SICOM3008PN Managed Industrial Ethernet Switch Web Operation Manual

Publication Date: Oct. 2018

Version: V1.1

KYLAND

Disclaimer:

Kyland Technology Co., Ltd. tries to keep the content of this manual as accurate and as updated as possible. This document is not guaranteed to be error-free, and we reserve the right to amend it without notice to users.

Website: http://www.kyland.com

FAX: +86-10-88796678

Email:support@kyland.com

Contents

Preface

Scope

This document provides an overview on SICOM3008PN Managed Industrial Ethernet Switch

Safety Instructions

When a connector is removed during installation, testing, or servicing, or when an energized fiber is broken, a risk of ocular exposure to optical energy that may be potentially hazardous occurs, depending on the laser output power.

The primary hazards of exposure to laser radiation from an optical-fiber communication system are:

Damage to the eye by accidental exposure to a beam emitted by a laser source.

Damage to the eye from viewing a connector attached to a broken fiber or an energized fiber.

Documentation Conventions

The following conventions are used in this manual to emphasize information that will be of interest to the reader.

Symbol	Explanation
Caution	The matters need attention during the operation and configuration, and they are supplement to the operation description.
Note	Necessary explanations to the operation description.
Warning	The matters call for special attention. Incorrect operation might cause data loss or damage to devices.

Document Obtainment

Product documents can be obtained by:

- CD shipped with the device
- Kyland website: www.kyland.com

1 Product Introduction

1.1 Overview

Managed video surveillance SICOM3008PN Industrial Ethernet Switch applied in the ITS, highway, industrial automation, oil&gas and many other industries. The SICOM3008PN are applicable to harsh and hazardous industrial environments due to its high-performance switching engine, solid closed housing, fanless but heat dissipation-capable single-rib shaped chassis, overcurrent, overvoltage, and EMC protection for power input, and EMC protection of RJ45 ports. The redundant network and power input support guarantees the reliable operation of the system.

The SICOM3008PN provide powerful network management functions. The device can be managed through CLI, Telnet, Web.

1.2 Software Features

This series switches provide abundant software features, satisfying customers' various requirements.

- Redundancy protocols: STP, RSTP, MSTP, Static trunk or Dynamic via LACP (Link Aggregation Control Protocol)
- Multicast protocols: IGMP v1, v2, IGMP snooping and querying, Immediate leave and leave proxy, Throttling and filtering
- Switching attributes: VLAN, QoS
- Security: IP and MAC-based access control, IEEE 802.1X authentication Network Access Control, Multicast/Broadcast/Flooding Storm Control
- Device management: Configuration Import/Export, Firmware Upgrade
- Device diagnosis: port mirroring, LLDP
- Network management: management by CLI, Telnet, Web, HTTPs, SSH, DHCP, and SNMPv1/v2c
- …

2 Switch Access

You can access the switch by:

- Console port
- Telnet/SSH
- Web browser

For details, refer to its user manual.

2.1 Access through Console Port

You can access a switch by its console port and the hyper terminal of Windows OS or other software that supports serial port connection, such as HTT3.3. The following example shows how to use Hyper Terminal to access switch by console port.

1. Connect the 9-pin serial port of a PC to the console port of the switch with the DB9-RJ45 console cable.

2. Run the Hyper Terminal in Windows desktop. Click [Start] → [All Programs] → [Accessories] → [Communications] → [Hyper Terminal], as shown in Figure 1.

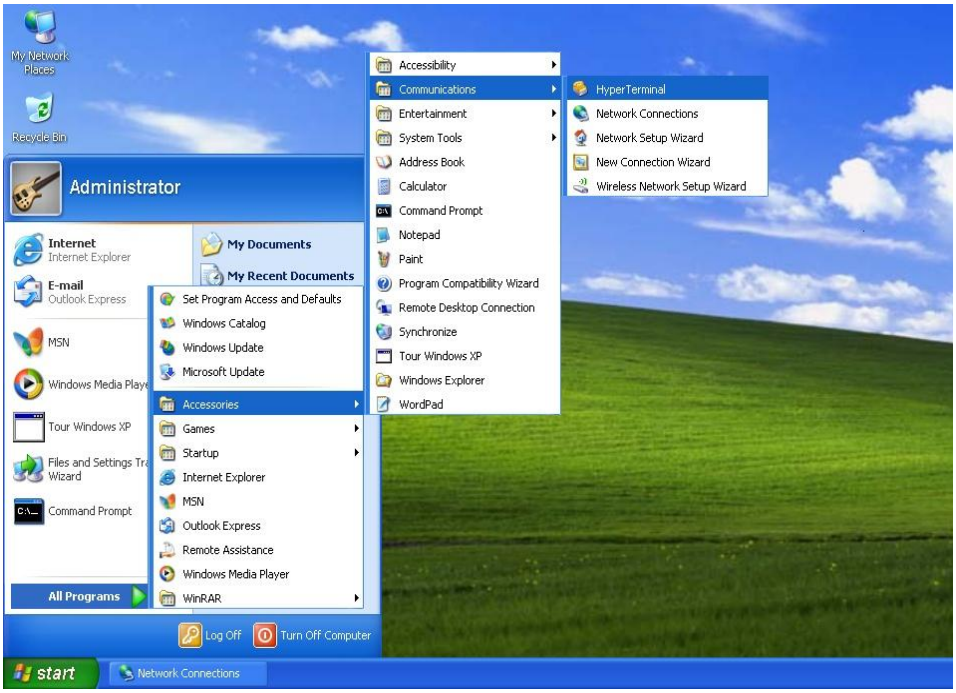


Figure 1 Starting the Hyper Terminal

3. Create a new connection "Switch", as shown in Figure 2.

Figure 2 Creating a New Connection

4. Connect the communication port in use, as shown in Figure 3.

Figure 3 Selecting the Communication Port

Note:

To confirm the communication port in use, right-click [My Computer] and click [Property] → [Hardware] → [Device Manager] → [Port].

5. Set port parameters (Bits per second: 115200, Data bits: 8, Parity: None, Stop bits: 1, and

Flow control: None), as shown in Figure 4.

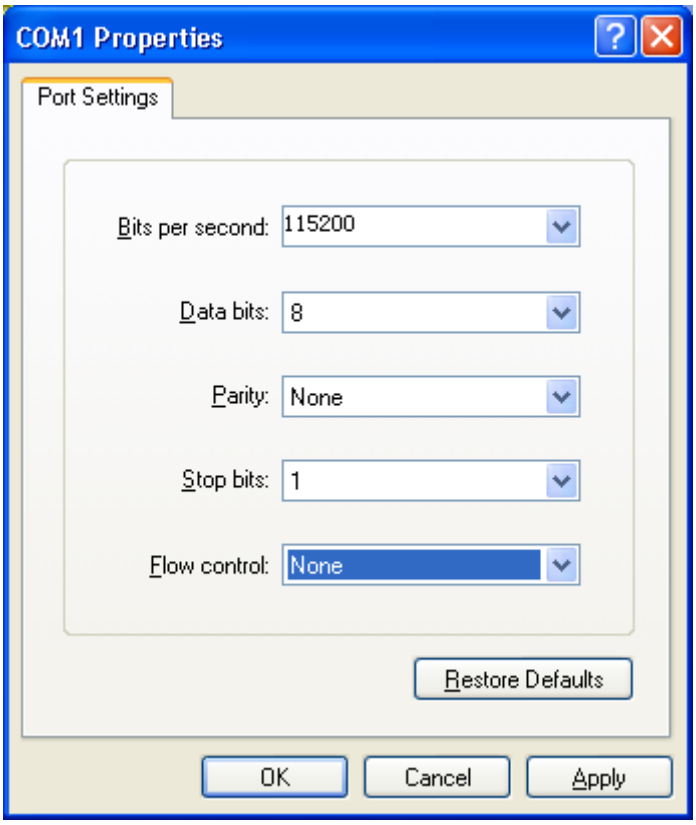


Figure 4 Setting Port Parameters

6. Click <OK> button to enter the switch CLI. Input password "admin" and press <Enter> to enter the General mode, as shown in Figure 5.

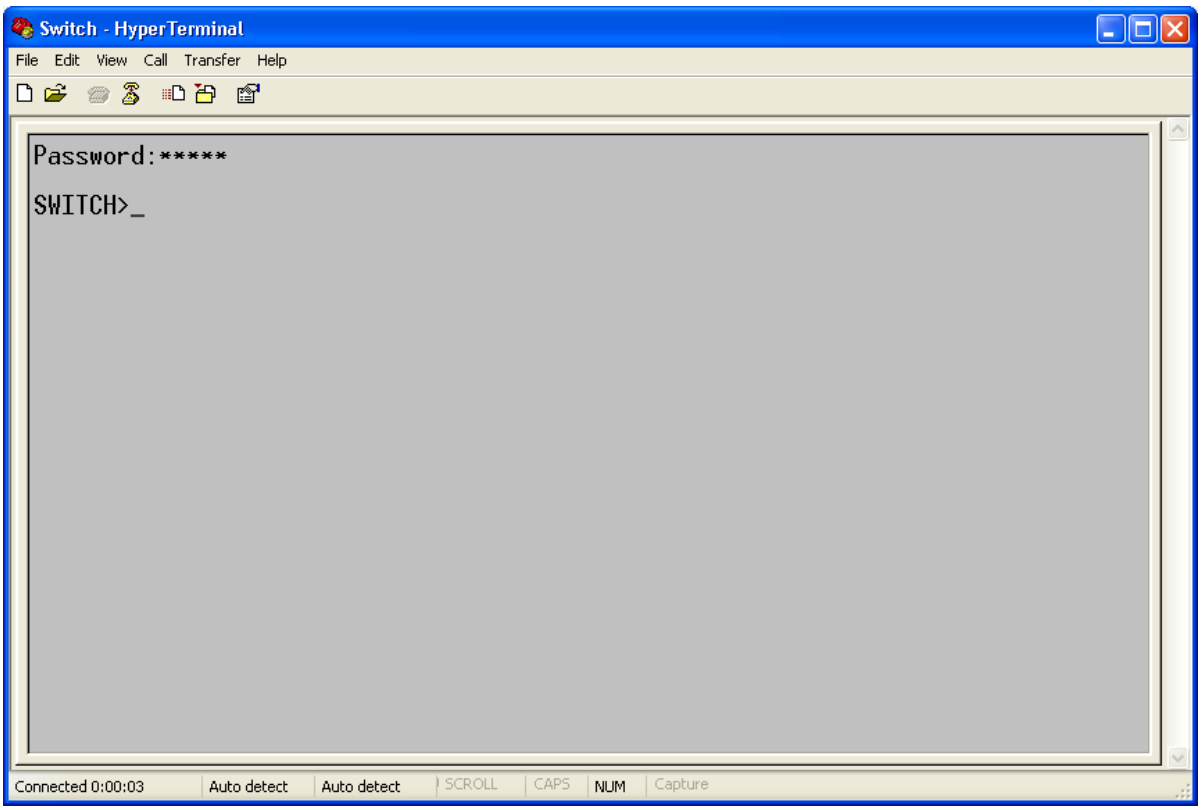


Figure 5 CLI

7. Input command “enable”, default user "admin”, and password “none” to enter the privileged mode. You can also input other created users and password, as shown in Figure 6.

