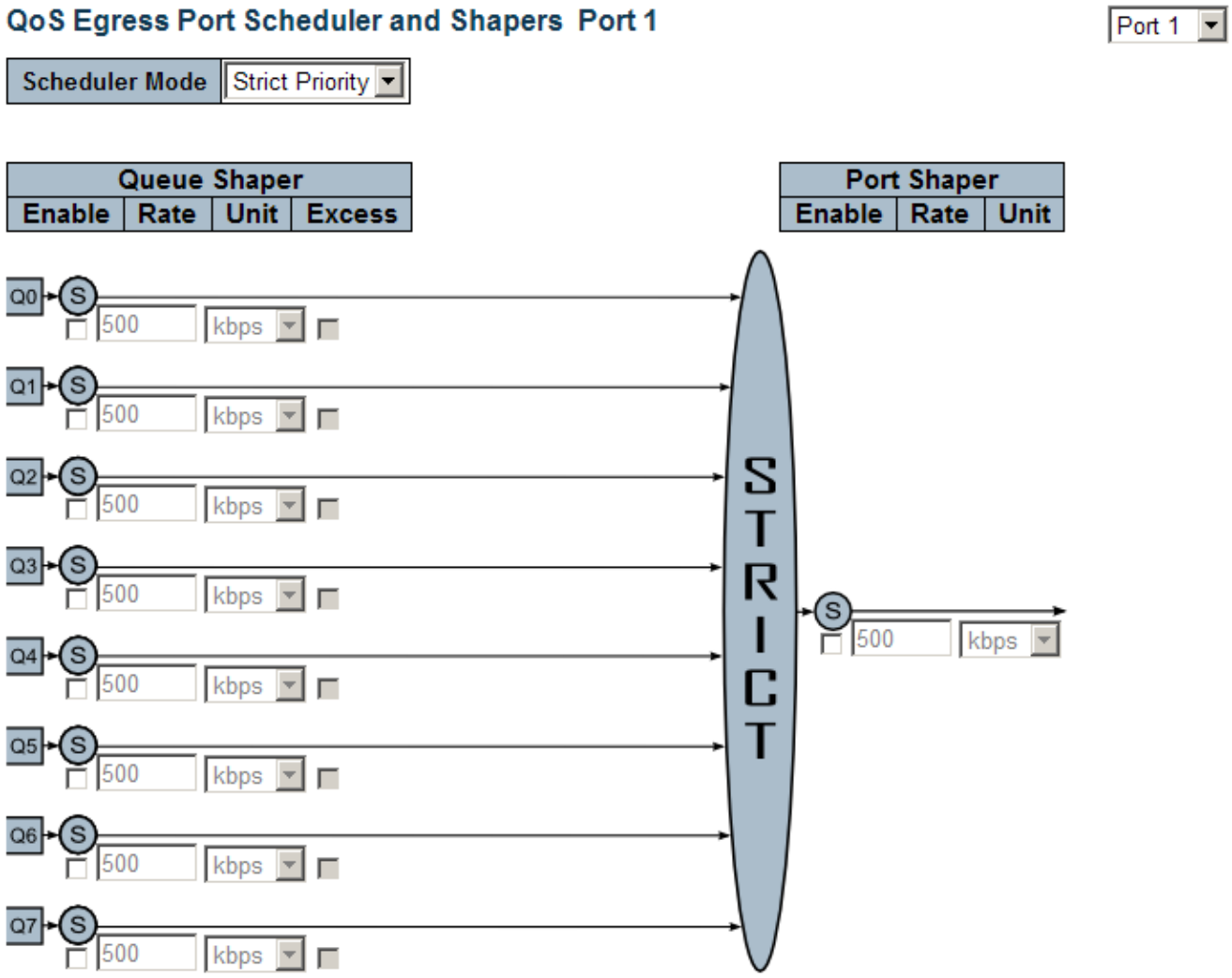
2.18.4 Shaping

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
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
13	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
14	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
15	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
16	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
17	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
18	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
19	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
20	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
21	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
22	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
23	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
24	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.

2.18.5 Tag Remarking

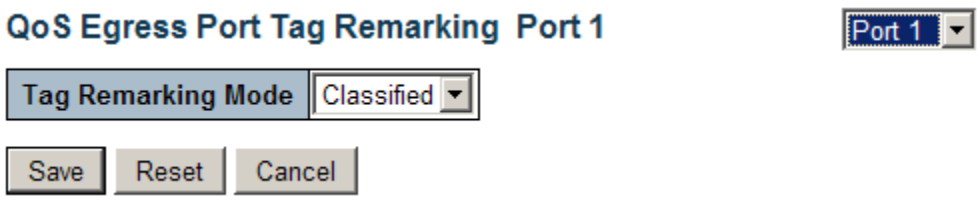
QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified
15	Classified
16	Classified
17	Classified
18	Classified
19	Classified
20	Classified
21	Classified
22	Classified
23	Classified
24	Classified

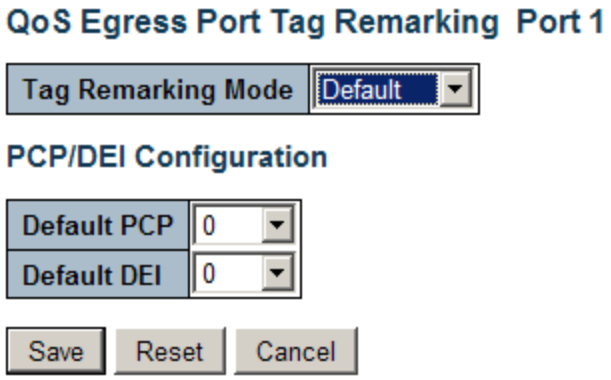
Configuration	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.
Mode	Shows the tag remarking mode for this port. *Classified*: Use classified PCP/DEI values. *Default*: Use default PCP/DEI values. *Mapped*: Use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

Click Port 1 icon as an example:

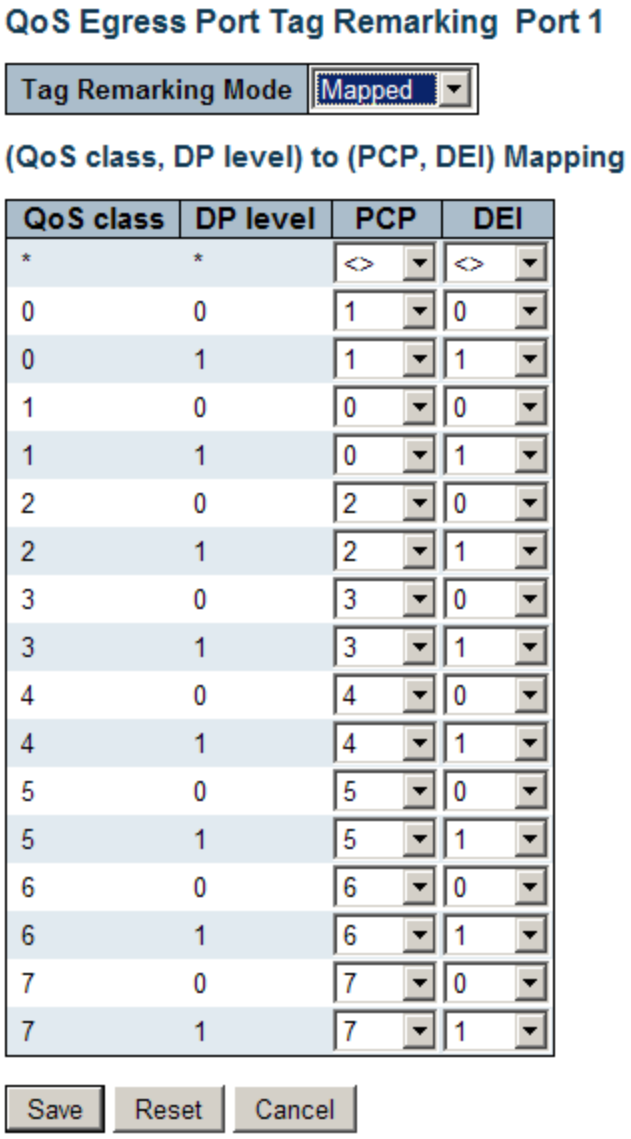
Mode = *Classified*



Mode = *Default*



Mode = *Mapped*

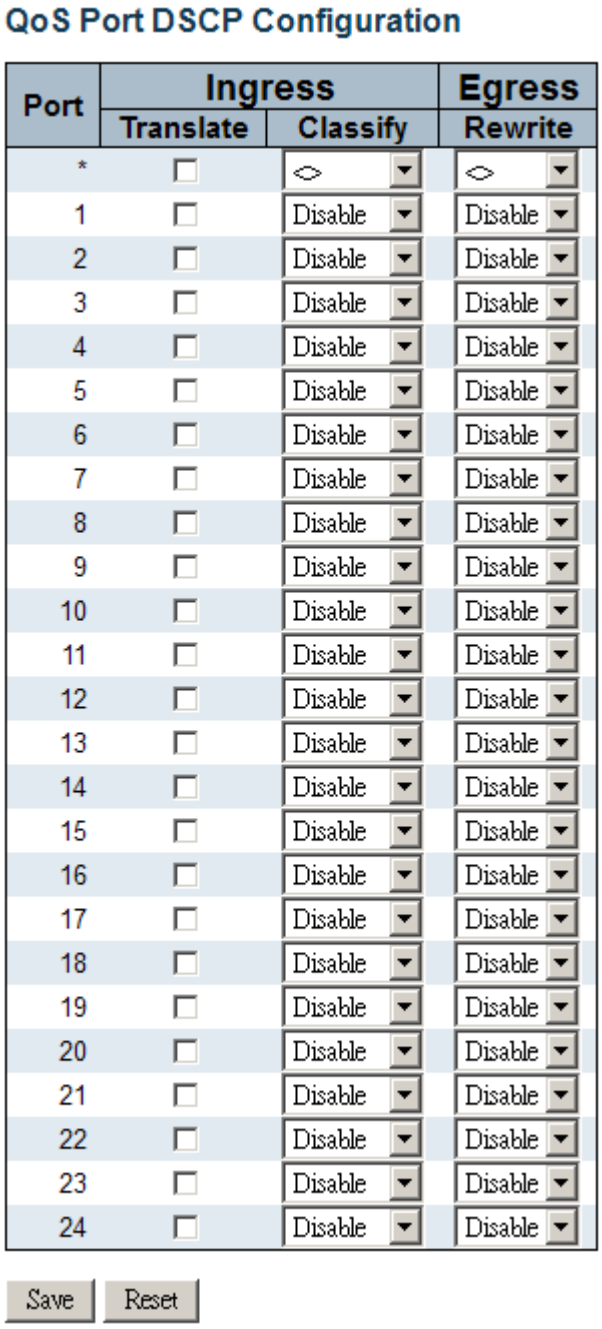


Configuration	Description

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.

2.18.6 Port DSCP



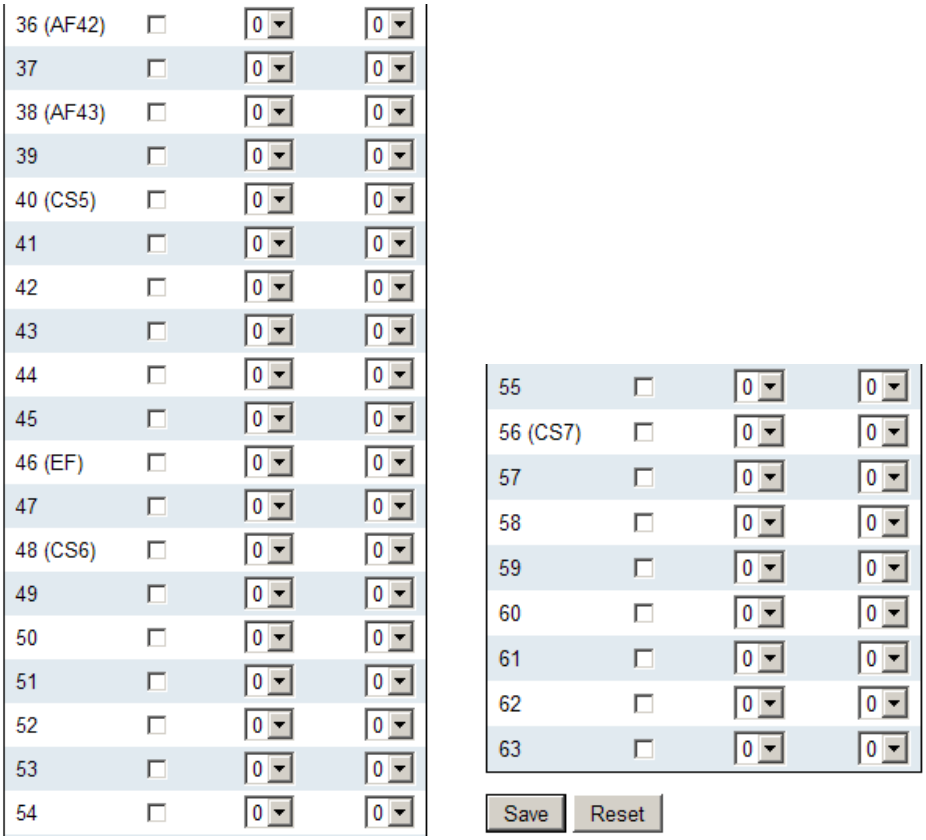
Configuration	Description
Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
Ingress	
Translate	To Enable the Ingress Translation click the checkbox.
Classify	Classification for a port have 4 different values. *Disable*: No Ingress DSCP Classification.

	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.