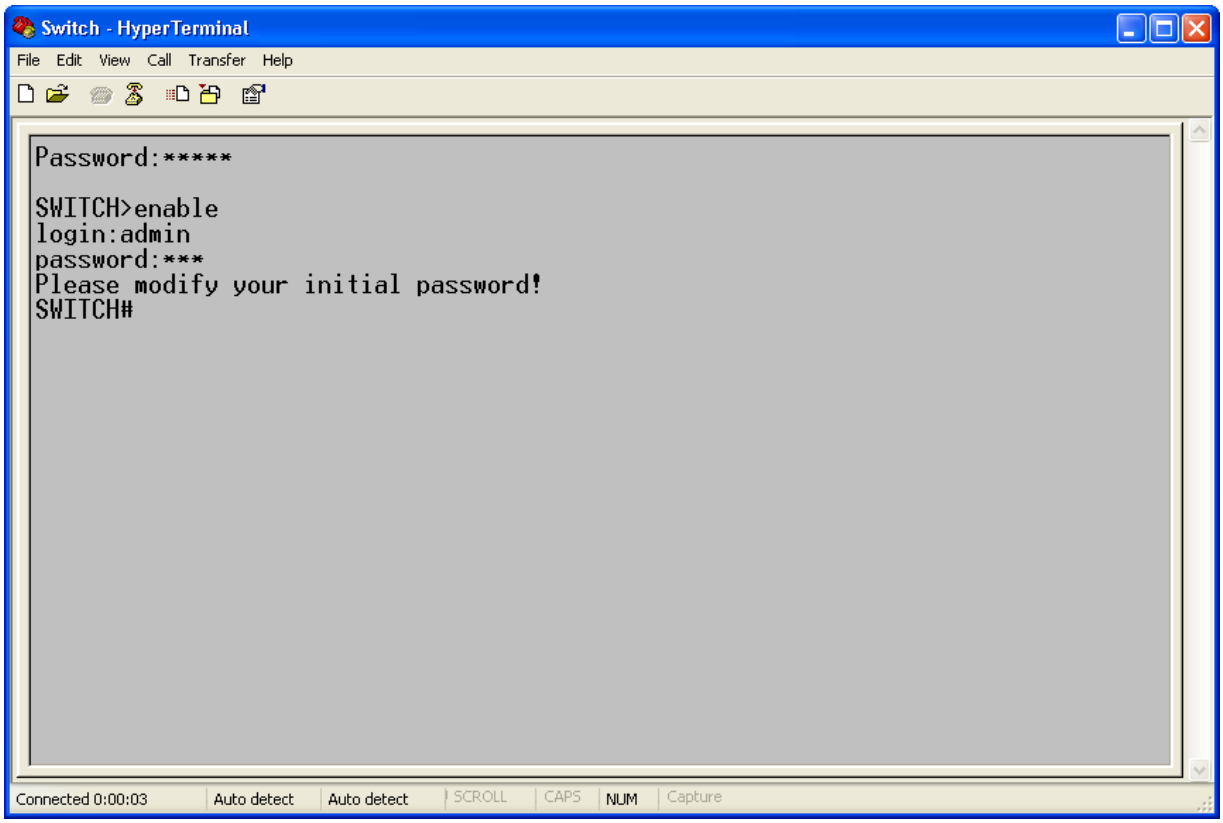


Figure 6 Privileged mode

2.2 Access through Telnet

The precondition for accessing a switch by Telnet is the normal communication between the PC and the switch.

1. Enter "**telnet** *IP address*" in the Run dialog box, as shown in Figure 7. The default IP address of a Kyland switch is 192.168.0.2.

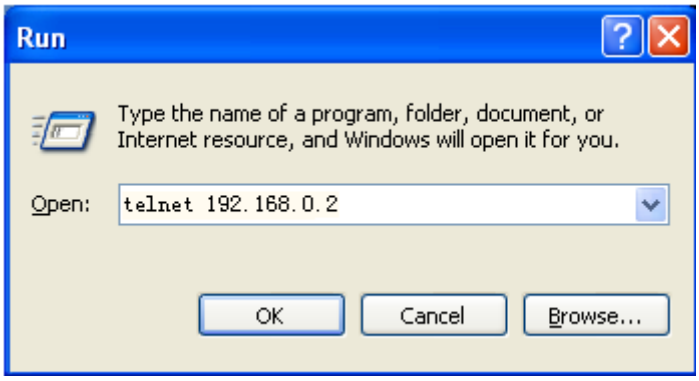


Figure 7 Telnet Access

2. In the Telnet interface, input user "admin", and password "none" to log in to the switch. You can also input other created users and password, as shown in Figure 8.

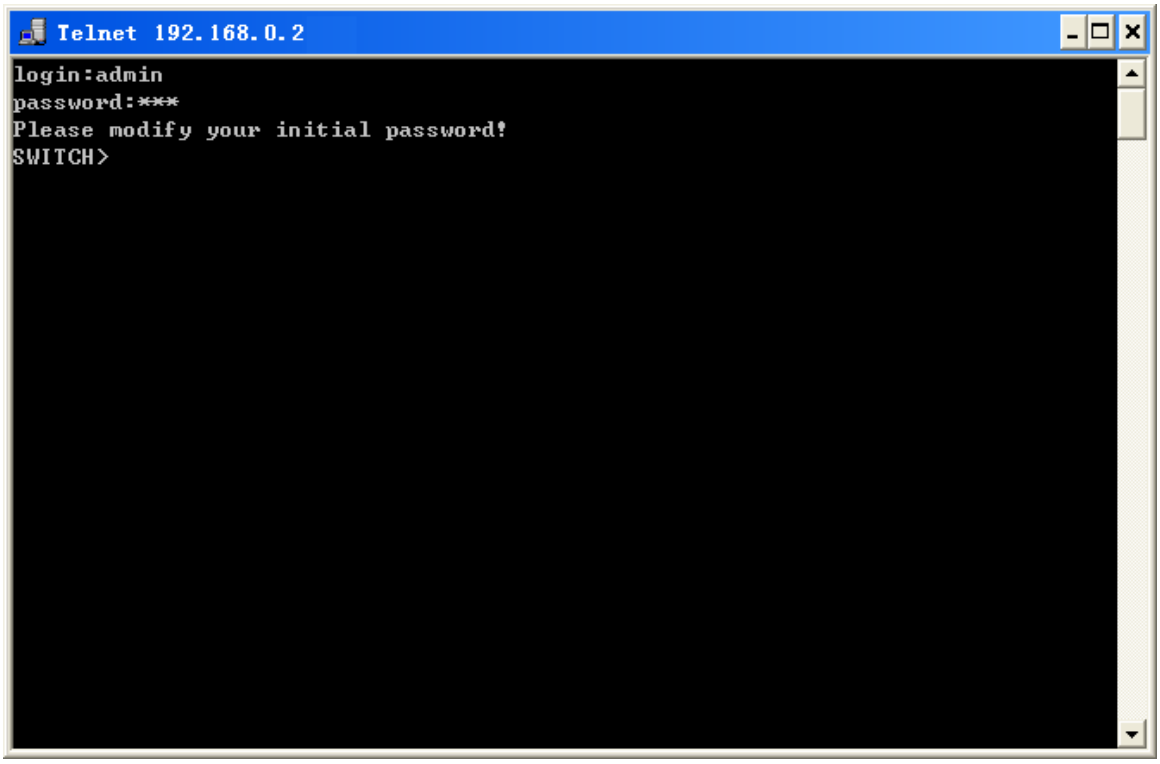


Figure 8 Telnet Interface

2.3 Access through Web

The precondition for accessing a switch by Web is the normal communication between the PC and the switch.

Note:

IE8.0 or a later version is recommended for the best Web display results.

1. Input "*IP address*" in the browser address bar. The login interface is displayed, as shown below. Input the default user name "admin", password "none", and the Verification. Click <Login>. You can also input other created users and password.

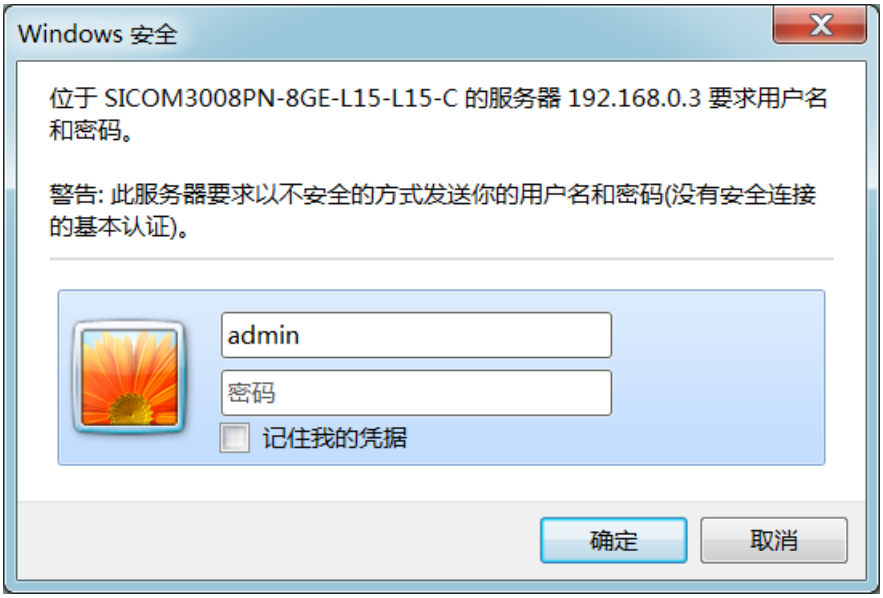


Figure 9 Web Login

2. The prompt of modifying the initial password is displayed, click <OK> button.

3. After you log in successfully, there is a navigation tree on the left of the interface, as shown below.

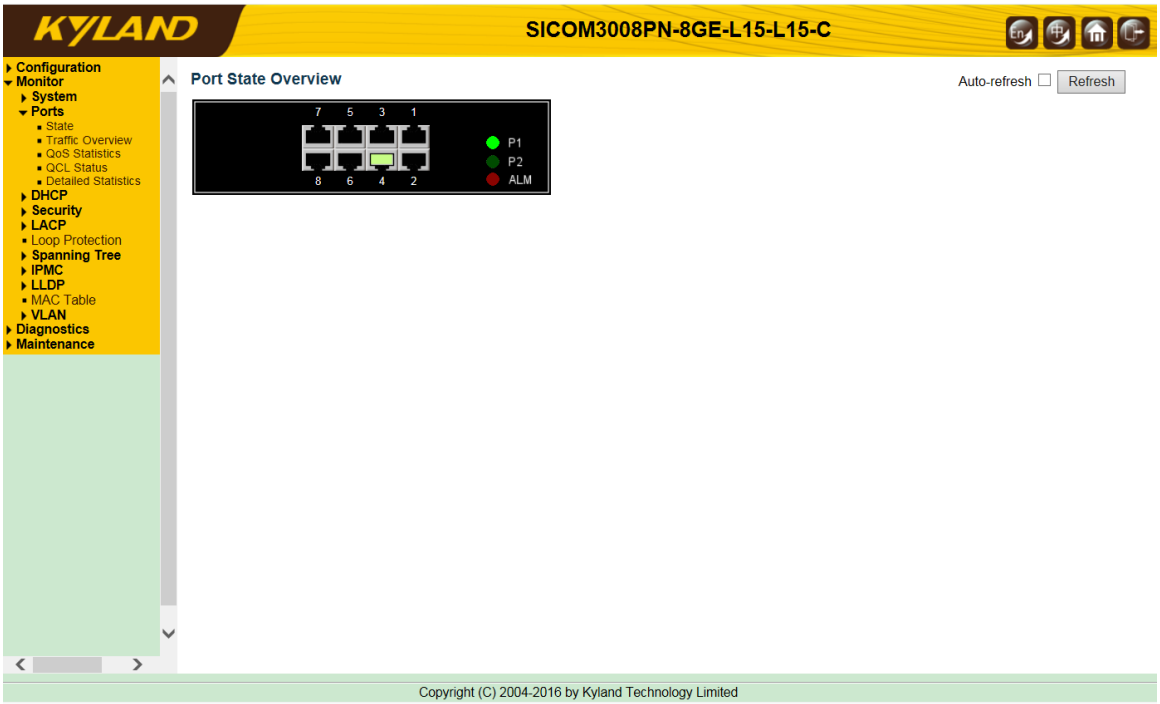


Figure 10 Web Interface

3 Configuration

3.1 System

3.1.1 System Information

The switch system information is provided here.

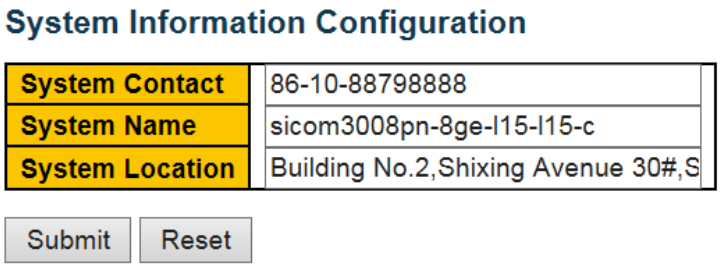


Figure 11 system information

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

Buttons	
Submit	Click to save changes.
Reset	Click to revert to previously saved values.

3.1.2 System IP

Configure IP basic settings, control IP interfaces and IP routes.

The maximum number of interfaces supported is 8 and the maximum number of routes is 32.

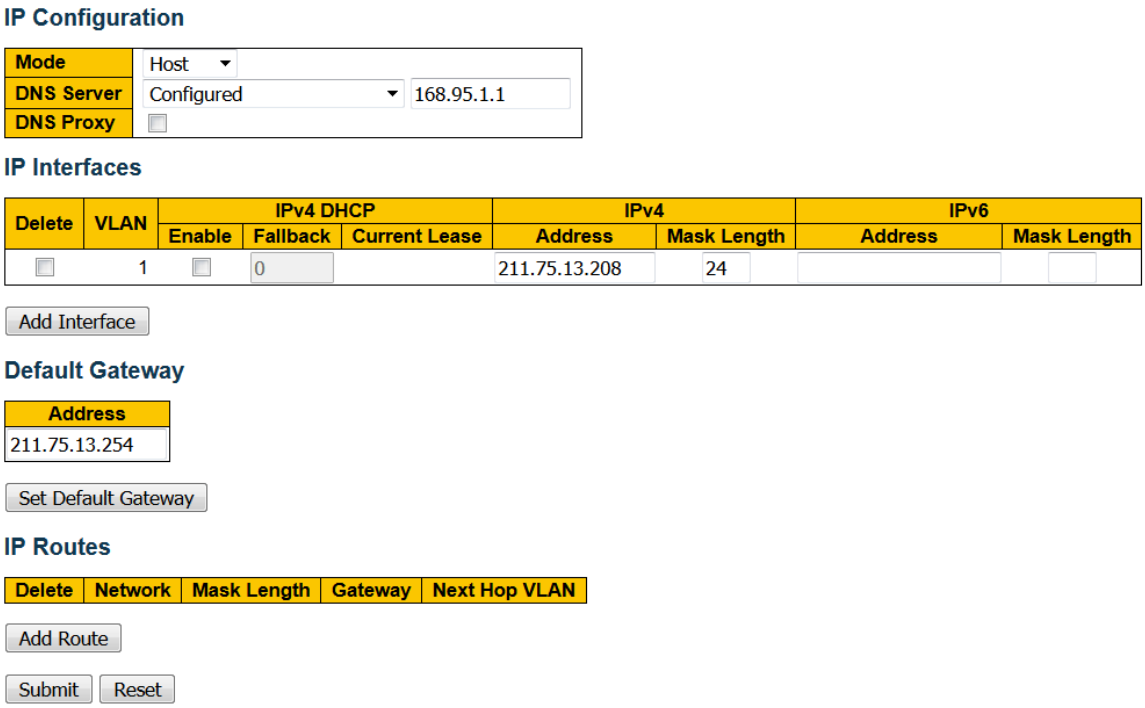


Figure 12 System IP

Object	Description
IP Configuration	
Mode	Configure whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.
DNS Server	This setting controls the DNS name resolution done by the switch. 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, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.
IP Interfaces	
Delete	Select this option to delete an existing IP interface.
VLAN	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating an new interface.
IPv4 DHCP Enabled	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.
IPv4 DHCP Fallback Timeout	The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are

	0 to 4294967295 seconds.
IPv4 DHCP Current Lease	For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.
IPv4 Address	The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
IPv4 Mask	The IPv4 network mask, in number of bits (*prefix length*). Valid values are between 0 and 30 bits for 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. It can also represent a legally valid IPv4 address. For example, ::192.1.2.34. The field may be left blank if IPv6 operation on the interface is not desired.
IPv6 Mask	The IPv6 network mask, in number of bits (*prefix length*). Valid values are between 1 and 128 bits for a IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.
Default Gateway	
Address	The IP address of the gateway valid format is dotted decimal notation.
IP Routes	

Delete	Select this option to delete an existing IP route.
Network	The destination IP network or host address of this route. Valid format is dotted decimal notationor a valid IPv6 notation. A default route can use the value 0.0.0.0or IPv6 :: notation.
Mask Length	The destination IP network or host mask, in number of bits (*prefix length*). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).
Gateway	The IP address of the IP gateway. Valid format is dotted decimal notationor a valid IPv6 notation. Gateway and Network must be of the same type.
Next Hop VLAN(Only for IPv6)	The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 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.

Buttons	
Add Interface	Click to add a new IP interface. A maximum of 8 interfaces is supported.
Set Default Gateway	Click to save changes.
Add Route	Click to add a new IP route. A maximum of 32 routes is supported.
Submit	Click to save changes.

Reset	Click to revert to previously saved values.

3.1.3 System NTP

Configure NTP on this page.

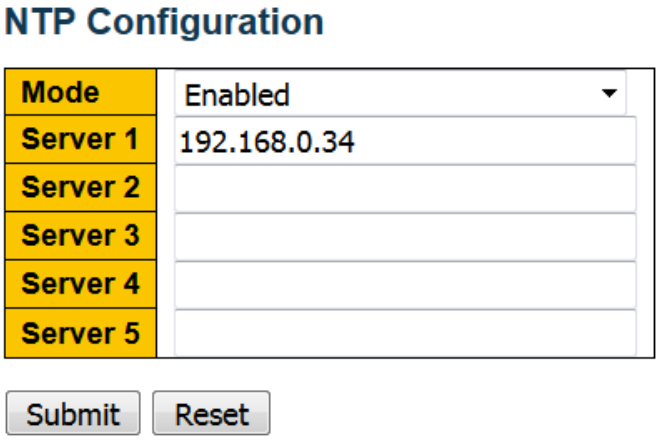


Figure 13 NTP Configure

Object	Description
Mode	Indicates the NTP mode operation. Possible modes are: Enabled: Enable NTP client mode operation. Disabled: Disable NTP client mode operation.
Server #	Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Buttons

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

3.1.4 System Time

This page allows you to configure the Time Zone.

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

Date/Time Configuration

Date/Time settings	
Year	2000 (2000 - 2037)
Month	Jan
Date	2
Hours	20
Minutes	29
Seconds	51

Submit Reset

Figure 14 Time Zone Configuration

Object	Description
Time Zone Configuration	
Time Zone	Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set.
Acronym	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 characters)
Daylight Saving Time Configuration	
Daylight Saving Time	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default : Disabled)
Recurring Configurations	
Start time settings	
Week	Select the starting week number.
Day	Select the starting day.
Month	Select the starting month.
Hours	Select the starting hour.
Minutes	Select the starting minute
End time settings	
Week	Select the ending week number.
Day	Select the ending day.
Month	Select the ending month.
Hours	Select the ending hour.
Minutes	Select the ending minute
Offset settings	

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

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

3.1.5 System Log

Configure System Log on this page.

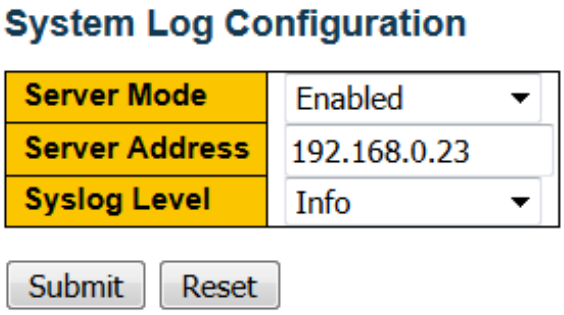


Figure 15 System Log configuration

Object	Description
Server Mode	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: 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 informations, warnings and errors. Warning: Send warnings and errors. Error: Send errors.

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

3.1.6 System Alarm Profile

Alarm Profile is provided here to enable/disable alarm.

Alarm Profile

ID	Description	Enabled
*	*	☐
1	Port 1 Link Down	☐
2	Port 2 Link Down	☐
3	Port 3 Link Down	☑
4	Port 4 Link Down	☑
5	Port 5 Link Down	☐
6	Port 6 Link Down	☐
7	Port 7 Link Down	☐
8	Port 8 Link Down	☐
9	Port 9 Link Down	☐
10	Port 10 Link Down	☐
11	Port 11 Link Down	☐

Figure 16 Alarm Profile

Object	Description
ID	The identification of the Alarm Profile entry.
Description	Alarm Type Description.

Enabled	If alarm entry is Enabled, then alarm will be shown in alarm history/current when it occurs. Alarm LED will be on (lighted), Alarm Relay also be enabled. SNMP trap will be sent if any SNMP trap entry exists and enabled.
Disabled	If alarm entry is Disabled, then alarm will not be captured/shown in alarm history/current when alarm occurs; then it will not trigger the Alarm LED change, Alarm Relay and SNMP trap either.
Note: When any alarm exists, the Alarm LED will be on (lighted), Alarm Output Relay will also be enabled.	

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

3.2 Ports

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

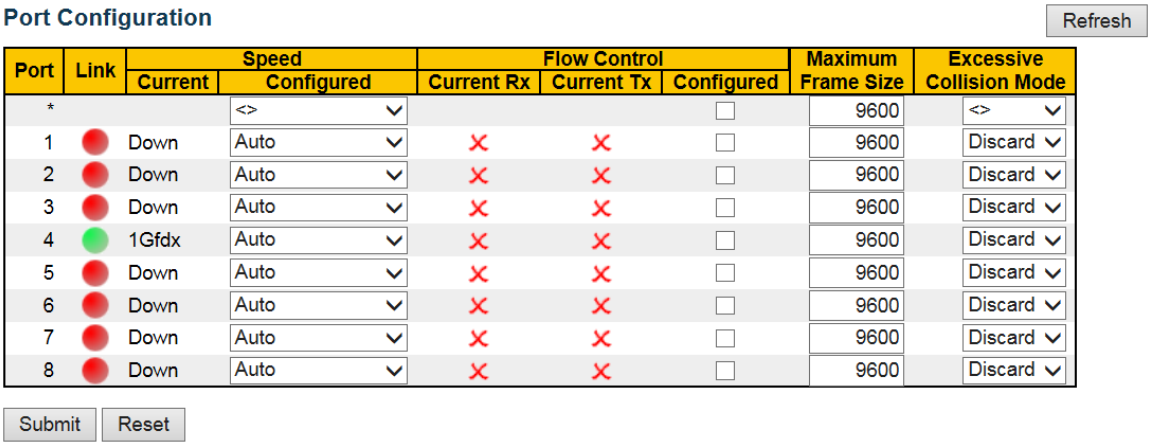


Figure 17 Port Configuration

Object	Description
Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
Current Link Speed	Provides the current link speed of the port.
Configured Link Speed	Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are: Disabled - Disables the switch port operation. Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner. 10Mbps HDX - Forces the cu port in 10Mbps half duplex mode. 10Mbps FDX - Forces the cu port in 10Mbps full duplex mode. 100Mbps HDX - Forces the cu port in 100Mbps half duplex mode. 100Mbps FDX - Forces the cu port in 100Mbps full duplex mode. 1Gbps FDX - Forces the port in 1Gbps full duplex .

Flow Control	When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
Maximum Frame Size	Enter the maximum frame size allowed for the switch port, including FCS.
Excessive Collision Mode	Configure port transmit collision behavior. Discard: Discard frame after 16 collisions (default). Restart: Restart backoff algorithm after 16 collisions.

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

3.3 DHCP

3.3.1 DHCP Server

3.3.1.1 DHCP Server Mode

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

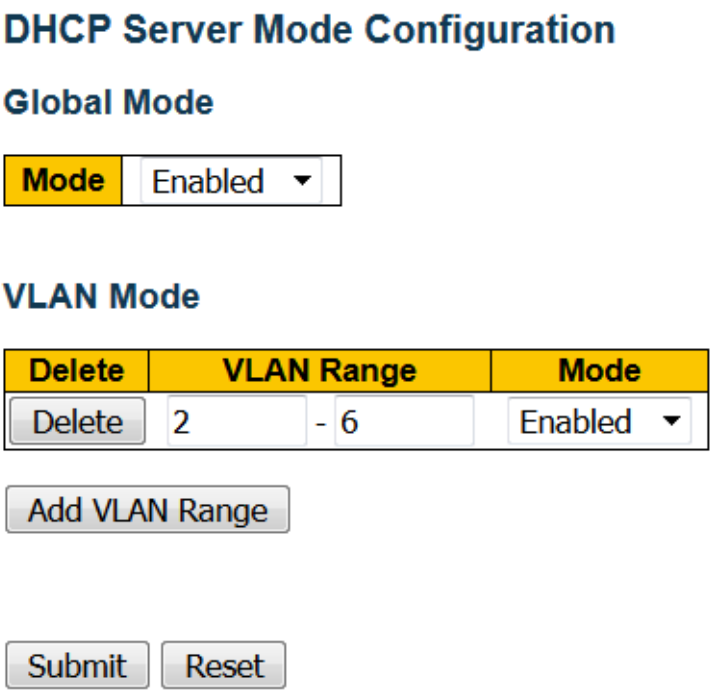


Figure 18 DHCP Server Mode Configuration

Object	Description
Global Mode	
Mode	Configure the operation mode per system. Possible modes are: Enabled: Enable DHCP server per system. Disabled: Disable DHCP server pre system.
VLAN Mode	
VLAN Range	Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input

	it into either one of the first and second VLAN ID or both. On the other hand, if you want to disable existed VLAN range, then you can follow the steps. 1. press 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.