2.18.7 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



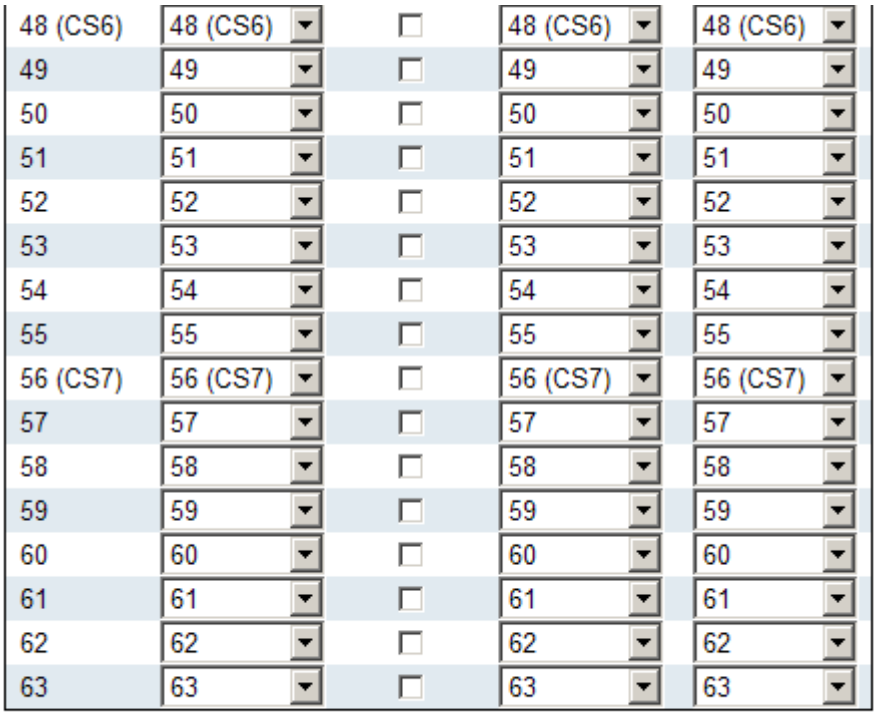
Configuration	Description
DSCP	Maximum number of supported DSCP values are 64.
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS 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.

2.18.8 DSCP Translation

DSCP Translation

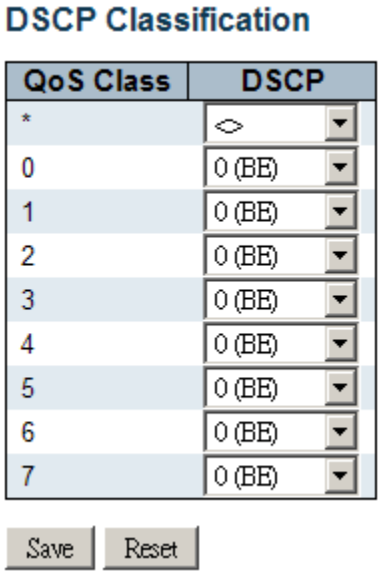
DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	☐	<>	<>
0 (BE)	0 (BE)	☐	0 (BE)	0 (BE)
1	1	☐	1	1
2	2	☐	2	2
3	3	☐	3	3
4	4	☐	4	4
5	5	☐	5	5
6	6	☐	6	6
7	7	☐	7	7
8 (CS1)	8 (CS1)	☐	8 (CS1)	8 (CS1)
9	9	☐	9	9
10 (AF11)	10 (AF11)	☐	10 (AF11)	10 (AF11)
11	11	☐	11	11
12 (AF12)	12 (AF12)	☐	12 (AF12)	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.

2.18.9 DSCP Classification



Configuration	Description
QoS Class	Actual QoS class.
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.

2.18.10 QoS Port 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.

QoS Port Storm Control

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enabled	Rate	Unit	Enabled	Rate	Unit	Enabled	Rate	Unit
*	☐		<>	☐		<>	☐		<>
1	☐	500	kbps	☐	500	kbps	☐	500	kbps
2	☐	500	kbps	☐	500	kbps	☐	500	kbps
3	☐	500	kbps	☐	500	kbps	☐	500	kbps
4	☐	500	kbps	☐	500	kbps	☐	500	kbps
5	☐	500	kbps	☐	500	kbps	☐	500	kbps
6	☐	500	kbps	☐	500	kbps	☐	500	kbps
7	☐	500	kbps	☐	500	kbps	☐	500	kbps
8	☐	500	kbps	☐	500	kbps	☐	500	kbps
9	☐	500	kbps	☐	500	kbps	☐	500	kbps
10	☐	500	kbps	☐	500	kbps	☐	500	kbps
11	☐	500	kbps	☐	500	kbps	☐	500	kbps
12	☐	500	kbps	☐	500	kbps	☐	500	kbps
13	☐	500	kbps	☐	500	kbps	☐	500	kbps
14	☐	500	kbps	☐	500	kbps	☐	500	kbps
15	☐	500	kbps	☐	500	kbps	☐	500	kbps
16	☐	500	kbps	☐	500	kbps	☐	500	kbps
17	☐	500	kbps	☐	500	kbps	☐	500	kbps
18	☐	500	kbps	☐	500	kbps	☐	500	kbps
19	☐	500	kbps	☐	500	kbps	☐	500	kbps
20	☐	500	kbps	☐	500	kbps	☐	500	kbps
21	☐	500	kbps	☐	500	kbps	☐	500	kbps
22	☐	500	kbps	☐	500	kbps	☐	500	kbps
23	☐	500	kbps	☐	500	kbps	☐	500	kbps
24	☐	500	kbps	☐	500	kbps	☐	500	kbps

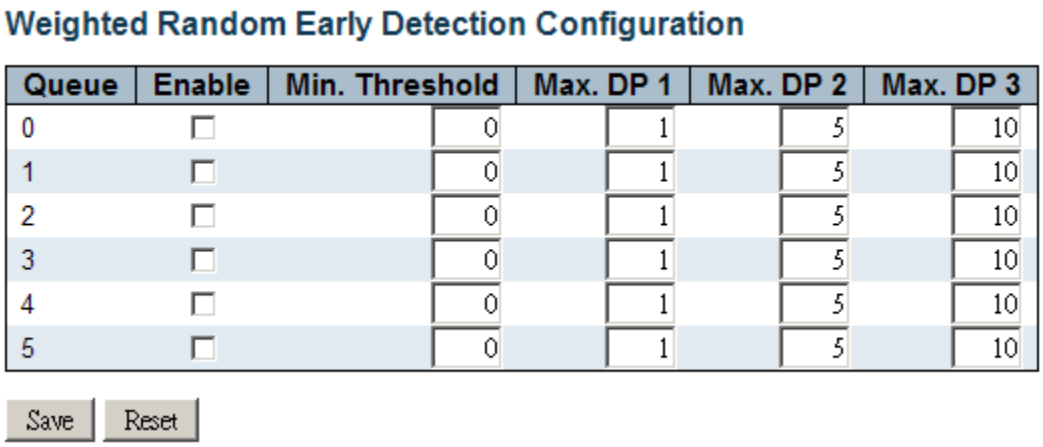
Save Reset

Configuration	Description
Enabled	Enable or disable the storm control status for the given frame type.
Rate	Controls the rate for the storm control. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-13200 when the "Unit" is "Mbps" or "kfps".
Unit	Controls the unit of measure for the storm control rate as kbps, Mbps, fps or kfps . 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.

2.18.11 WRED

This page allows you to configure the Random Early Detection (RED) settings for queue 0 to 5. RED cannot be applied to queue 6 and 7.

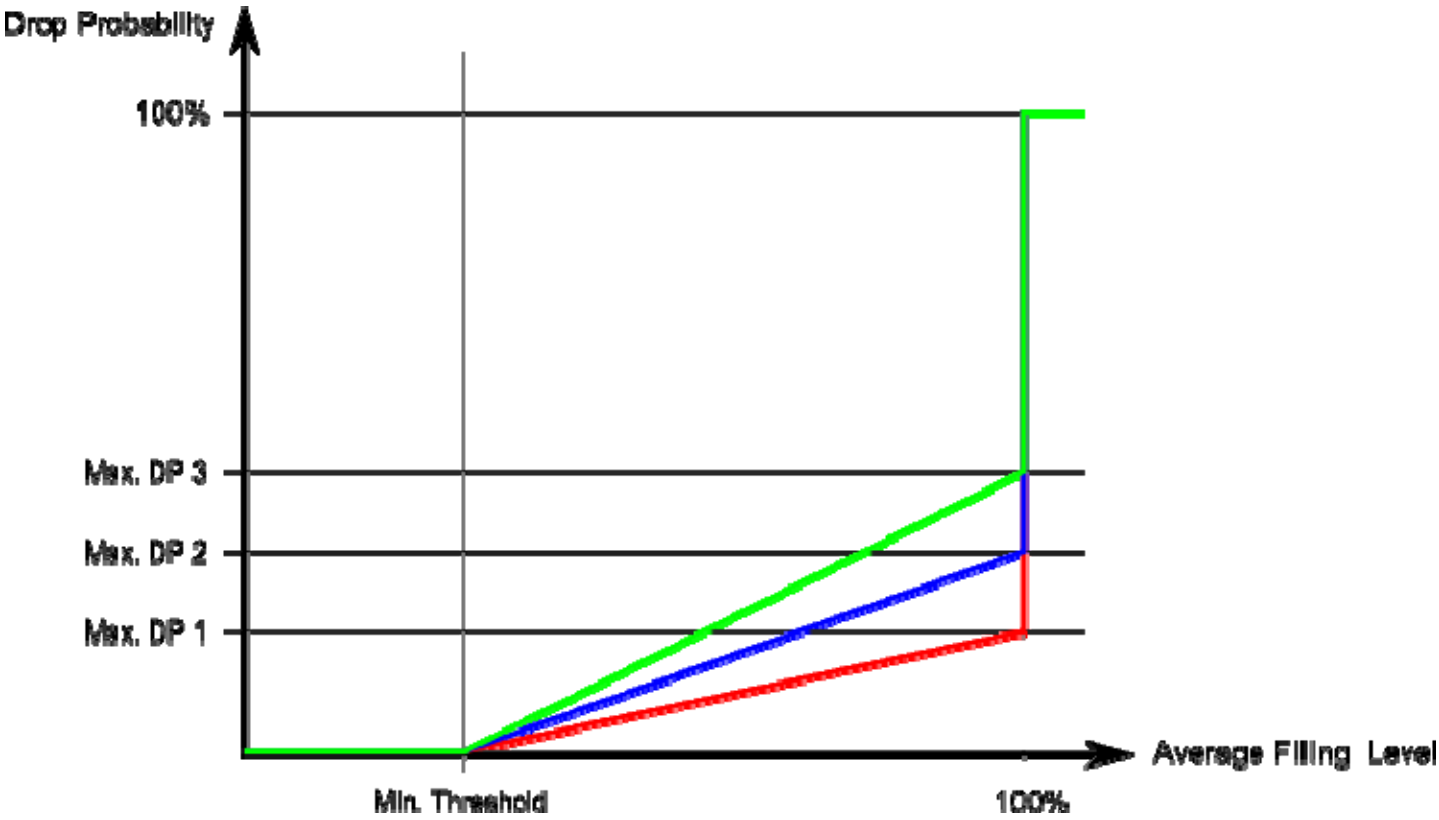
Through different RED configuration for the queues (QoS classes) it is possible to obtain Weighted Random Early Detection (WRED) operation between queues.



Configuration	Description
Queue	The queue number (QoS class) for which the configuration below applies.
Enable	Controls whether RED is enabled for this queue.
Min. Threshold	Controls the lower RED threshold. If the average queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100.
Max. DP1	Controls the drop probability for frames marked with Drop Precedence Level 1 when the average queue filling level is 100%. This value is restricted to 0-100.
Max. DP2	Controls the drop probability for frames marked with Drop Precedence Level 2 when the average queue filling level is 100%. This value is restricted to 0-100.
Max. DP3	Controls the drop probability for frames marked with Drop Precedence Level 3 when the average queue filling level is 100%. This value is restricted to 0-100.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

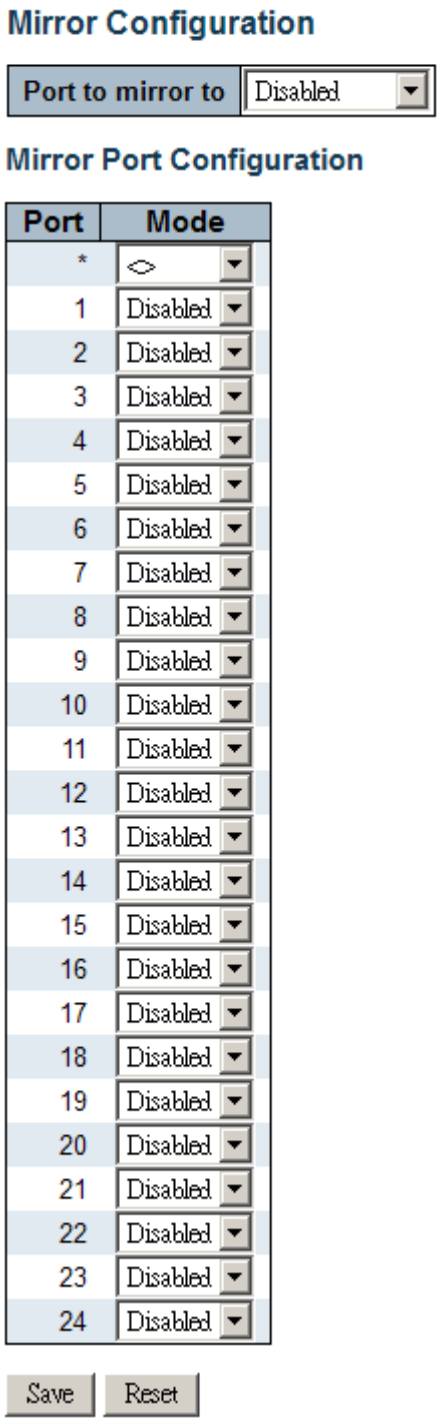
RED Drop Probability Function

The following illustration shows the drop probability function with associated parameters.