Buttons	
Delete	Click to delete the setting.
Add VLAN Range	Click to add a new VLAN range.
Submit	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

3.3.1.2 DHCP Server Excluded IP

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

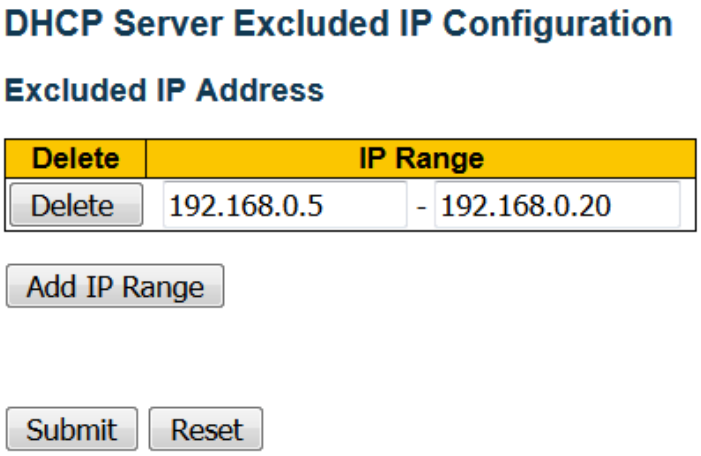


Figure 19 DHCP Server Excluded IP

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

Buttons	
Delete	Click to delete the setting.
Add IP Range	Click to add a new excluded IP range.
Submit	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

3.3.1.3 DHCP Server Pool

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

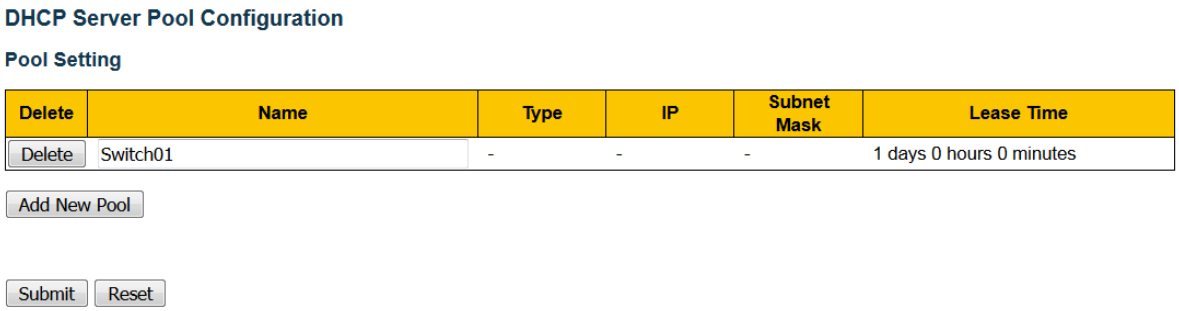


Figure 20 DHCP Server Pool

Object	Description
Name	Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.
Type	Display which type of the pool is. 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.

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

3.3.2 DHCP Snooping

Configure DHCP Snooping on this page.

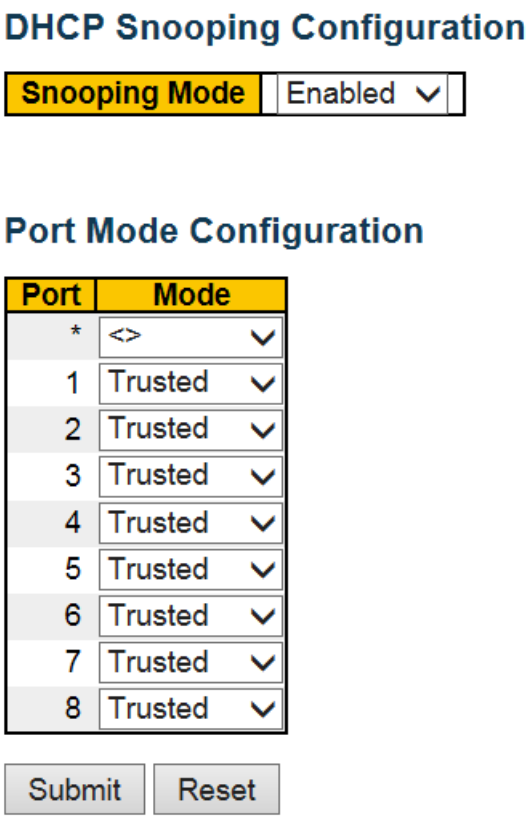


Figure 21 DHCP Snooping

Object	Description
Snooping Mode	Indicates the DHCP snooping mode operation. Possible modes are: Enabled: Enable DHCP snooping mode operation. When DHCP

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

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

3.4 Security

3.4.1 Switch

3.4.1.1 Users

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

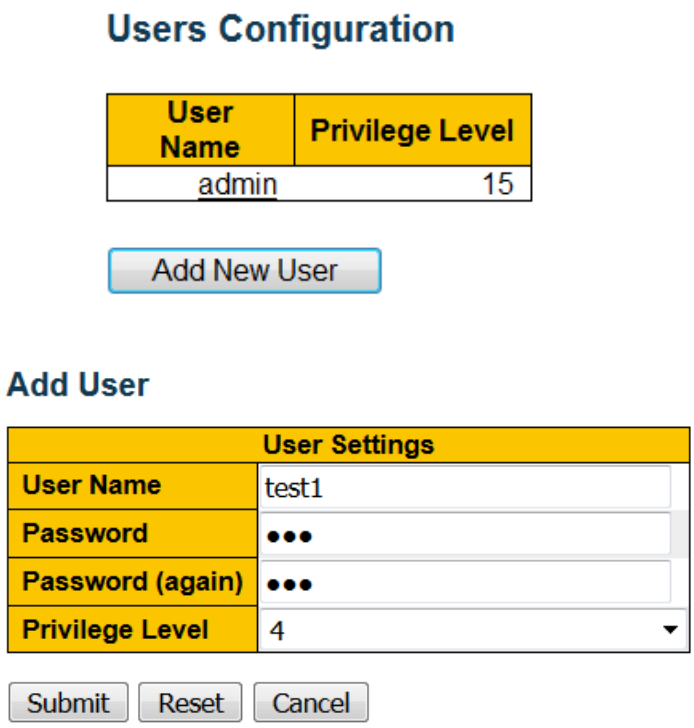


Figure 22 User

Object	Description
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31. The valid user name allows letters, numbers and underscores.
Password	The password of the user. The allowed string length is 0 to 31. Any printable characters including space is accepted.
Privilege Level	The privilege level of the user. The allowed range is 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.

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

3.4.1.2 Privilege Level

This page provides an overview of the privilege levels.

Privilege Level Configuration

Group Name	Privilege Level			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Debug	15	15	15	15
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
VCL	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
XXRP	5	10	5	10

Submit Reset

Figure 23 privilege level

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

	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.

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

3.4.1.3 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.

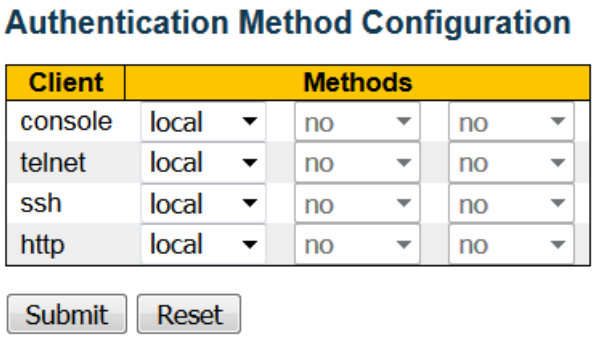


Figure 24 authentication Method

Object	Description
Client	The management client for which the configuration below applies.
Methods	Method can be set to one of the following values: • no: Authentication is disabled and login is not possible. • local: Use the local user database on the switch for authentication. • radius: Use remote RADIUS server(s) for authentication. • tacacs+: Use remote TACACS+ server(s) for authentication. Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

Buttons

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

3.4.1.4 SSH/TELNET

Configure SSH/TELNET on this page.

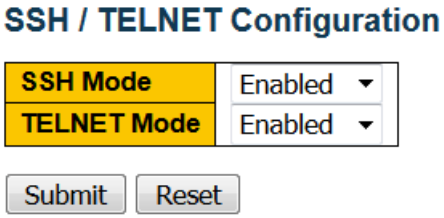


Figure 25 SSH/TELNET Configuration

Object	Description
SSH Mode	Indicates the SSH mode operation. Possible modes are: Enabled: Enable SSH mode operation. Disabled: Disable SSH mode operation.
TELNET Mode	Indicates the TELNET mode operation. Possible modes are: Enabled: Enable TELNET mode operation. Disabled: Disable TELNET mode operation.

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

3.4.1.5 HTTPS

Configure HTTPS on this page.

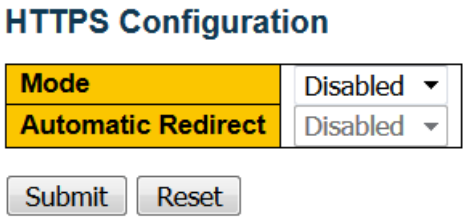


Figure 26 HTTPS Configuration

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

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

3.4.1.6 Access Management

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

to the switch.

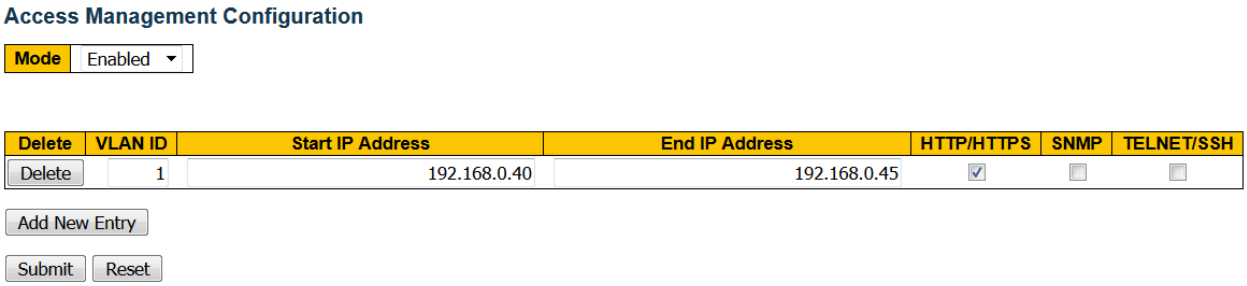


Figure 27 access management Configuration

Object	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.
VLAN ID	Indicates the VLAN ID for the access management entry.
Start IP address	Indicates the start IP address for the access management entry.
End IP address	Indicates the end IP address for the access management entry.
HTTP/HTTPS	Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
SNMP	Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.
TELNET/SSH	Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

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

3.4.2 SNMP

3.4.2.1 SNMP System Configuration

Configure SNMP on this page.

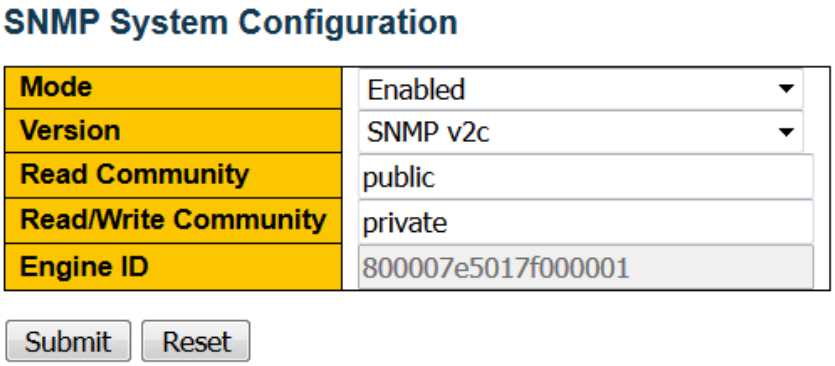


Figure 28 SNMP System configuration

Object	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 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Write Community	Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

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

3.4.2.2 SNMP Trap Configuration

Configure SNMP trap on this page.

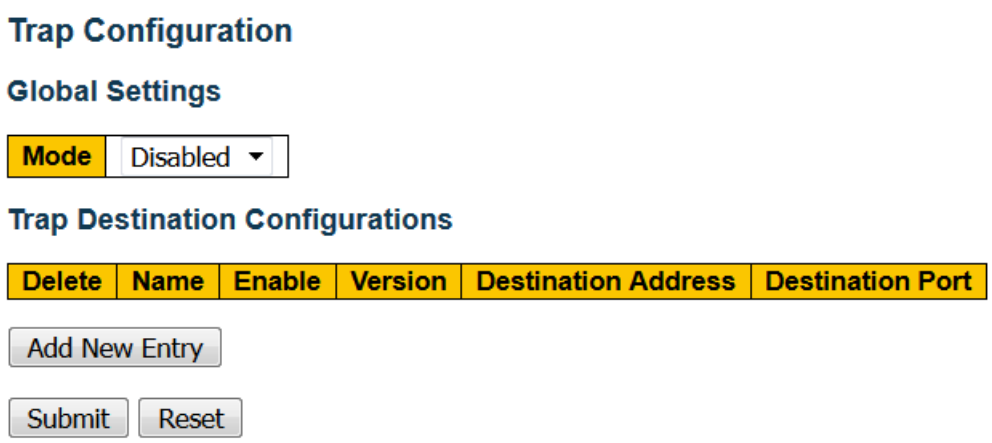


Figure 29 SNMP Trap Configuration

Object	Description
Global Settings	
Mode	Indicates the trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Trap Destination Configurations	
Name	Indicates the trap Configuration's name. Indicates the trap destination's name.
Enable	Indicates the trap destination mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Version	Indicates the SNMP trap supported version. Possible versions are: **SNMPv1**: Set SNMP trap supported version 1. **SNMPv2c**: Set SNMP trap supported version 2c. **SNMPv3**: Set SNMP trap supported version 3.
Destination Address	Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of

	contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
Destination port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

The SNMP Trap Configuration page includes the following fields:

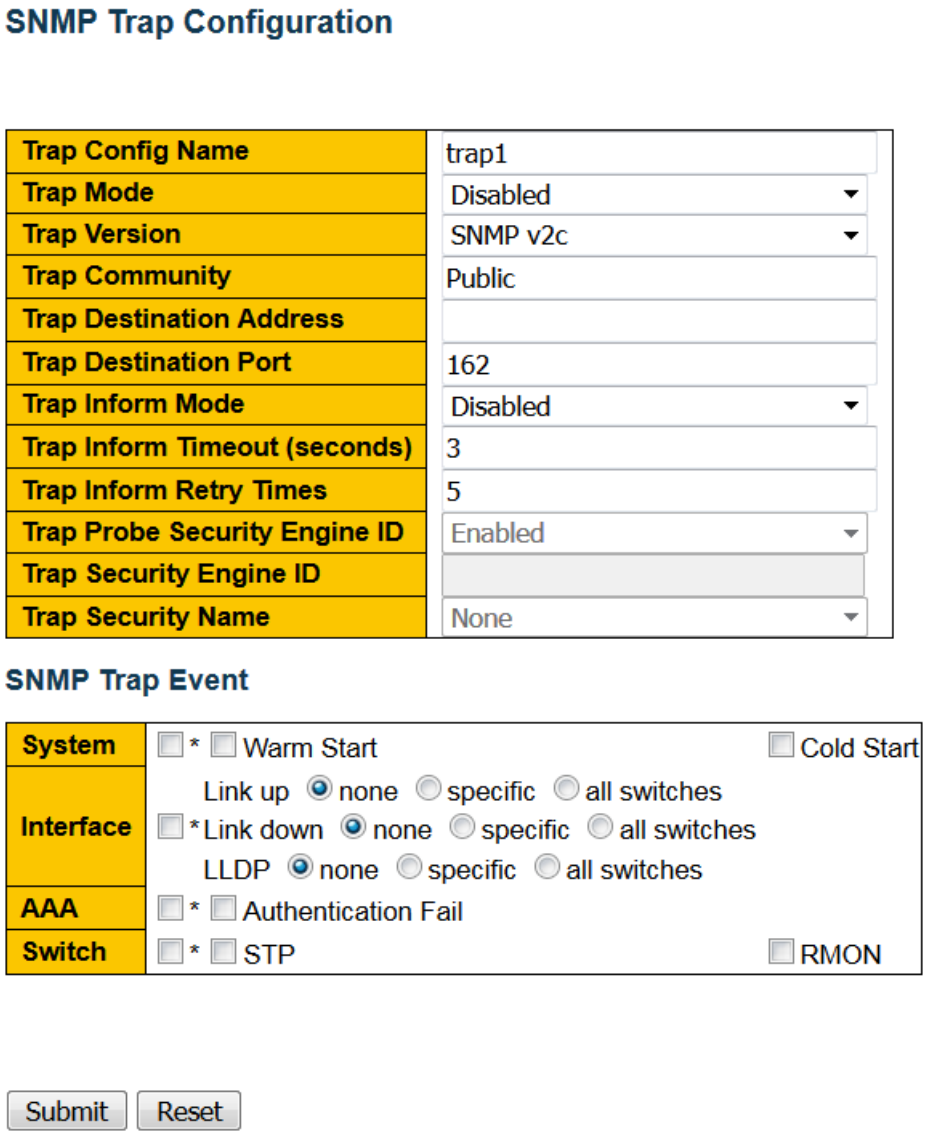


Figure 30 SNMP Trap Configuration Details

Object	Description
Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation.

	Disabled: Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Possible versions are: **SNMP v1**: Set SNMP trap supported version 1. **SNMP v2c**: Set SNMP trap supported version 2c. **SNMP v3**: Set SNMP trap supported version 3.
Trap Community	Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.
Trap Destination Address	Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash
Trap Destination IIPv6 Address	Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
Trap Authentication Failure	Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are: Enabled: Enable SNMP trap authentication failure. Disabled: Disable SNMP trap authentication failure.
Trap Link-up and Link-down	Indicates the SNMP trap link-up and link-down mode operation. Possible modes are: Enabled: Enable SNMP trap link-up and link-down mode operation.

	Disabled: Disable SNMP trap link-up and link-down mode operation.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: Enabled: Enable SNMP trap inform mode operation. Disabled: Disable SNMP trap inform mode operation.
Trap Inform Timeout (seconds)	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Buttons	
Add New Entry	Click to add a new user.
Save	Click to save changes.

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

3.4.2.3 SNMP Communities

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

SNMPv3 Community Configuration

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

Add New Entry Submit Reset

Figure 31 SNMPv3 community configuration

Object	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 ASCII characters from 33 to 126. The community string will be treated 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 be used to restrict source subnet when combined with source mask.
Source Mask	Indicates the SNMP access source address mask.

Buttons	
Add New Entry	Click to add a new community entry.
Submit	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

3.4.2.4 SNMP Users

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

SNMPv3 User Configuration

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

Add New Entry Submit Reset

Figure 32 SNMPv3 user configuration

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
User name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: No authentication and no privacy.

	Auth, NoPriv: Authentication and no privacy. Auth, Priv: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: None: No authentication protocol. **MD5**: An optional flag to indicate that this user uses MD5 authentication protocol. **SHA**: An optional flag to indicate that this user uses 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 password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: None: No privacy protocol. **DES**: An optional flag to indicate that this user uses DES authentication protocol. **AES**: An optional flag to indicate that this user uses AES authentication protocol.
Privacy Password	A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

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

3.4.2.5 SNMP Groups

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

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 Submit Reset

Figure 33 SNMPv3 group configuration

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: 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 ASCII characters from 33 to 126.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons	
Add New Entry	Click to add a new group entry

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

3.4.2.6 SNMP Views

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

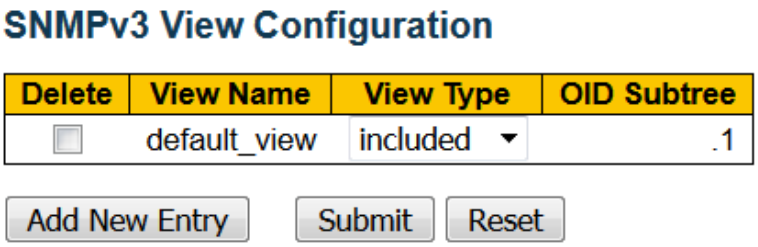


Figure 34 SNMPv3 view configuration

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: included: An optional flag to indicate that this view subtree should be included. excluded: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

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

3.4.2.7 SNMP Access

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

SNMPv3 Access Configuration

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

Add New Entry Submit Reset

Figure 35 SNMPv3 access

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: any: Any security model accepted(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: No authentication and no privacy. Auth, NoPriv: Authentication and no privacy. Auth, Priv: Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

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

3.4.3 RMON

3.4.3.1 RMON Statistics

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

Figure 36 RMON Statistics table

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

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

3.4.3.2 RMON History

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

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted

Add New Entry Submit Reset

Figure 37 RMON History table

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

Buttons	
Add New Entry	Click to add a new community entry.
Submit	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

3.4.3.3 RMON Alarm

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

RMON Alarm Configuration

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

Add New Entry Submit Reset

Figure 38 RMON Alarm table

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65
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).

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

	values.

3.4.3.4 RMON Event

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

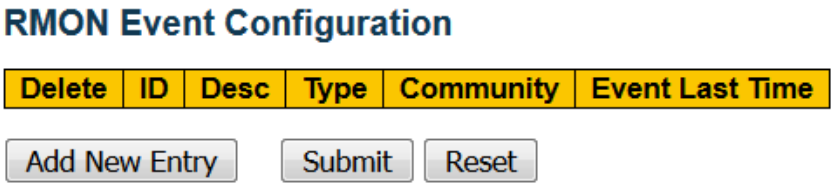


Figure 39 RMON Event table

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Desc	Indicates this event, the string length is from 0 to 127, default is a null string.
Type	Indicates the notification of the event, the possible types are: none: No SNMP log is created, no SNMP trap is sent. log: Create SNMP log entry when the event is triggered. snmptrap: Send SNMP trap when the event is triggered. logandtrap: Create SNMP log entry and sent SNMP trap when the event is triggered.
Community	Specify the community when trap is sent, the string length is from 0 to 127, default is "public".
Event Last Time	Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons	
Add New Entry	Click to add a new community entry.

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

3.4.4 Network

3.4.4.1 NAS

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration→Security→AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

The NAS configuration consists of two sections, a system- and a port-wide.

Network Access Server Configuration

System Configuration

Mode	Disable	
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

Submit Reset

Figure 40 NAS configuration

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

Reauthentication Period	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.
Aging Period	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • 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 an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. 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 Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, 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 determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.
RADIUS-Assigned VLAN Enabled	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the

	RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.
Guest VLAN Enabled	A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.
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 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	
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 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 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) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e. • Port-based 802.1X • Single 802.1X **<u>RADIUS attributes used in identifying a QoS Class:</u>**

	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' - '7', which translates into the desired QoS Class in the range [0; 7].
RADIUS-Assigned VLAN Enabled	When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. 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 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 fulfil 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 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 transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN. 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 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. **Reinitialize:** Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

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

3.4.5 ACL

3.4.5.1 ACL Port

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	548
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	1645
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Submit Reset

Figure 41 ACL port

Object	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.
Action	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
Rate Limiter ID	Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".
Port Redirect	Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".

Mirror	Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled".
Loggig	Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are: 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". Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of this port. The allowed values are: 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". Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).
State	Specify the port state of this port. The allowed values are: 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.

Buttons	
Submit	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved

	values.
Refresh	Click to refresh the page; any changes made locally will be undone.
Clear	Click to clear the counters.

3.4.5.2 ACL Rate Limiters

Configure the rate limiter for the ACL of the switch.

ACL Rate Limiter Configuration

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

Submit Reset

Figure 42 ACL rate Limiters

Object	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The rate range is located **0-3276700** in pps. Or **0, 100, 200, 300, ..., 1000000** in kbps.
Unit	Specify the rate unit. The allowed values are:

	pps: packets per second. kbps: Kbits per second.

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

3.4.5.3 Access Control List

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch.

Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

Access Control List Configuration

Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
								⊕

Figure 43 Access Control List

Object	Description
Ingress Port	Indicates the ingress port of the ACE. Possible values are: All: The ACE will match all ingress port. Port: The ACE will match a specific ingress port.
Policy / Bitmask	Indicates the policy number and bitmask of the ACE.
Frame Type	Indicates the frame type of the ACE. Possible values are: Any: The ACE will match any frame type. EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

	ARP: The ACE will match ARP/RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/**ICMP**: The ACE will match IPv4 frames with ICMP protocol. IPv4/**UDP**: The ACE will match IPv4 frames with UDP protocol. IPv4/**TCP**: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. IPv6: The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped. Filter: Frames matching the ACE are filtered.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
Mirror	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: 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.
Modification Buttons	You can modify each ACE (Access Control Entry) in the table using the following buttons: ⊕: Inserts a new ACE before the current row. ⓔ: Edits the ACE row.