Max. DP 1-3 is the drop probability when the average queue filling level is 100%. Frames marked with Drop Precedence Level 0 are never dropped. Min. Threshold is the average queue filling level where the queues randomly start dropping frames. The drop probability for frames marked with Drop Precedence Level n increases linearly from zero (at Min. Threshold average queue filling level) to Max. DP n (at 100% average queue filling level).

2.19 Mirroring



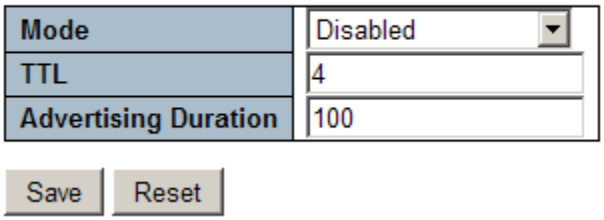
To debug network problems, selected traffic can be copied, or mirrored, on a **mirror port** where a frame analyzer can be attached to analyze the frame flow. The traffic to be copied on the **mirror port** is selected as follows:

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.

2.20 UPnP

UPnP Configuration

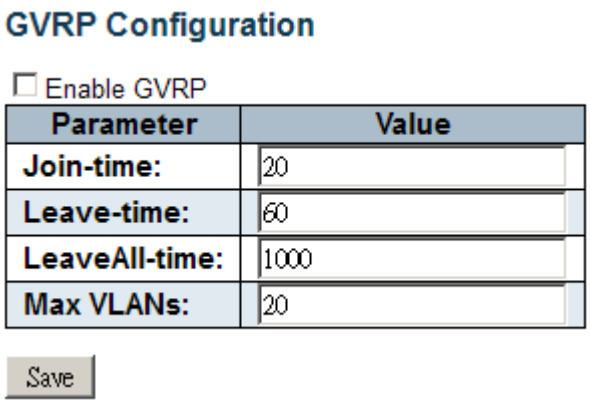


Configuration	Description
Mode	Indicates the UPnP operation mode. Possible modes are: ***Enabled:*** Enable UPnP mode operation. ***Disabled:*** Disable UPnP mode operation. When the mode is enabled, two ACEs are added automatically to trap UPnP related packets to CPU. The ACEs are automatically removed 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.

2.21 GVRP

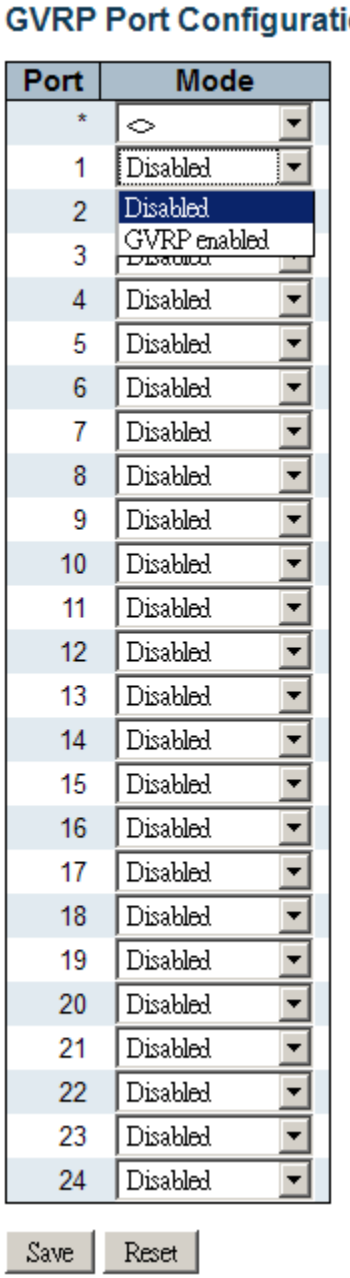
This page is to configure GVRP protocol timers.

2.21.1 Global Config



Configuration	Description
Enable GVRP	The GVRP feature is enabled by setting the check mark in the checkbox named Enable GVRP.
Join-time	Join-time is a value in the range 1-20 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 20.
Leave-time	Leave-time is a value in the range 60-300 in the units of centi seconds, i.e. in units of one hundredth of a second.The default is 60.
LeaveAll-time	LeaveAll-time is a value in the range 1000-5000 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 1000.
Max VLANs	When GVRP is enabled a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off.
Save	Click to save the changes.

2.21.2 Port Config



Configuration	Description
Port	Switch port
Mode	Disable or enable GVRP.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.22 sFlow

sFlow Configuration

Agent Configuration

IP Address	127.0.0.1

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
7	☐	0	128	☐	0
8	☐	0	128	☐	0
9	☐	0	128	☐	0
10	☐	0	128	☐	0
11	☐	0	128	☐	0
12	☐	0	128	☐	0
13	☐	0	128	☐	0
14	☐	0	128	☐	0
15	☐	0	128	☐	0
16	☐	0	128	☐	0
17	☐	0	128	☐	0
18	☐	0	128	☐	0
19	☐	0	128	☐	0
20	☐	0	128	☐	0
21	☐	0	128	☐	0
22	☐	0	128	☐	0
23	☐	0	128	☐	0
24	☐	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.
Release	The button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).
IP Address/Hostname	The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.
UDP Port	The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
Timeout	The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.
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.

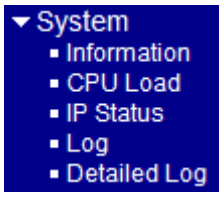
Port Configuration	
Port	The port number for which the configuration below applies.
Flow Sampler	
Enabled	Enables/disables flow sampling on this port.
Sampling Rate	The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. 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.

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

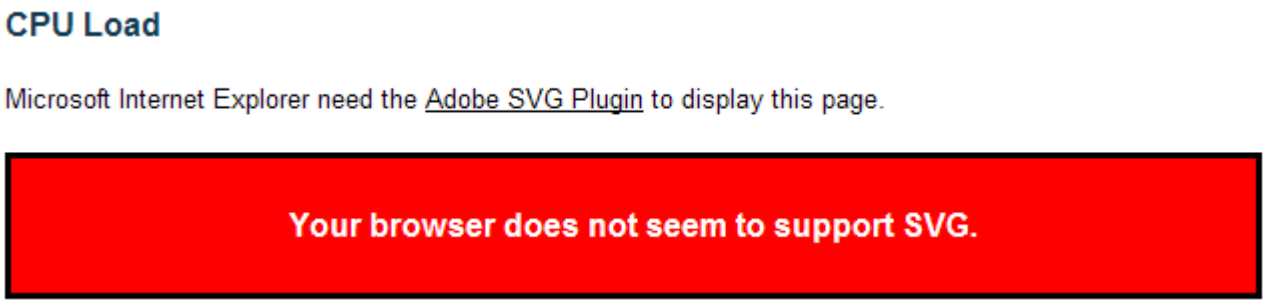
System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-40-f6-04-08-06
Chip ID	VSC7434
Time	
System Date	1970-01-03T18:32:11+00:00
System Uptime	2d 18:32:11
Software	
Software Version	v1.01 Beta 20150417PM1500
Software Date	2015-04-17T14:59:55+08:00
Acknowledgments	Details

Status	Description
Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person.
Name	An administratively assigned name for this managed node.
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.
Software Version	The software version of this switch
Software Date	The date when the switch software was produced.
Acknowledgments	Declaration for some system Open-source code Click Details to see more information.

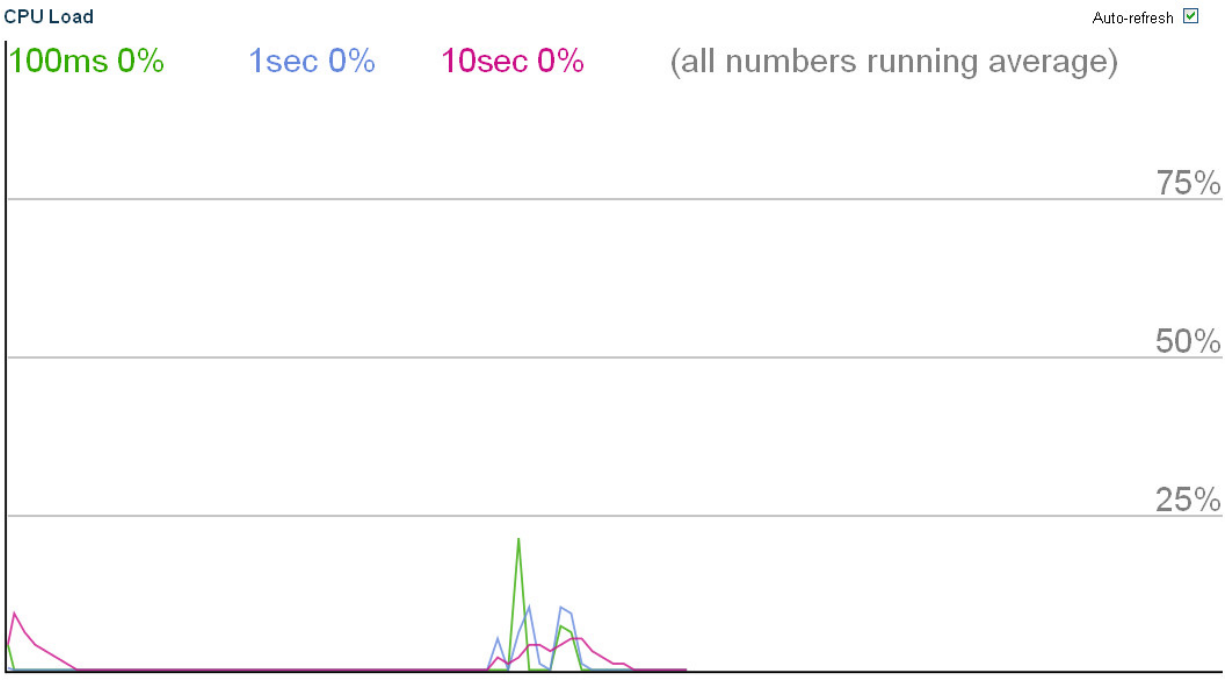
3.1.2 CPU Load

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 IP Status

IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	::1/128	
OS:lo	IPv6	fe80::1/64	
VLAN1	LINK	00-40-f6-04-08-06	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.179/24	
VLAN1	IPv6	fe80::240:f6ff:fe04:806/64	
VLAN1	IPv6	2000::5001/64	
VLAN2	LINK	00-40-f6-04-08-06	<UP BROADCAST RUNNING MULTICAST>
VLAN2	IPv4	192.168.1.179/24	
VLAN2	IPv6	2001::5001/64	
VLAN2	IPv6	fe80::240:f6ff:fe04:806/64	
VLAN3	LINK	00-40-f6-04-08-06	<UP BROADCAST RUNNING MULTICAST>
VLAN3	IPv4	192.168.2.179/24	
VLAN3	IPv6	2002::5001/64	
VLAN3	IPv6	fe80::240:f6ff:fe04:806/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
192.168.0.0/24	VLAN1	<UP HW_RT>
192.168.1.0/24	VLAN2	<UP HW_RT>
192.168.2.0/24	VLAN3	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>
2000::/64	VLAN1	<UP HW_RT>
2000::5001/128	40:f604:806::	<UP HOST>
2001::/64	VLAN2	<UP HW_RT>
2001::5001/128	40:f604:806::	<UP HOST>
2002::/64	VLAN3	<UP HW_RT>
2002::5001/128	40:f604:806::	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.0.113	VLAN1:00-22-15-be-84-af
192.168.0.120	VLAN1:fc-f5-28-fa-8d-34
2000::5001	VLAN1:00-40-f6-04-08-06
fe80::240:f6ff:fe04:806	VLAN1:00-40-f6-04-08-06
2001::5001	VLAN2:00-40-f6-04-08-06
fe80::240:f6ff:fe04:806	VLAN2:00-40-f6-04-08-06
2002::5001	VLAN3:00-40-f6-04-08-06
fe80::240:f6ff:fe04:806	VLAN3:00-40-f6-04-08-06

Status	Description

IP Interfaces

Interface	The name of the interface.
Type	The address type of the entry. This may be LINK or IPv4.
Address	The current address of the interface (of the given type).
Status	The status flags of the interface (and/or address).