	: Moves the ACE up the list. : Moves the ACE down the list. : Deletes the ACE. : The lowest plus sign adds a new entry at the bottom of the ACE listings.

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

The ACE Configuration page includes the following fields:

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Save Reset Cancel

Figure 44 ACE configuration

Object	Description
Ingress Port	Select the ingress port for which this ACE applies.

	All: The ACE applies to all port. Port *n*: The ACE applies to this port number, where *n* is the number of the switch port.
Policy Filter	Specify the policy number filter for this ACE. 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.
Policy Value	When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255.
Policy Bitmask	When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.
Frame Type	Select the frame type for this ACE. These frame types are mutually exclusive. Any: Any frame can match this ACE. **Ethernet Type**: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). **ARP**: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type. IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type. IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.
Action	Specify the action to take with a frame that hits this ACE.

	Permit: The frame that hits this ACE is granted permission for the ACE operation. Deny: The frame that hits this ACE is dropped. Filter: Frames matching the ACE are filtered.
Rate Limiter	Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.
Port Redirect	Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.
Mirror	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are: 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 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.
MAC Parameters	
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 Parameters	
802.1Q Tagged	Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are: Any: Any value is allowed ("don't-care").

	Enabled: Tagged frame only. Disabled: Untagged frame only. The default value is "Any".
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".)
ARP Parameters	
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.
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.
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	
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.
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.
DIP Mask	When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.
IPv6 Parameters	
Next Header Filter	Specify the IPv6 next header filter for this ACE. 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	
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.

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

3.4.6 AAA

3.4.6.1 RADIUS

This page allows you to configure the RADIUS servers.

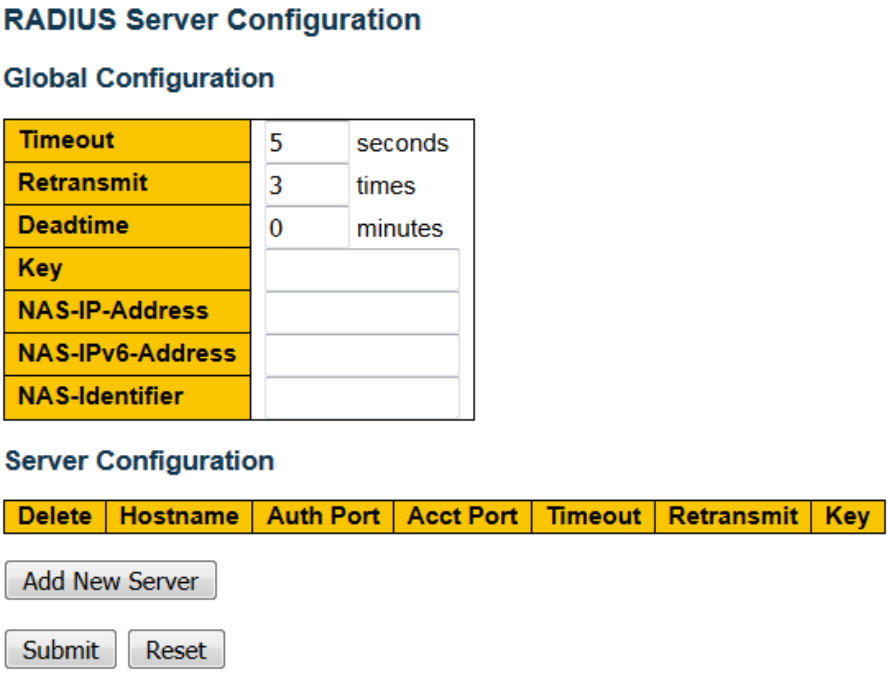


Figure 45 RADIUS servers configuration

Object	Description
Global Configuration	
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
Retransmit	Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.
Deadtime	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous

	request. This will stop the switch from continually trying to contact a server that it has already determined as dead. 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(Attribute 4)	The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
NAS-IPv6-Address(Attribute 95)	The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
NAS-Identifier (Attribute 32)	The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.
Server Configuration	
Delete	To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IP address or hostname of the RADIUS server.
Auth Port	The UDP port to use on the RADIUS server for authentication.
Acct Port	The UDP port to use on the RADIUS server for accounting.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Retransmit	This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.

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

3.4.6.2 TACACS+

This page allows you to configure the TACACS+ servers.

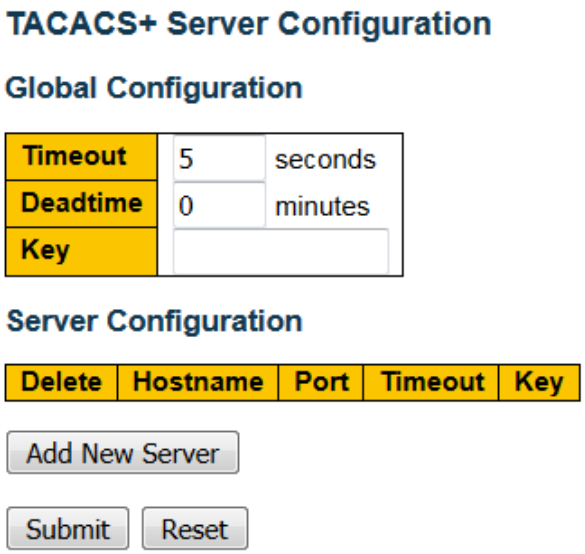


Figure 46 TACACS+ servers configuration

Object	Description
Global Configuration	
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.
Deadtime	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. 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 Configuration	
Delete	To delete a TACACS+ server entry, check this box. The entry will be

	deleted during the next Save.
Hostname	The IP address or hostname of the TACACS+ server.
Port	The TCP port to use on the TACACS+ server for authentication.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.

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

3.5 Aggregation

3.5.1 Static Aggregation

This page is used to configure the Aggregation hash mode and the aggregation group.

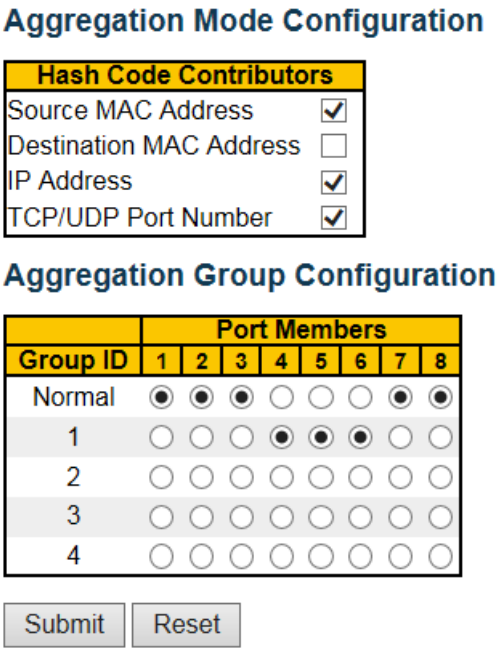


Figure 47 Aggregation configuration

Object	Description
Hash Code Contributors	
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.

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

3.5.2 LACP Aggregation

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

LACP Port Configuration

Ports	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
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

Submit Reset

Figure 48 LACP port configuration

Object	Description
Port	The switch port number.
LACP Enabled	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.
Key	The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
Role	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
Timeout	The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds

	before sending a LACP packet.
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.

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

3.6 Loop Protection

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

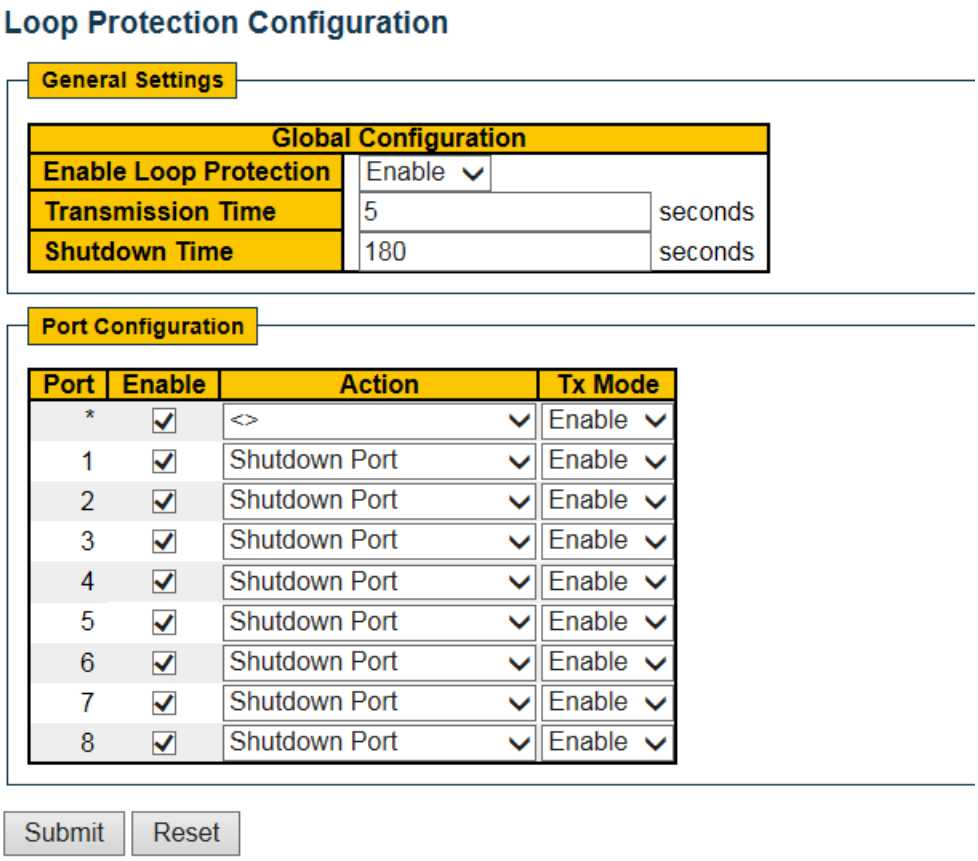


Figure 49 Loop Protection configuration

Object	Description
General Settings	
Enable Loop Protection	Controls whether loop protections is enabled (as a whole).
Transmission Time	The interval between each loop protection PDU sent on each port, valid values are 1 to 10 seconds.
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 Configuration	
Port	The switch port number of the port.
Enable	Controls whether loop protection is enabled on this switch port.
Action	Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.
Tx Mode	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

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

3.7 Spanning Tree

3.7.1 Bridge Settings

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

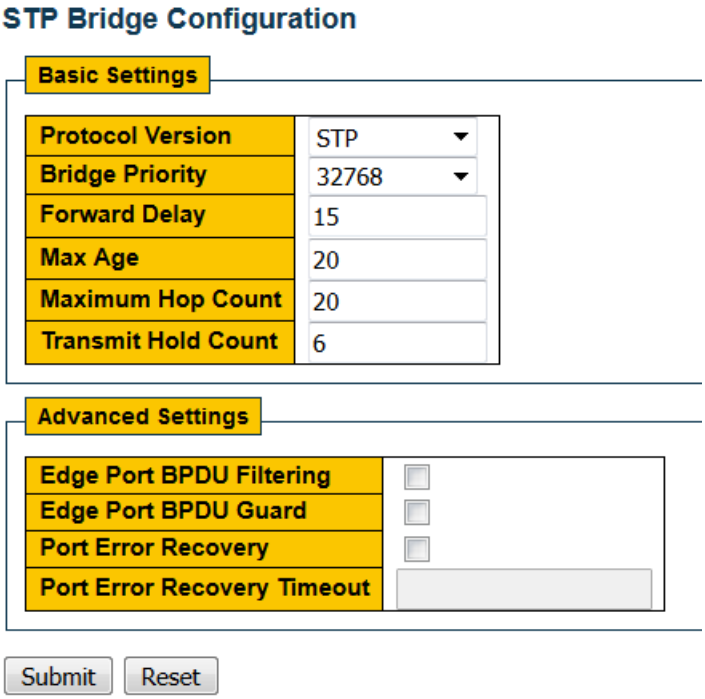


Figure 50 STP Bridge configuration

Object	Description
Basic Settings	
Protocol Version	The MSTP / RSTP / STP protocol version setting. Valid values are STP, RSTP and MSTP.
Bridge Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*. 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 transit Root and Designated Ports to