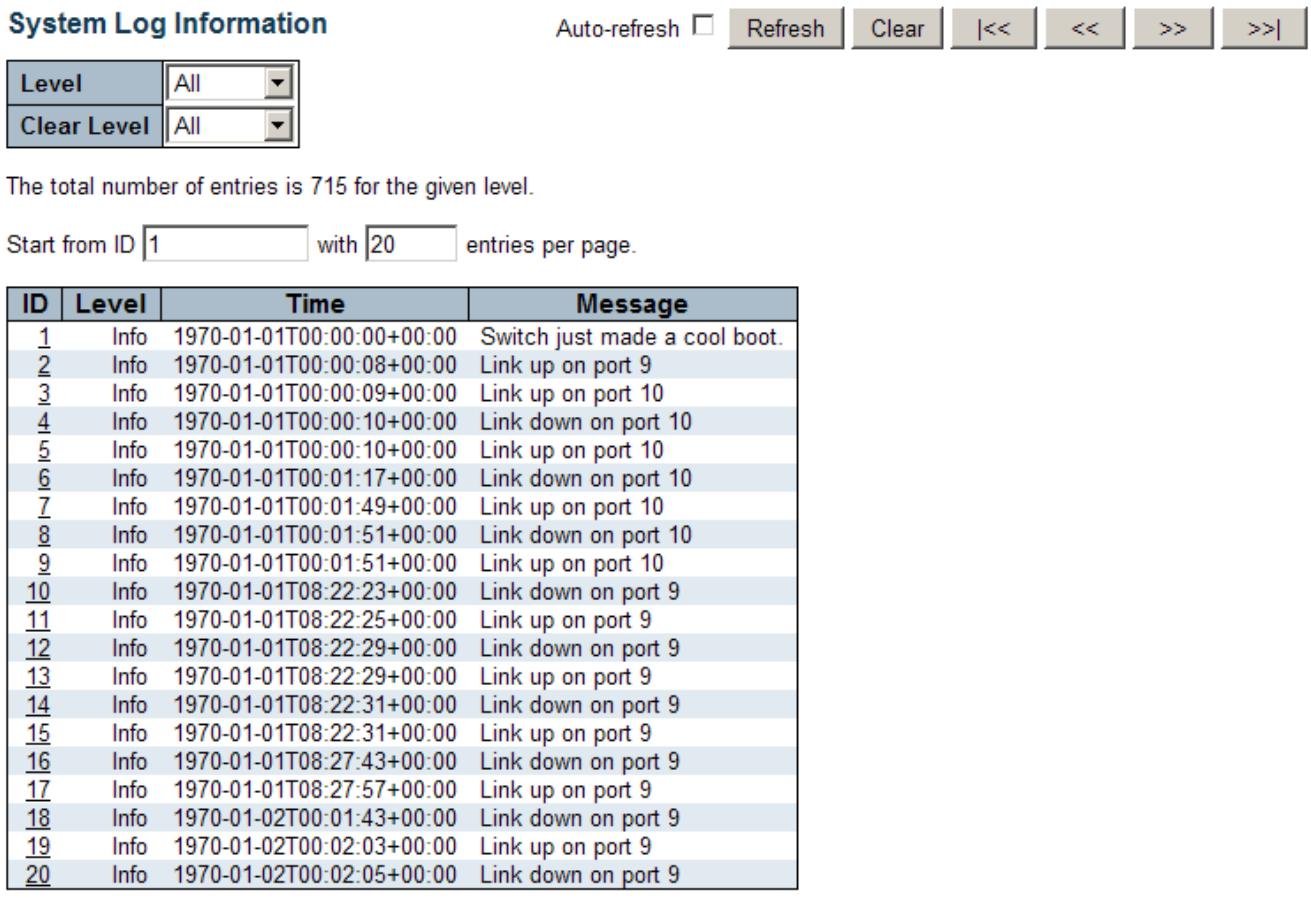
IP Routers

Network	The destination IP network or host address of this route.
Gateway	The gateway address of this route.
Status	The status flags of the route.

Neighbour cache

IP Address	The IP address of the entry.
Link Address	The Link (MAC) address for which a binding to the IP address given exist..

3.1.4 Log



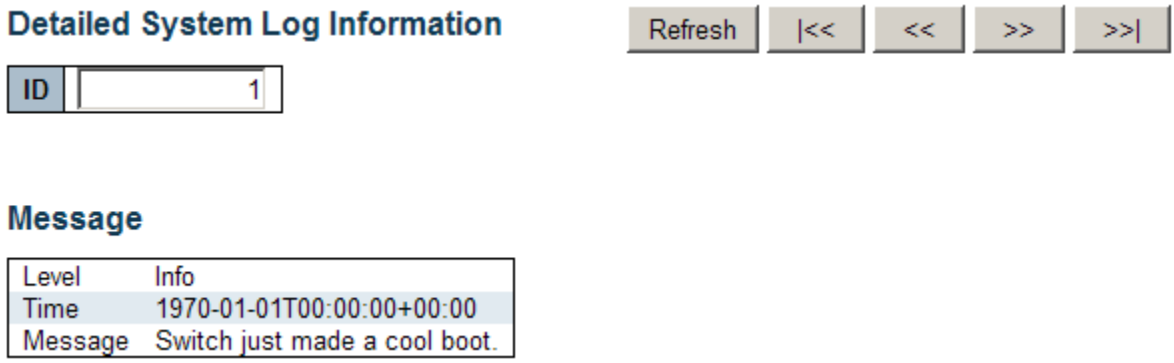
Status	Description

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.

3.1.5 Detailed Log



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

3.2 Green Ethernet – Port Power Savings

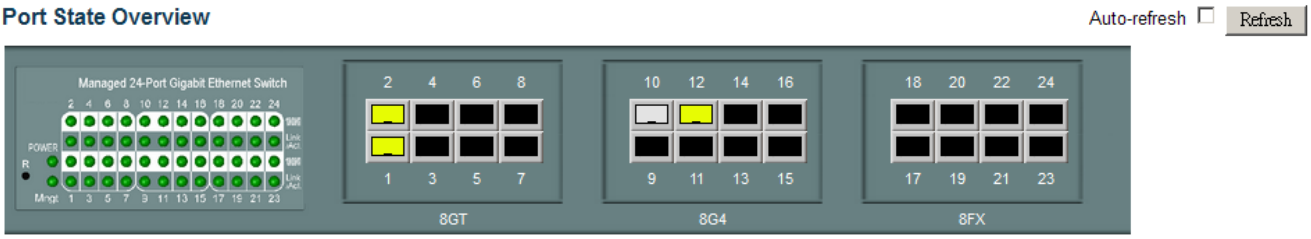
Port Power Savings Status

Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach Savings
1	●	✓	✗	✗	✗	✗	✗
2	●	✓	✗	✗	✗	✗	✗
3	●	✓	✗	✗	✗	✗	✗
4	●	✓	✗	✗	✗	✗	✗
5	●	✓	✗	✗	✗	✗	✗
6	●	✓	✗	✗	✗	✗	✗
7	●	✓	✗	✗	✗	✗	✗
8	●	✓	✗	✗	✗	✗	✗
9	●	✓	✗	✗	✗	✗	✗
10	●	✓	✗	✗	✗	✗	✗
11	●	✓	✗	✗	✗	✗	✗
12	●	✓	✗	✗	✗	✗	✗
13	●	✓	✗	✗	✗	✗	✗
14	●	✓	✗	✗	✗	✗	✗
15	●	✓	✗	✗	✗	✗	✗
16	●	✓	✗	✗	✗	✗	✗
17	●	✓	✗	✗	✗	✗	✗
18	●	✓	✗	✗	✗	✗	✗
19	●	✓	✗	✗	✗	✗	✗
20	●	✓	✗	✗	✗	✗	✗
21	●	✓	✗	✗	✗	✗	✗
22	●	✓	✗	✗	✗	✗	✗
23	●	✓	✗	✗	✗	✗	✗
24	●	✓	✗	✗	✗	✗	✗

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

3.3 Ports

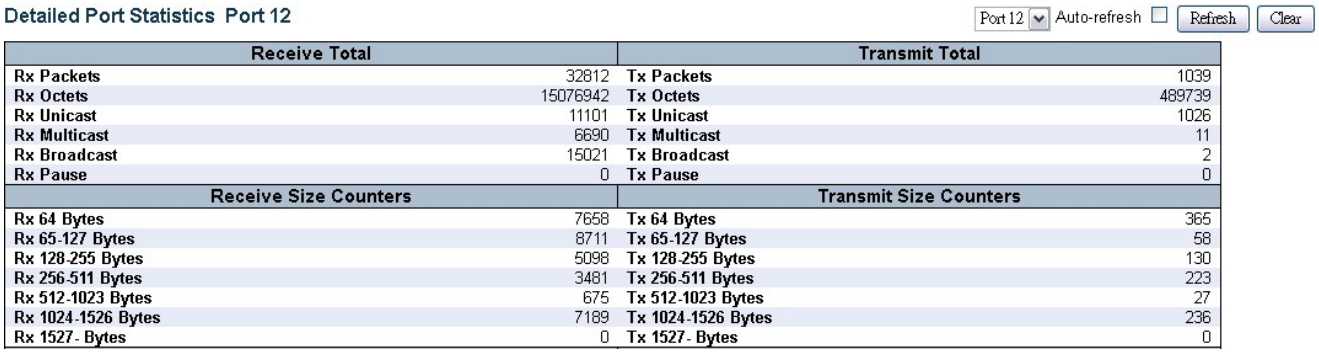
3.3.1 State



Status	Description
	Port disabled
	Port link down
	Port link up

Click Port Icon to display detailed statistics of the port.

Example for Port 12:



Receive Total		Transmit Total	
Rx Packets	32812	Tx Packets	1039
Rx Octets	15076942	Tx Octets	489739
Rx Unicast	11101	Tx Unicast	1026
Rx Multicast	6690	Tx Multicast	11
Rx Broadcast	15021	Tx Broadcast	2
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	7658	Tx 64 Bytes	365
Rx 65-127 Bytes	8711	Tx 65-127 Bytes	58
Rx 128-255 Bytes	5098	Tx 128-255 Bytes	130
Rx 256-511 Bytes	3481	Tx 256-511 Bytes	223
Rx 512-1023 Bytes	675	Tx 512-1023 Bytes	27
Rx 1024-1526 Bytes	7189	Tx 1024-1526 Bytes	236
Rx 1527 - Bytes	0	Tx 1527 - Bytes	0

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	0	0	0	0	0	0	0	0	0
2	199	44	303674	10265	0	0	0	0	34
3	0	0	0	0	0	0	0	0	0
4	250	51	381500	14445	0	0	0	0	22
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	1821576	63443	303672150	6132406	0	0	44	0	10668
10	69687	1777337	5424511	297450052	7519	0	0	0	10

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

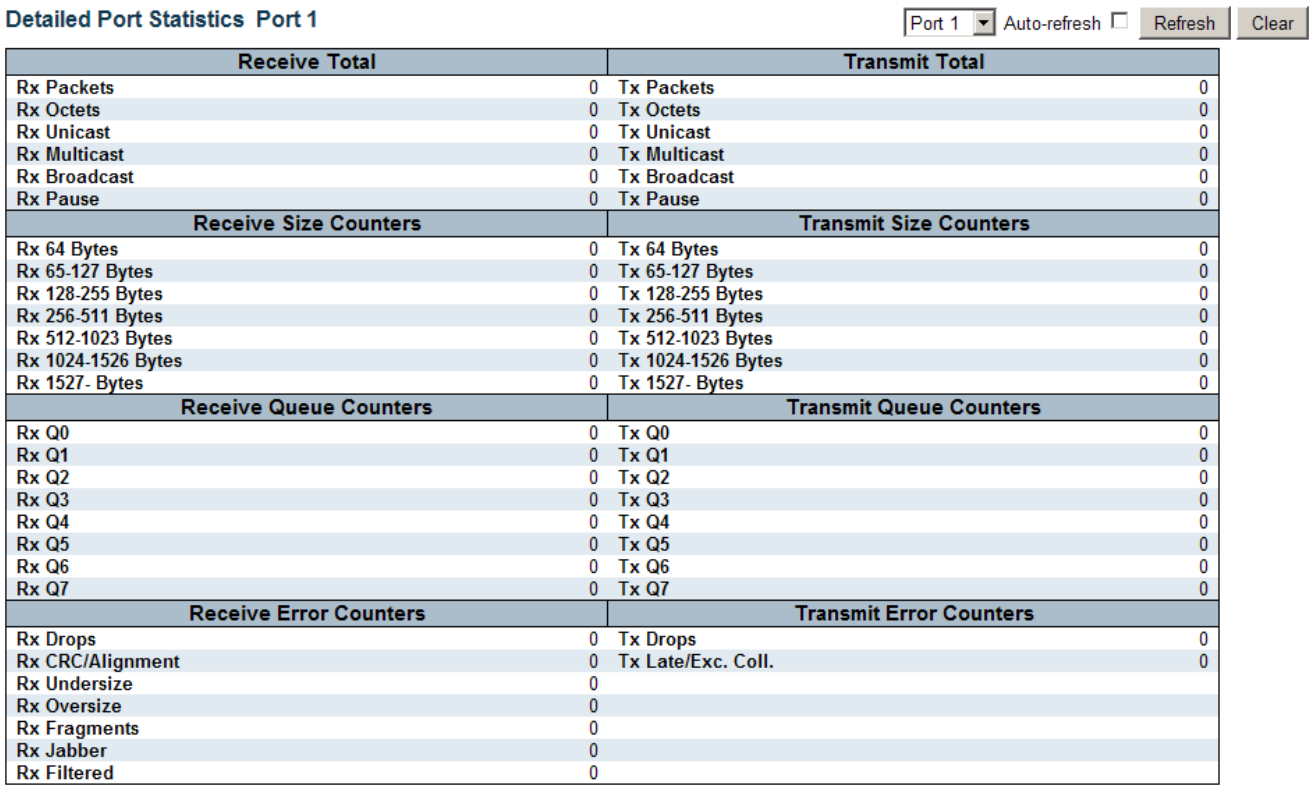
3.3.3 QoS Statistics

Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	110
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	109
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	6290	0	0	0	0	0	0	0	0	0	0	0	0	0	0	336
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	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 Detailed Statistics



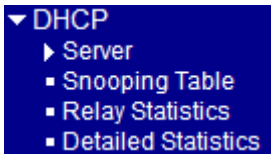
Status	Description
Receive Total and Transmit Total	
Rx and Tx Packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	The number of received and transmitted (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.