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

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

3.7.2 MSTI Mapping

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

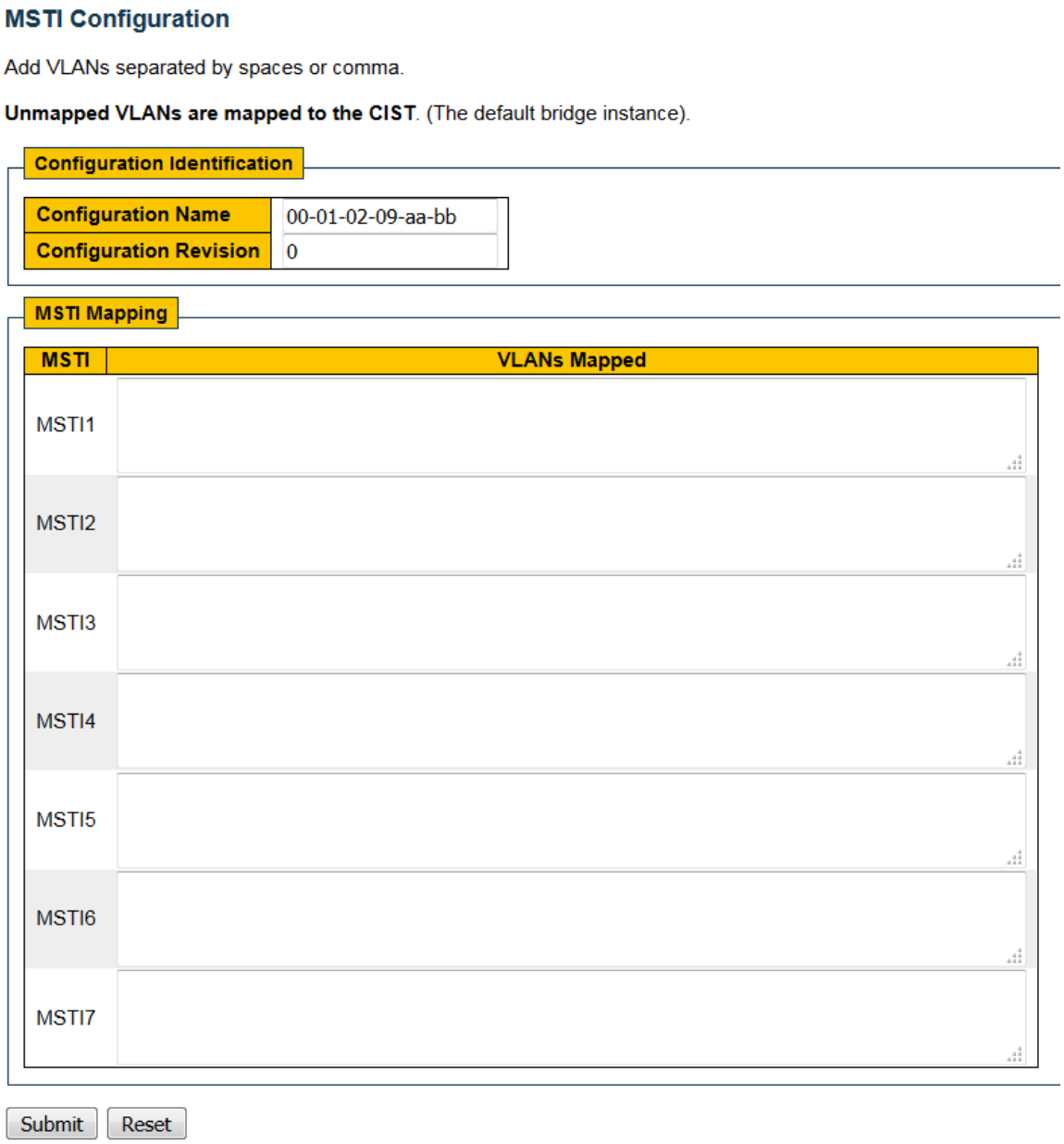


Figure 51 MSTI configuration

Object	Description
Configuration Identification	
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping

	configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
MSTI Mapping	
MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
VLANs Mapped	The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to *one* MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2,5,20-40.

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

3.7.3 MSTI Priorities

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

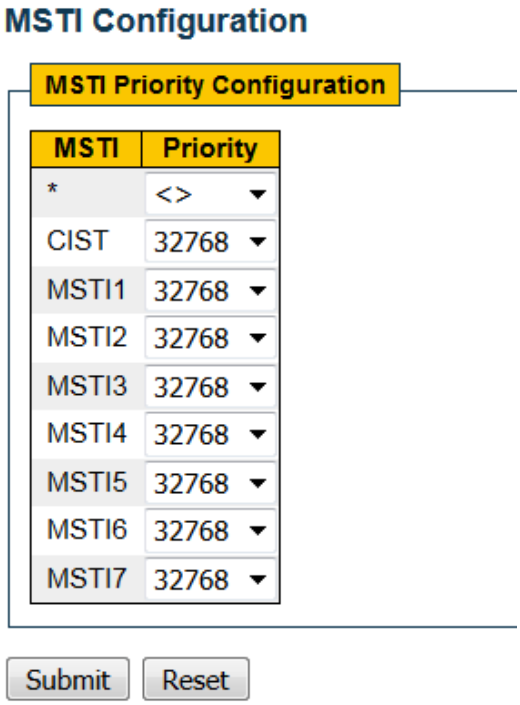


Figure 52 MSTI configuration

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

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

3.7.4 CIST Ports

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

This page contains settings for physical and aggregated ports.

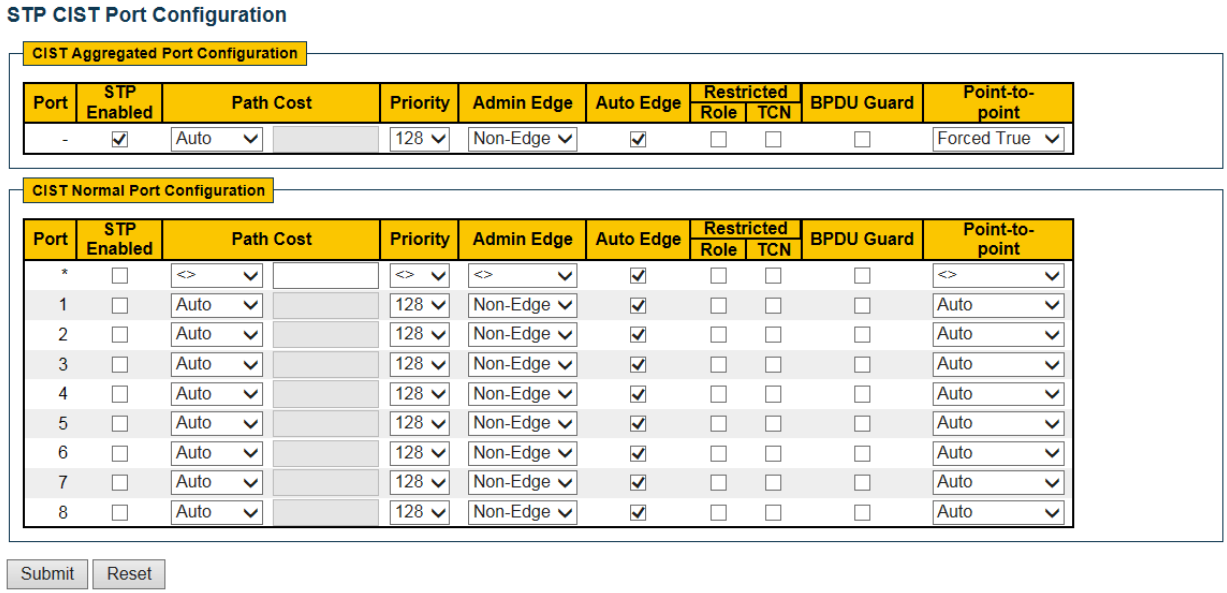


Figure 53 STP CIST port configuration

Object	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
operEdge (state flag)	Operational flag describing whether the port is connecting directly to edge

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

	Contrary to the similar bridge setting, the port Edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
Point-to-Point	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

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

3.7.5 MSTI Ports

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

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

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

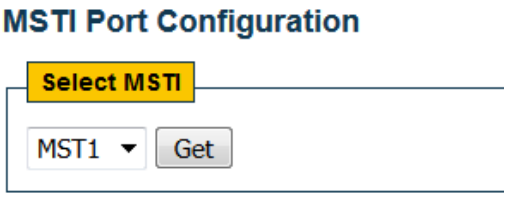


Figure 54 MSTI port configuration

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

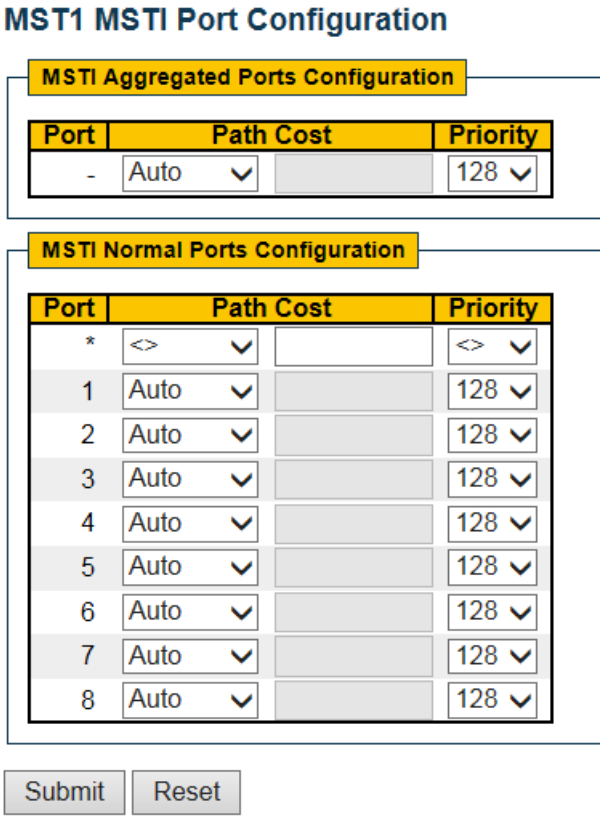


Figure 55 specific MSTI port configuration

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

Buttons	
Get	Click to retrieve settings for a specific MSTI.
Submit	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

3.8 IPMC

3.8.1 IGMP Snooping

3.8.1.1 Basic Configuration

This page provides IGMP Snooping related configuration.

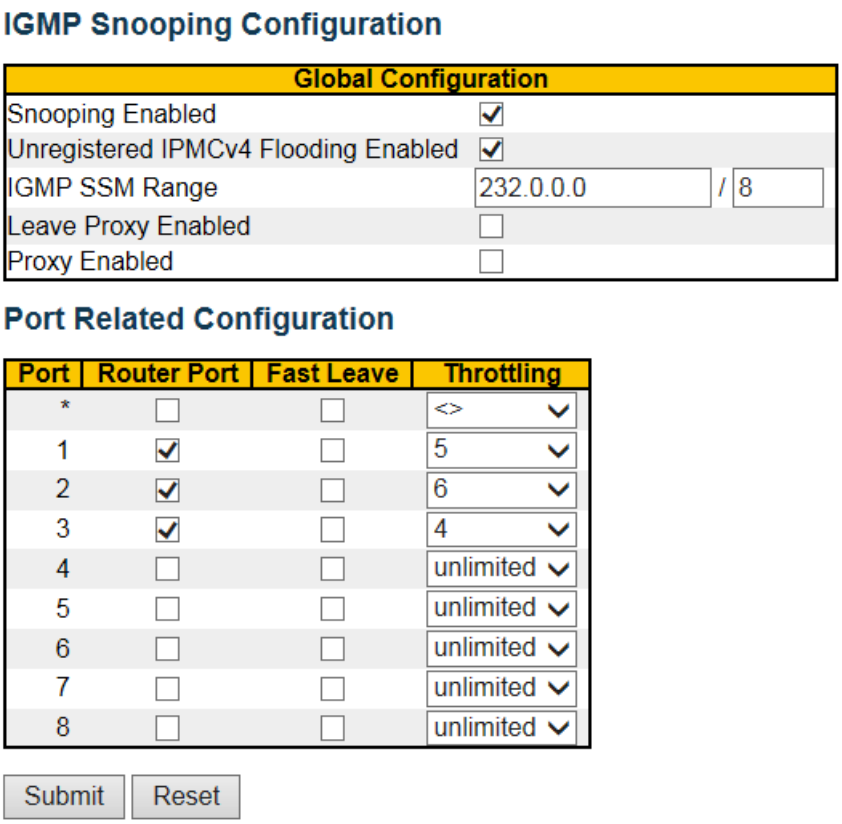


Figure 56 IGMP snooping configuration

Object	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.

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

3.8.1.2 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.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table.