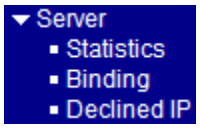
Transmit Error Counters

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 DHCP



3.4.1 Server



3.4.1.1 Statistics

DHCP Server Statistics

Database Counters

Pool	Excluded IP Address	Declined IP Address
0	0	0

Binding Counters

Automatic Binding	Manual Binding	Expired Binding
0	0	0

DHCP Message Received Counters

DISCOVER	REQUEST	DECLINE	RELEASE	INFORM
0	0	0	0	0

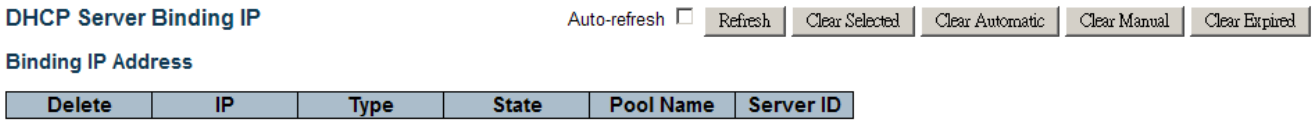
DHCP Message Sent Counters

OFFER	ACK	NAK
0	0	0

Status	Description
Database Counters	**Display counters of various databases.**
Pool	Number of pools.
Excluded IP Address	Number of excluded IP address ranges.
Declined IP Address	Number of seclined IP addresses.
Binding Counters	**Display counters of various databases.**
Automatic Binding	Number of bindings with network-type pools.
Manual Binding	Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.

Expired Binding	Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.
DHCP Message Received Counters	
	Display counters of DHCP messages received by DHCP server.
DISCOVER	Number of DHCP DISCOVER messages received.
REQUEST	Number of DHCP REQUEST messages received.
DECLINE	Number of DHCP DECLINE messages received.
RELEASE	Number of DHCP RELEASE messages received.
INFORM	Number of DHCP INFORM messages received.
DHCP Message Sent Counters	
	Display counters of DHCP messages sent by DHCP server.
OFFER	Number of DHCP OFFER messages sent.
ACK	Number of DHCP ACK messages sent.
NAK	Number of DHCP NAK messages sent.

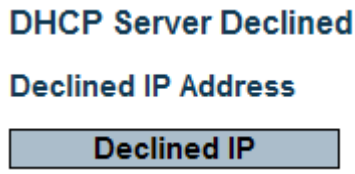
3.4.1.2 Binding



Status	Description
Delete	Check to delete the displayed IP status.
IP	IP address allocated to DHCP client.
Type	Type of binding. Possible types are Automatic, Manual, Expired.
State	State of binding. Possible states are Committed, Allocated, Expired.
Pool Name	The pool that generates the binding.
Server ID	Server IP address to service the binding.
Refresh	Click to refresh the page immediately.
Clear Select	Click to clear selected bindings. If the selected binding is *Automatic* or *Manual*, then it is changed to be Expired. If the selected binding is *Expired*, then it is freed.
Clear Automatic	Click to clear all *Automatic* bindings and change them to *Expired* bindings.
Clear Manual	Click to clear all *Manual* bindings and change them to *Expired* bindings.
Clear Expired	Click to clear all *Expired* bindings and free them.

3.4.1.3 Declined IP

Display IP addresses declined by DHCP clients.



Status	Description
Declined IP	List of IP addresses declined.

3.4.2 Snooping Table

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

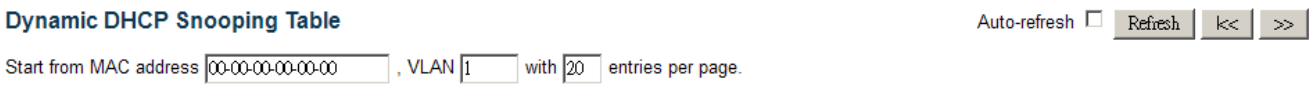
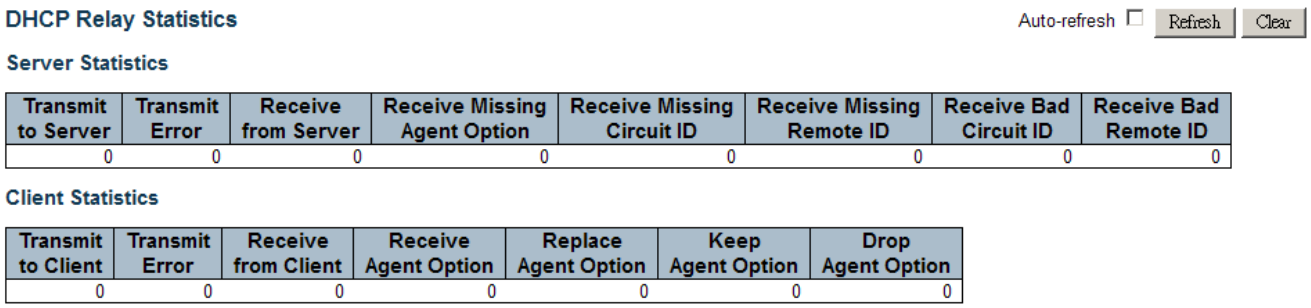


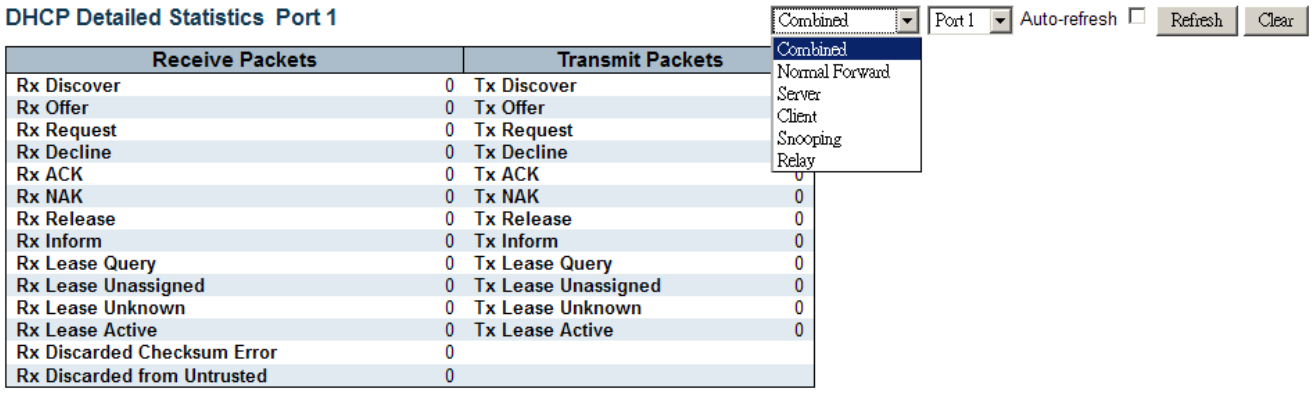
Table Column Status	Description
MAC Address	User MAC address of the entry.
VLAN ID	VLAN-ID in which the DHCP traffic is permitted.
Source Port	Switch Port Number for which the entries are displayed.
IP Address	User IP address of the entry.
IP Subnet Mask	User IP subnet mask of the entry.
DHCP Server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

3.4.3 Relay Statistics



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.

3.4.4 Detailed Statistics



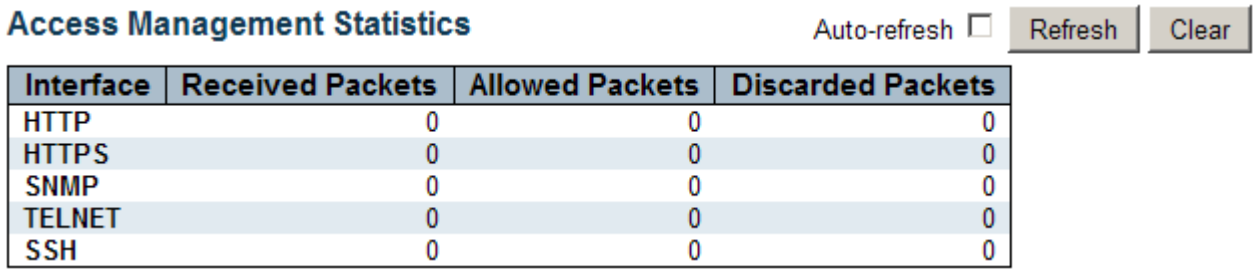
Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

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.
Rx Discarded checksum error	The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted	The number of discarded packet that are coming from untrusted port.

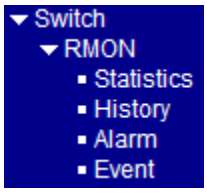
3.5 Security

3.5.1 Access Management Statistics

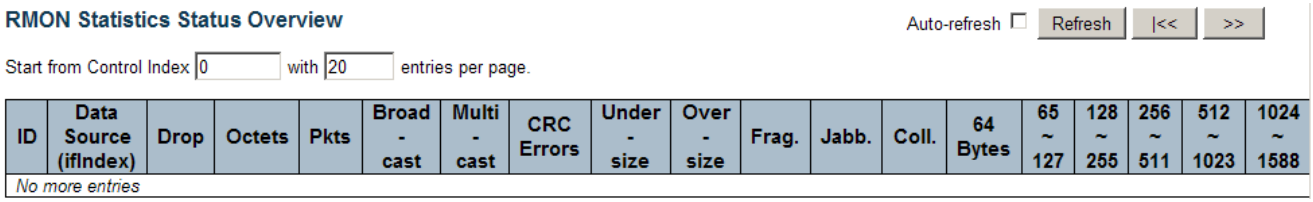


Status	Description
Interface	The interface type through which the remote host can access the switch.
Received Packets	Number of received packets from the interface when access management mode is enabled
Allowed Packets	Number of allowed packets from the interface when access management mode is enabled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

3.5.2 Switch – RMON



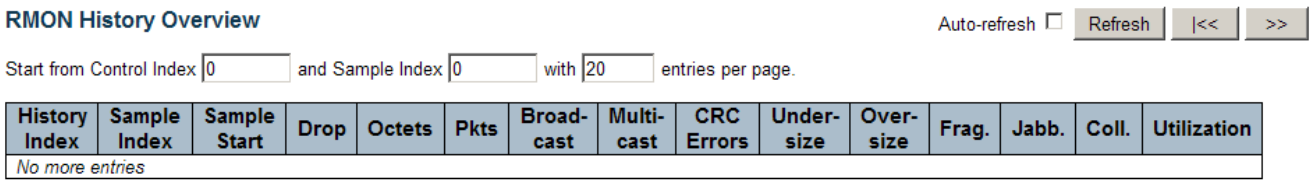
3.5.2.1 Statistics



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.

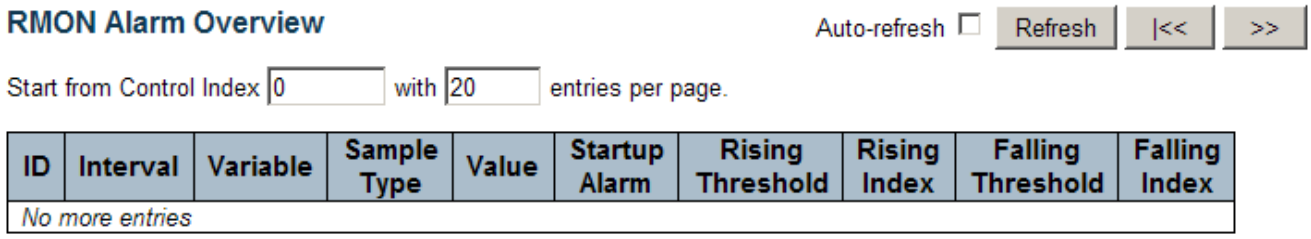
3.5.2.2 History



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.

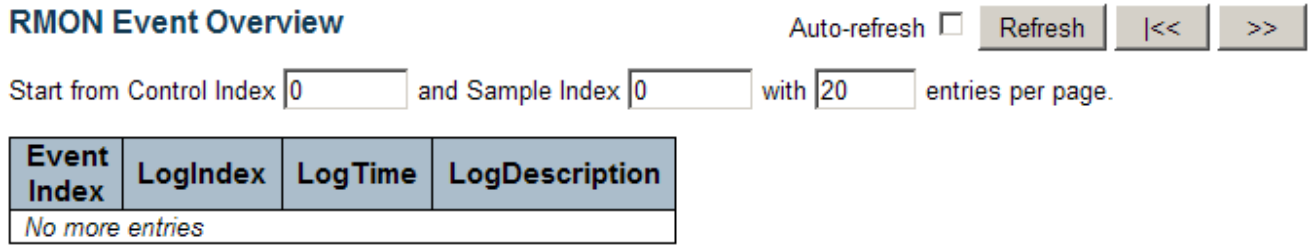
Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in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

3.5.2.3 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.

3.5.2.4 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.

3.5.3 Network

3.5.3.1 Port Security

3.5.3.1.1 Switch

Port Security Switch Status

User Module Legend

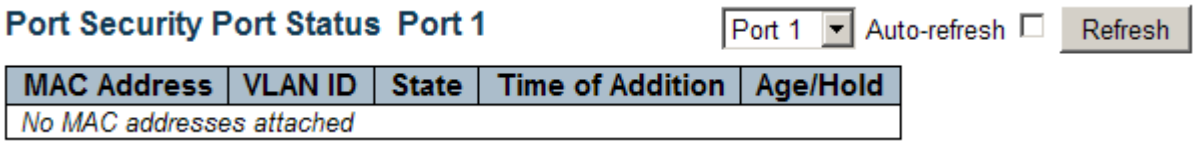
User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	---	Disabled	-	-
5	---	Disabled	-	-
6	---	Disabled	-	-
7	---	Disabled	-	-
8	---	Disabled	-	-
9	---	Disabled	-	-
10	---	Disabled	-	-
11	---	Disabled	-	-
12	---	Disabled	-	-
13	---	Disabled	-	-
14	---	Disabled	-	-
15	---	Disabled	-	-
16	---	Disabled	-	-
17	---	Disabled	-	-
18	---	Disabled	-	-
19	---	Disabled	-	-
20	---	Disabled	-	-
21	---	Disabled	-	-
22	---	Disabled	-	-
23	---	Disabled	-	-
24	---	Disabled	-	-

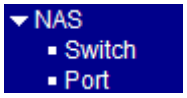
Status	Description
User Module Legend	The legend shows all user modules that may request Port Security services.
User Module Name	The full name of a module that may request Port Security services.
Abbr	A one-letter abbreviation of the user module. This is used in the Users column in the port status table.
Port Status	The table has one row for each port on the switch 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 (-).

3.5.3.1.2 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.

3.5.3.2 NAS



3.5.3.2.1 Switch

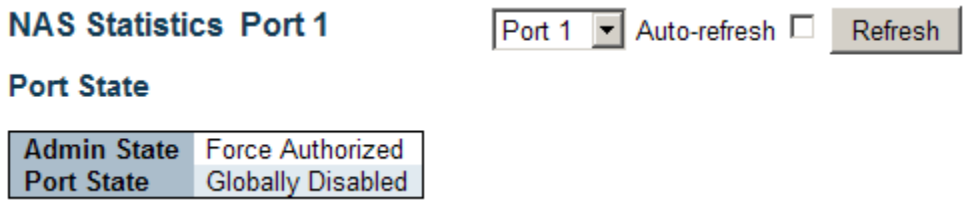
Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	
9	Force Authorized	Globally Disabled			-	
10	Force Authorized	Globally Disabled			-	
11	Force Authorized	Globally Disabled			-	
12	Force Authorized	Globally Disabled			-	
13	Force Authorized	Globally Disabled			-	
14	Force Authorized	Globally Disabled			-	
15	Force Authorized	Globally Disabled			-	
16	Force Authorized	Globally Disabled			-	
17	Force Authorized	Globally Disabled			-	
18	Force Authorized	Globally Disabled			-	
19	Force Authorized	Globally Disabled			-	
20	Force Authorized	Globally Disabled			-	
21	Force Authorized	Globally Disabled			-	
22	Force Authorized	Globally Disabled			-	
23	Force Authorized	Globally Disabled			-	
24	Force Authorized	Globally Disabled			-	

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

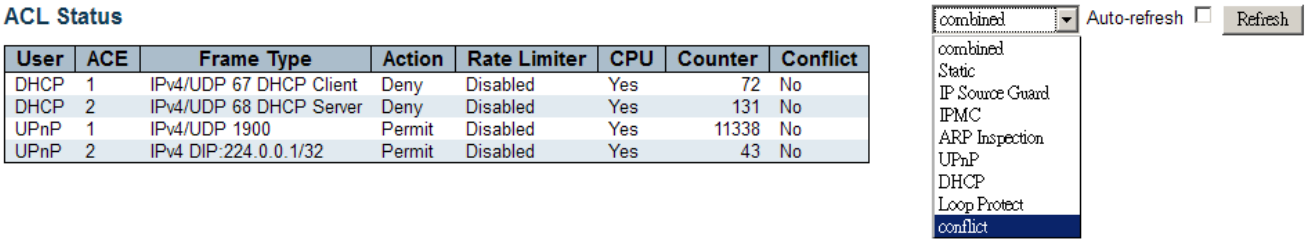
	authentication.
QoS Class	QoS Class assigned to the port by the RADIUS server if enabled.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN 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.

3.5.3.2.2 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.

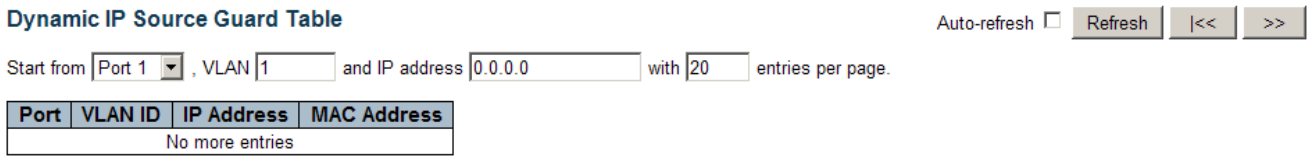
3.5.3.3 ACL Status



Status	Description
User	Indicates the ACL user.
ACE	Indicates the ACE ID on local switch.
Frame Type	Indicates the frame type of the ACE. Possible values are: *Any*: The ACE will match any frame type. *EType*: The ACE will match Ethernet Type frames. Note that an Ethernet Type based *ACE* will not get matched by IP and ARP frames.

	ARP: The ACE will match ARP/RARP frames. *IPv4*: The ACE will match all IPv4 frames. *IPv4/ICMP*: The ACE will match IPv4 frames with ICMP protocol. *IPv4/UDP*: The ACE will match IPv4 frames with UDP protocol. *IPv4/TCP*: The ACE will match IPv4 frames with TCP protocol. *IPv4/Other*: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. *IPv6*: The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. *Permit*: Frames matching the ACE may be forwarded and learned. *Deny*: Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When *Disabled* is displayed, the rate limiter operation is disabled.
CPU	Forward packet that matched the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Conflict	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

3.5.3.4 IP Source Guard

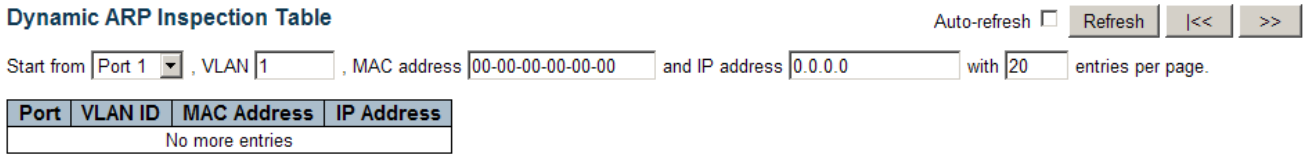


The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

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.

3.5.3.5 ARP Inspection

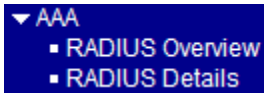


The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

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.

3.5.4 AAA



3.5.4.1 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

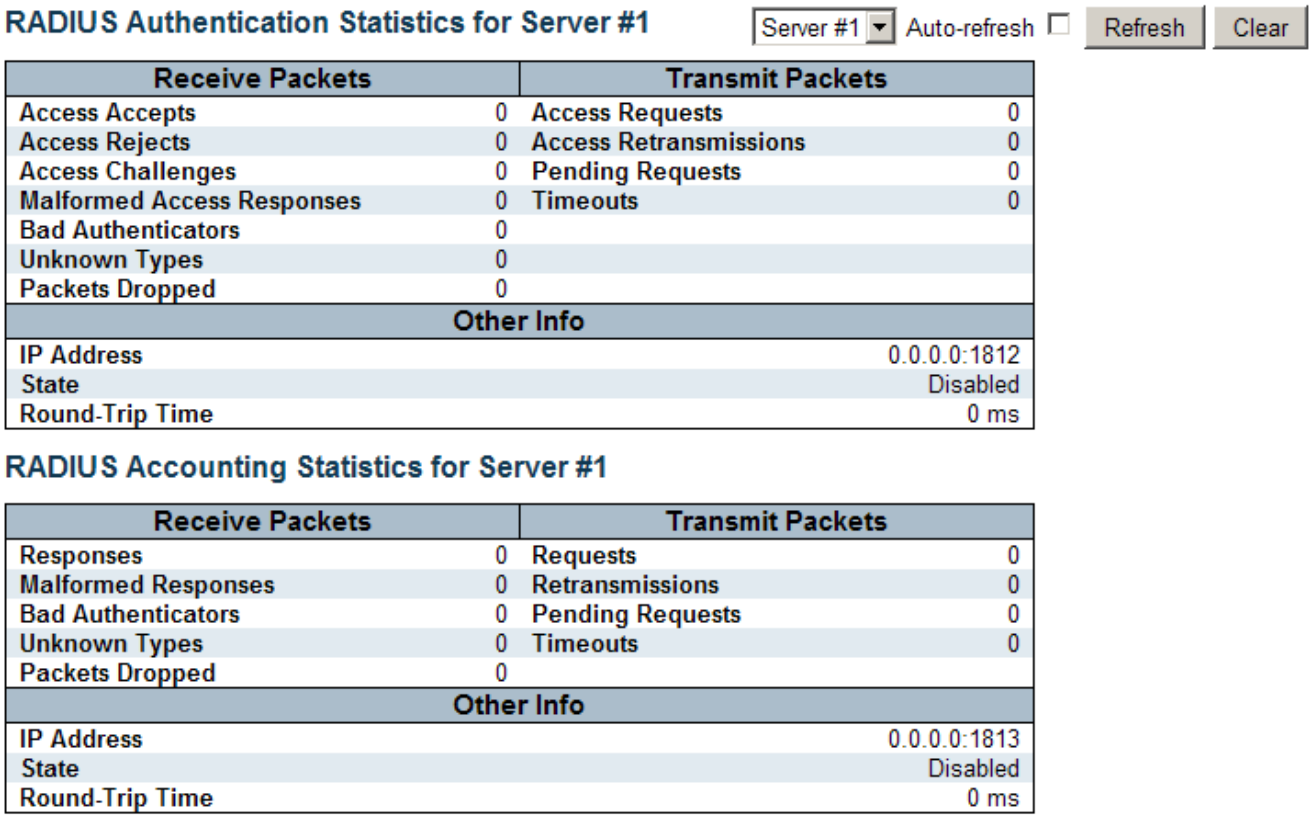
RADIUS Accounting Server Status Overview

#	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.

3.5.4.2 RADIUS Details



Server #1	Selects a RADIUS server to display.

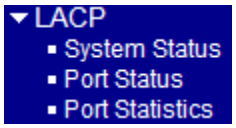
Authentication Server	Description
Server #	Select a RADIUS server number.
Rx Access Accepts	RFC4670 name: radiusAuthClientExtAccessAccepts The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx Access Rejects	RFC4670 name: radiusAuthClientExtAccessRejects The number 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.

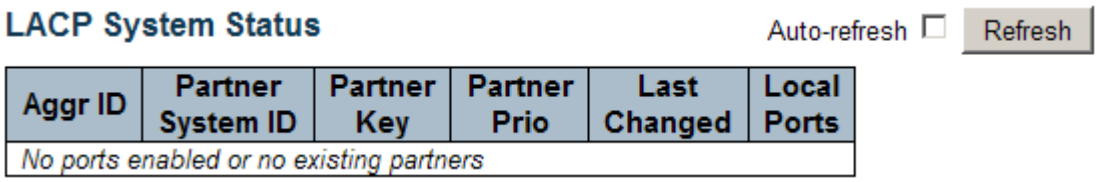
Accounting Server	**Description**
Rx Responses	RFC4670 name: radiusAccClientExtResponses The number of RADIUS packets (valid or invalid) received from the server.
Rx Malformed Responses	RFC4670 name: radiusAccClientExtMalformedResponses The number of malformed RADIUS packets received from the server. 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.

3.6 LACP



3.6.1 System Status



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".

3.6.2 Port Status

LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-
11	No	-	-	-	-	-
12	No	-	-	-	-	-
13	No	-	-	-	-	-
14	No	-	-	-	-	-
15	No	-	-	-	-	-
16	No	-	-	-	-	-
17	No	-	-	-	-	-
18	No	-	-	-	-	-
19	No	-	-	-	-	-
20	No	-	-	-	-	-
21	No	-	-	-	-	-
22	No	-	-	-	-	-
23	No	-	-	-	-	-
24	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.

3.6.3 Port Statistics

LACP 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
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	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.

3.7 Loop Protection

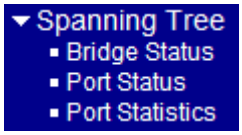
Loop Protection Status

Auto-refresh ☐ Refresh

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

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.

3.8 Spanning Tree



3.8.1 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.

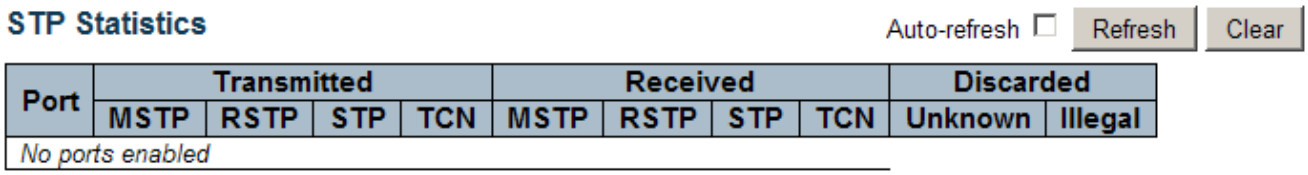
3.8.2 Port Status

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-
13	Non-STP	Forwarding	-
14	Non-STP	Forwarding	-
15	Non-STP	Forwarding	-
16	Non-STP	Forwarding	-
17	Non-STP	Forwarding	-
18	Non-STP	Forwarding	-
19	Non-STP	Forwarding	-
20	Non-STP	Forwarding	-
21	Non-STP	Forwarding	-
22	Non-STP	Forwarding	-
23	Non-STP	Forwarding	-
24	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.

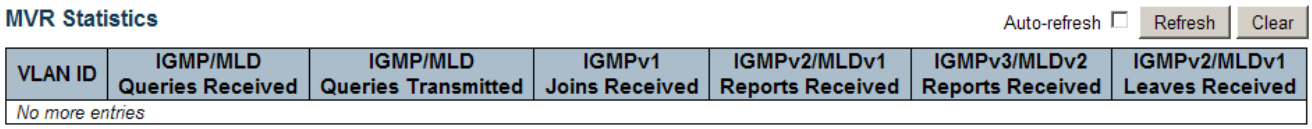
3.8.3 Port Statistics



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.

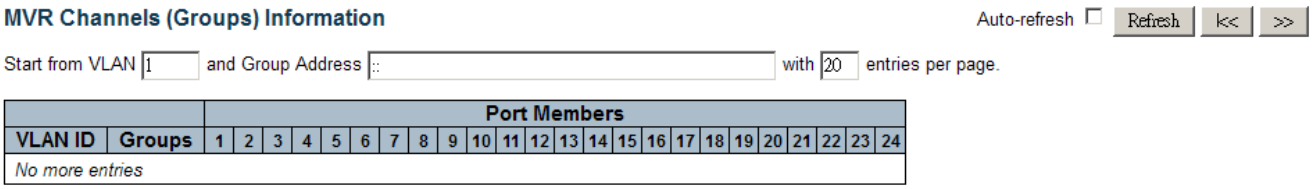
3.9 MVR

3.9.1 Statistics



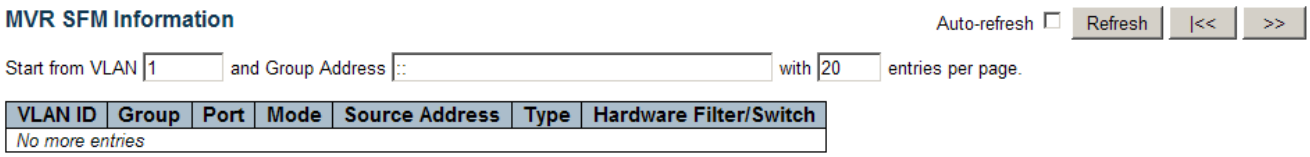
Status	Description
VLAN ID	The Multicast VLAN ID.
IGMP/MLD Queries Received	The number of Received Queries for IGMP and MLD, respectively.
IGMP/MLD Queries Transmitted	The number of Transmitted Queries for IGMP and MLD, respectively.
IGMPv1 Joins Received	The number of Received IGMPv1 Join's.
IGMPv2/MLDv1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

3.9.2 MVR Channel Groups



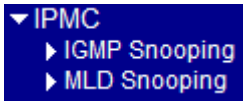
Status	Description
VLAN ID	VLAN ID of the group.
Groups	Group ID of the group displayed.
Port Members	Ports under this group.

3.9.3 MVR SFM Information

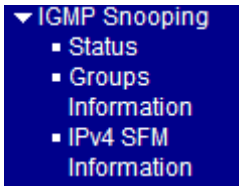


Status	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either *Include* or *Exclude*.
Source Address	IP Address of the source. Currently, 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.

3.10 IPMC



3.10.1 IGMP Snooping



3.10.1.1 Status

IGMP Snooping Status

Auto-refresh ☐ Refresh Clear

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

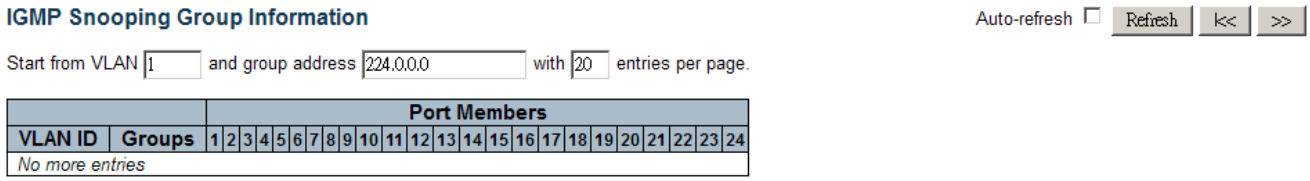
Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-
21	-
22	-
23	-
24	-

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.

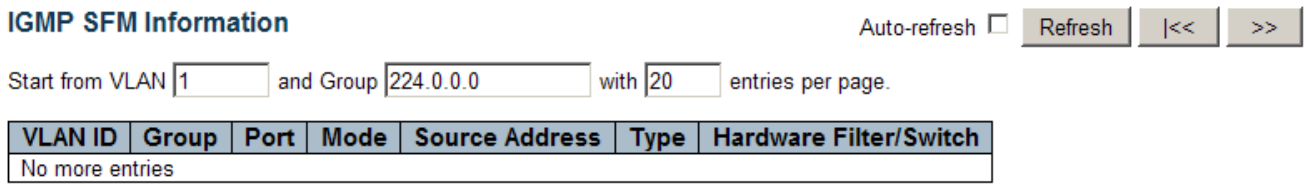
Queries Received	The number of Received Queries.
V1 Reports Received	The number of Received V1 Reports.
V2 Reports Received	The number of Received V2 Reports.
V3 Reports Received	The number of Received V3 Reports.
V2 Leaves Received	The number of Received V2 Leaves.
Router Port	Display which ports act 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.

3.10.1.2 Groups Information



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

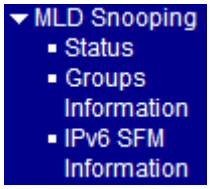
3.10.1.3 IPv4 SFM Information



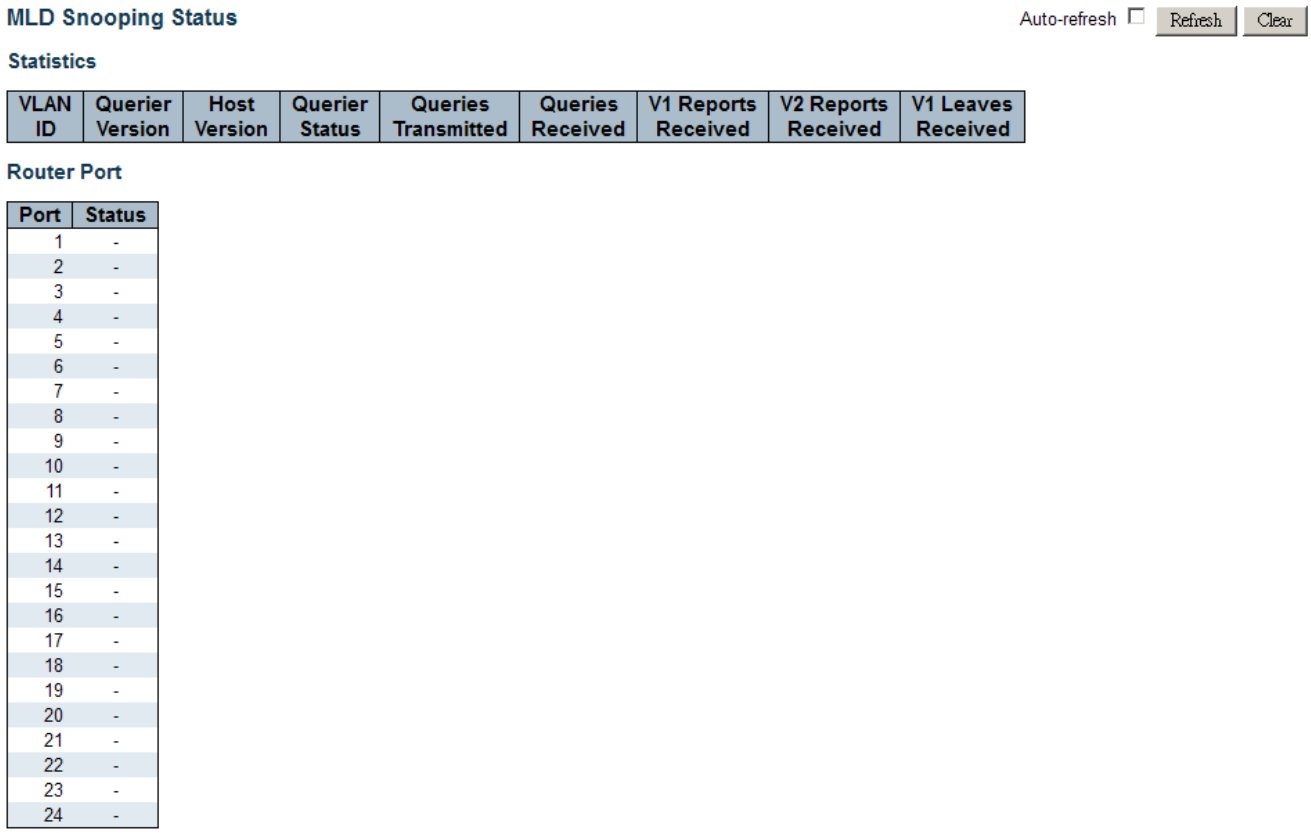
Status	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either *Include* or *Exclude*.
Source Address	IP Address of the source. Currently, 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.

3.10.2 MLD Snooping



3.10.2.1 Status



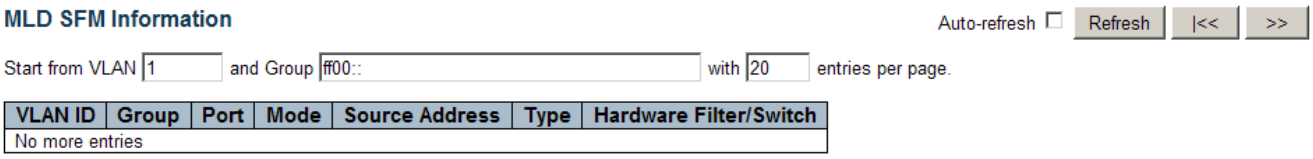
Status	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Shows the Querier status is ***ACTIVE*** or ***IDLE***. "***DISABLE***" denotes the specific interface is administratively disabled.

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.

3.10.2.2 Groups Information

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

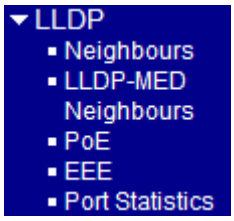
3.10.2.3 IPv6 SFM Information



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.

3.11 LLDP

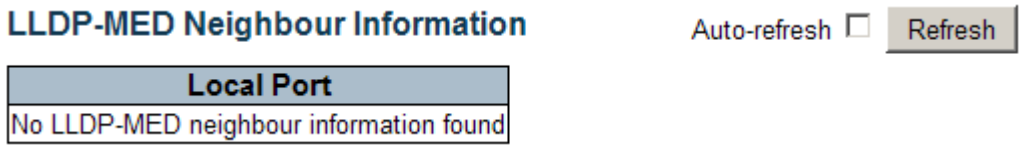


3.11.1 Neighbours

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.

3.11.2 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.

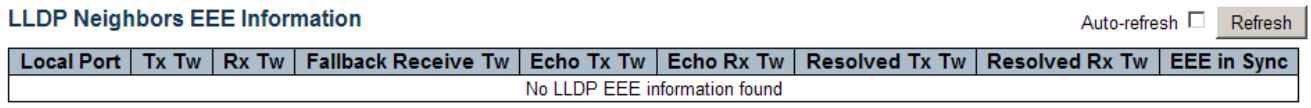
Discovery services defined in this class include media-type-specific network layer policy discovery.

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.

3.11.3 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.

3.11.4 Port Statistics

LLDP Global Counters

Auto-refresh ☐ Refresh Clear

Global Counters	
Neighbor entries were last changed	1970-01-01T00:00:00+00:00 (814 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local 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
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	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.

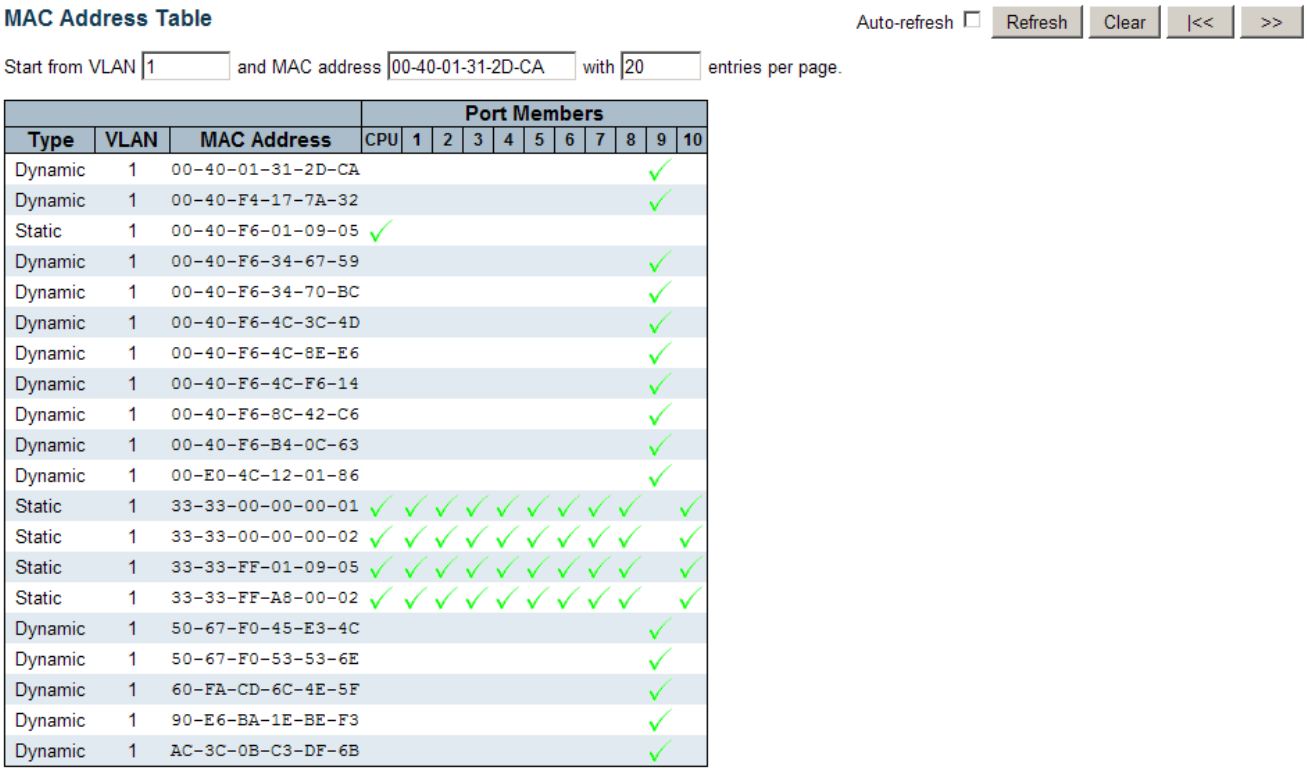
Total Neighbours Entries Aged Out

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.

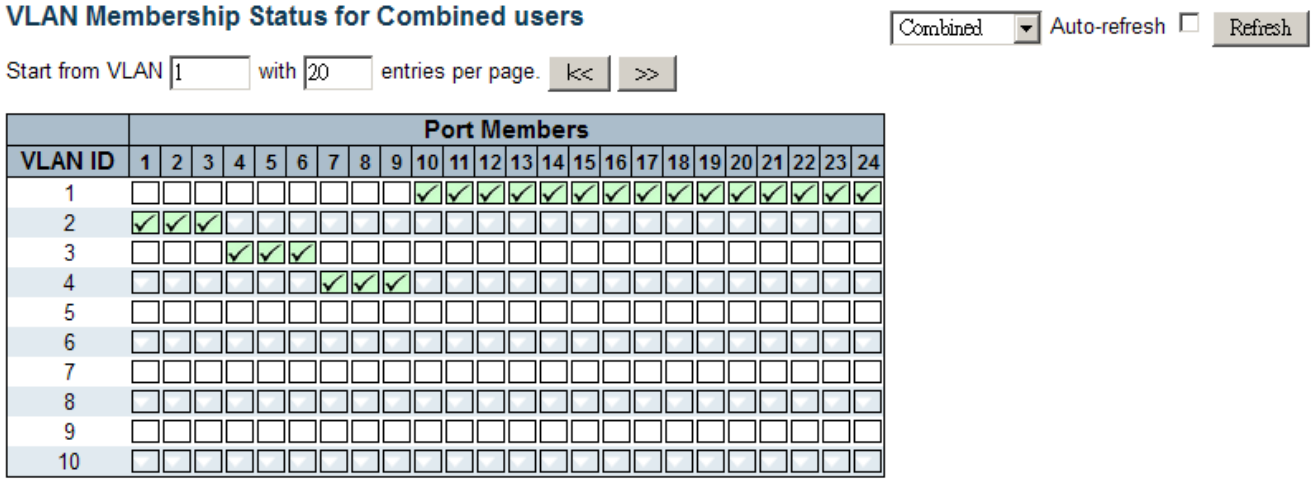
3.12 MAC Table



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.

3.13 VLANs

3.13.1 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 .

3.13.2 Ports

VLAN Port Status for Combined users

Combined | Auto-refresh | Refresh

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Egress Tag Insert Rule	Untagged VLAN ID	Conflicts
1	Unaware		All	2	No PVID		No
2	C-Port		All	2	No PVID		No
3	C-Port		All	2	No PVID		No
4	C-Port		All	3	No PVID		No
5	C-Port		All	3	No PVID		No
6	C-Port		All	3	No PVID		No
7	C-Port		All	4	No PVID		No
8	C-Port		All	4	No PVID		No
9	C-Port		All	4	No PVID		No
10	C-Port		All	1	No PVID		No
11	C-Port		All	1	No PVID		No
12	C-Port		All	1	No PVID		No
13	C-Port		All	1	No PVID		No
14	C-Port		All	1	No PVID		No
15	C-Port		All	1	No PVID		No
16	C-Port		All	1	No PVID		No
17	C-Port		All	1	No PVID		No
18	C-Port		All	1	No PVID		No
19	C-Port		All	1	No PVID		No
20	C-Port		All	1	No PVID		No
21	C-Port		All	1	No PVID		No
22	C-Port		All	1	No PVID		No
23	C-Port		All	1	No PVID		No
24	C-Port		All	1	No PVID		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.

3.14 sFlow

sFlow Statistics

Auto-refresh ☐ Refresh | Clear Receiver | Clear Ports

Receiver Statistics

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics

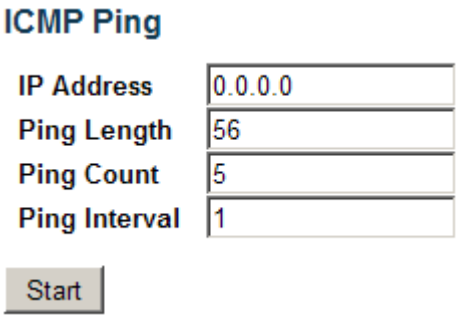
Port	Rx Flow Samples	Tx Flow Samples	Counter Samples
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0
9	0	0	0
10	0	0	0
11	0	0	0
12	0	0	0
13	0	0	0
14	0	0	0
15	0	0	0
16	0	0	0
17	0	0	0
18	0	0	0
19	0	0	0
20	0	0	0
21	0	0	0
22	0	0	0
23	0	0	0
24	0	0	0

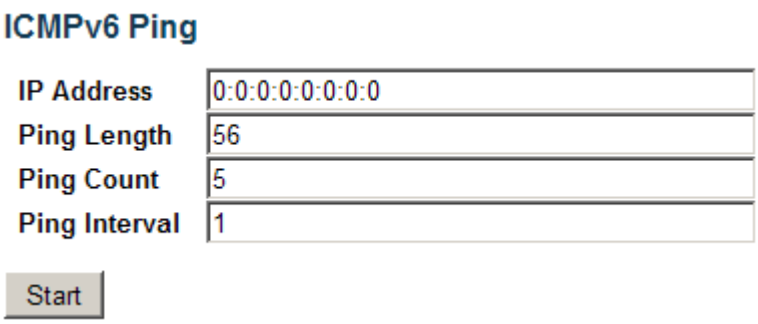
Status	Description
Owner	This field shows the current owner of the sFlow configuration. It assumes one of three values as follows: • If sFlow is currently unconfigured/unclaimed, Owner contains <none>. • If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>. • 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

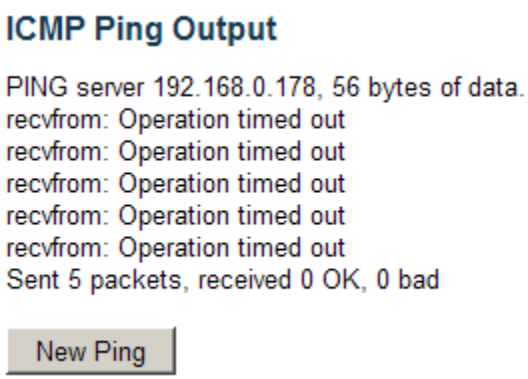
4.1 Ping & Ping6



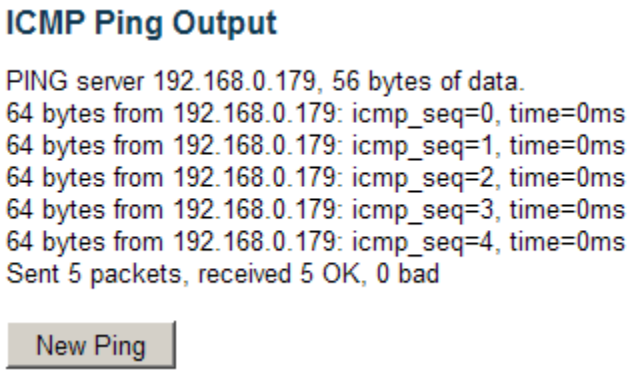


Settings	Description
IP Address	The destination IP Address.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second 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.

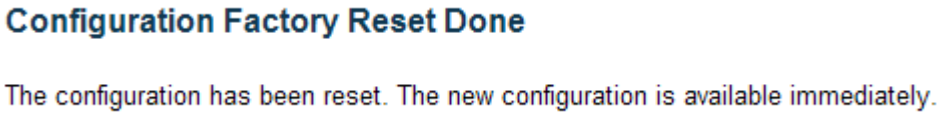
5. Maintenance

5.1 Reset 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

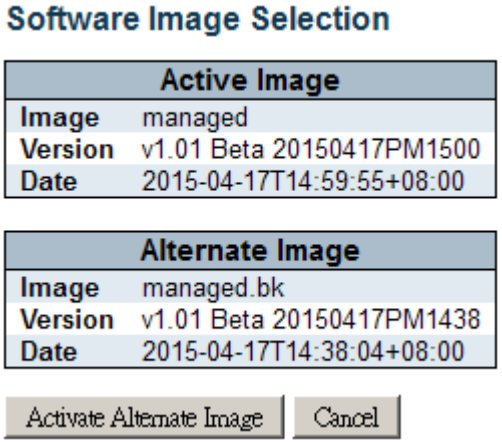
This page facilitates an update of the firmware controlling the switch.

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



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:

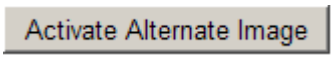
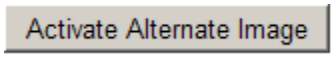
1. *In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the*  *button is also disabled.*
2. *If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device 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.

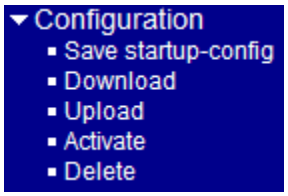


Click to use the alternate image. This button may be disabled depending on system state.

Cancel

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

5.4 Configuration



5.4.1 Save startup-config

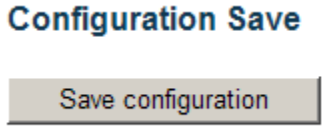
This copies *running-config* to *startup-config*, therefore ensures that the currently active configuration will be used at the next reboot.

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.

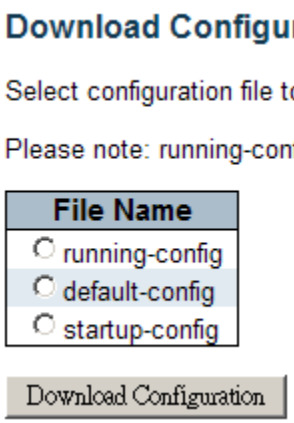
```
<?xml version="1.0"?>
<configuration>
  <platform>
    <pid val="3"></pid>
    <version val="1"></version>
  </platform>
  <global>
    <mac>
      <age val="200"></age>>
    </mac>
  </global>
  <switch sid="1">
    <mac>
      <entry port="1-24" learn_mode="auto"></entry>
    </mac>
```

```
  </switch>
</configuration>
```



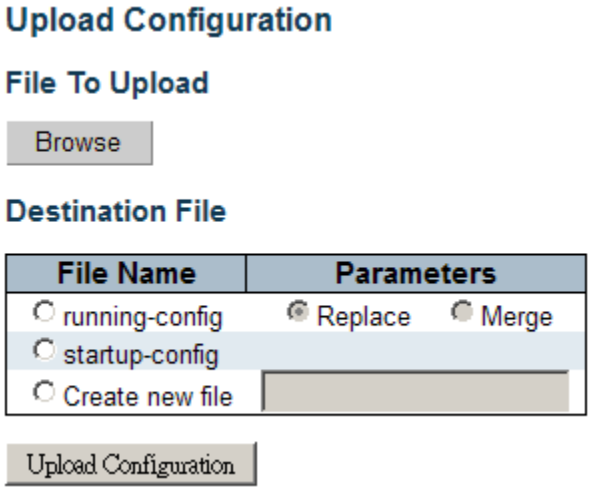
Save configuration	Click to start download of the configuration.

5.4.2 Download



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

5.4.3 Upload



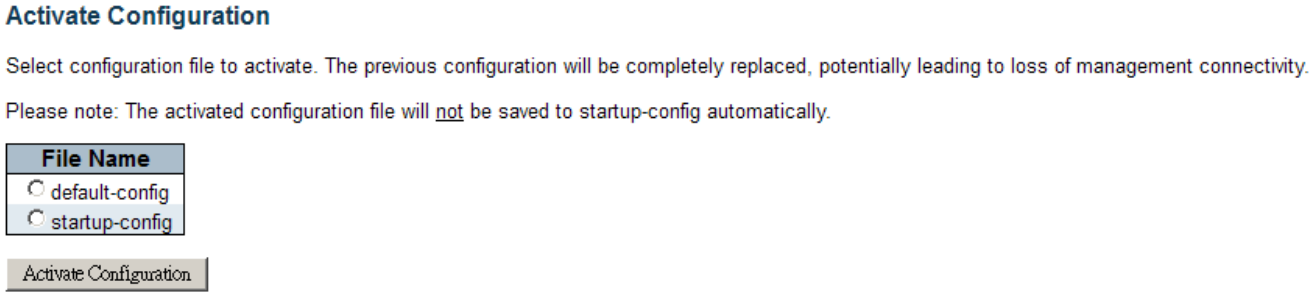
It is possible to upload a file from the web browser to all the files on the switch, except *default-config*, which is read-only. Select the file to upload, select the destination file on the target, then click Upload Configuration. If the destination is *running-config*, the file will be applied to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

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

If the file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

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

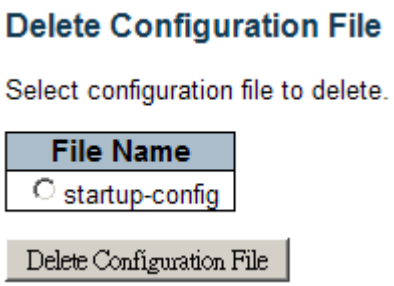
5.4.4 Activate



It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration. Select the file to activate and click Activate Configuration. This

will initiate the process of completely replacing the existing configuration with that of the selected file.

5.4.5 Delete



It is possible to delete any of the writable files stored in flash, including *startup-config*. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.

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.

G

GVRP

Generic VLAN Registration Protocol, or GVRP for short is specified in IEEE 802.1Q-2005, clause 11 and IEEE 802.1D.2004, clause 12.

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.