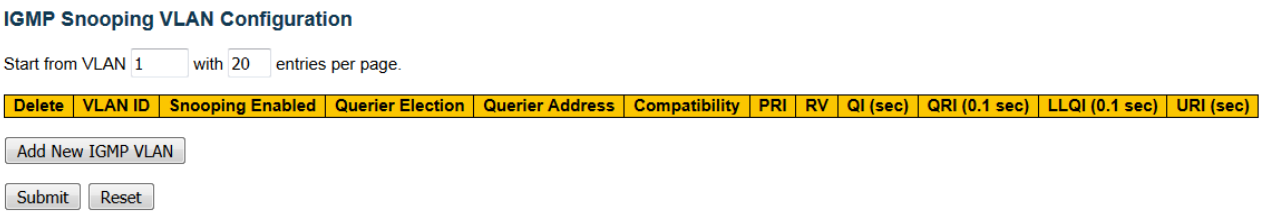


Figure 57 IGMP snooping VLan configuration

Object	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping 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

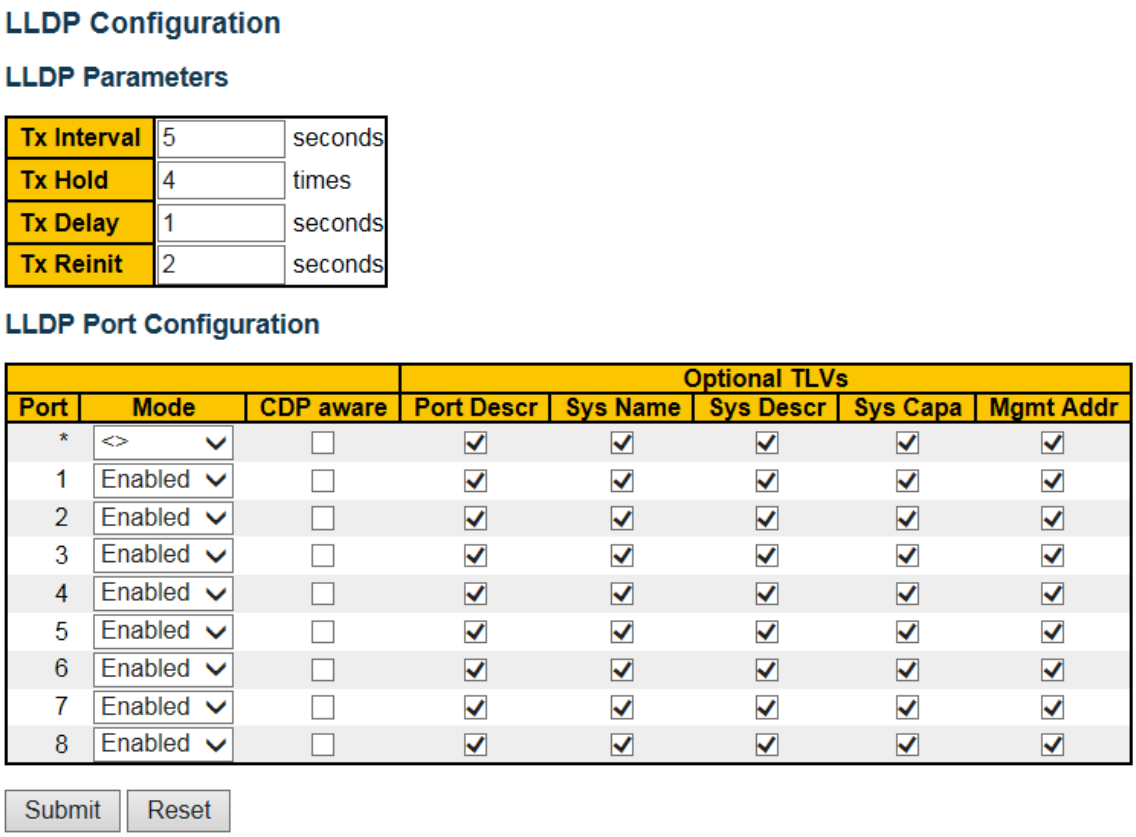
	member query interval is 10 in tenths of seconds (1 second).
URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons	
Refresh	Refreshes the displayed table starting from the "VLAN" input fields.
|<<	Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
>>	Updates the table, starting with the entry after the last entry currently displayed.
Add New 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.
Submit	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

3.9 LLDP

3.9.1 LLDP

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



LLDP Configuration

LLDP Parameters

Tx Interval	5	seconds
Tx Hold	4	times
Tx Delay	1	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	Enabled	☐	☑	☑	☑	☑	☑
2	Enabled	☐	☑	☑	☑	☑	☑
3	Enabled	☐	☑	☑	☑	☑	☑
4	Enabled	☐	☑	☑	☑	☑	☑
5	Enabled	☐	☑	☑	☑	☑	☑
6	Enabled	☐	☑	☑	☑	☑	☑
7	Enabled	☐	☑	☑	☑	☑	☑
8	Enabled	☐	☑	☑	☑	☑	☑

Submit Reset

Figure 58 LLDP port configuration

Object	Description
LLDP Parameters	
Tx Interval	The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds.
Tx Hold	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. Valid values are restricted to 2 - 10 times.

Tx Delay	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds.
Tx Reinit	When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signalling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.
LLDP Port Parameters	
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 on the port is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table

	as shown below. CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field. CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table. CDP TLV "Port ID" is mapped to the LLDP "Port ID" field. CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field. Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table. 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 on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.
Port Descr	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
Sys Name	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
Sys Descr	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
Sys Capa	Optional TLV: When checked the "system capability" is included in LLDP information transmitted.
Mgmt Addr	Optional TLV: When checked the "management address" is included in LLDP information transmitted.

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

3.10 MAC Table

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

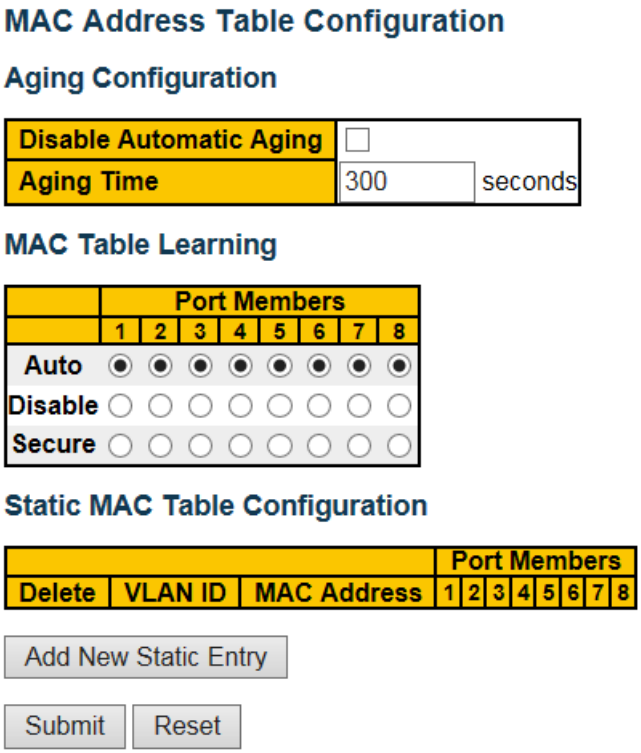


Figure 59 MAC address table configuration

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

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.
Static MAC Table Learning	
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click [Add New Static Entry] to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

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

3.11 VLANs

This page allows for controlling VLAN configuration on the switch.

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

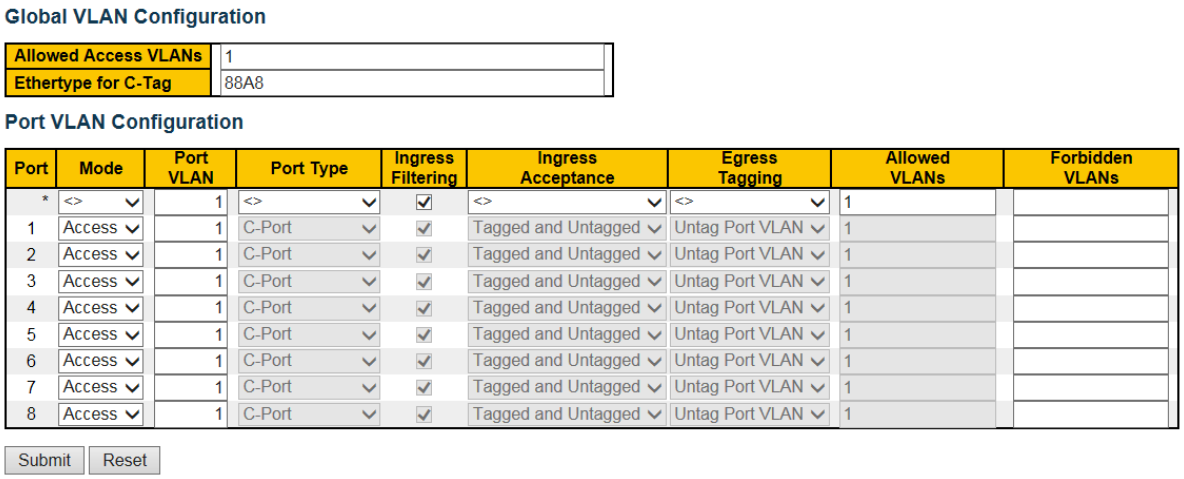


Figure 60 VLAN configuration

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

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

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

	the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. **S-Port:** On ingress, frames with a VLAN tag with TPID = 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, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.
Ingress Filtering	Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.
Ingress Acceptance	Hybrid ports allow for changing the type of frames that are accepted on ingress. **Tagged and Untagged** Both tagged and untagged frames are accepted. **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.
Egress Tagging	Ports in Trunk and Hybrid mode may control the tagging of frames on egress. **Untag Port VLAN** Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. **Tag All** All frames, whether classified to the Port VLAN or not, are transmitted with a tag. **Untag All** All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.
Allowed VLANs	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to **1-4095**. The field may be left empty, which means that the port will not become member of any VLANs.
Forbidden VLANs	A port may be configured to never 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.

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

3.12 QoS

3.12.1 Port Classification

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

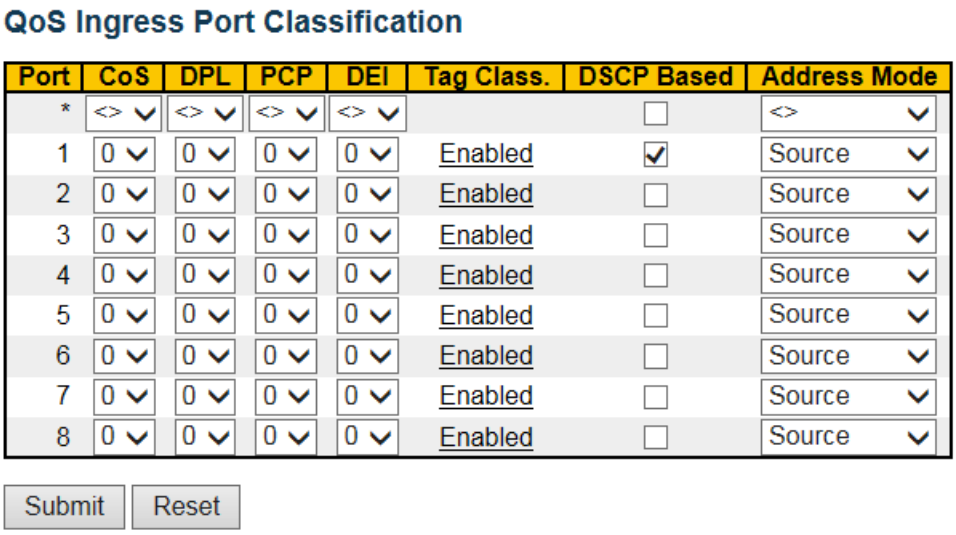


Figure 61 QoS Ingress port classification

Object	Description
Port	The port number for which the configuration below applies.
CoS	Controls the default class of service.

	All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS. The classified CoS can be overruled by a QCL entry. **Note:** If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.
DPL	Controls the default drop precedence level. All frames are classified to a drop precedence level. 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.
PCP	Controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	Controls the default DEI value. All frames are classified to a DEI value.

	If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Tag Class.	Shows the classification mode for tagged frames on this port. Disabled: Use default CoS and DPL for tagged frames. Enabled: Use mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping. **Note:** This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.
DSCP Based	Click to Enable DSCP Based QoS Ingress Port Classification.
Address Mode	The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are: Source: Enable SMAC/SIP matching. Destination: Enable DMAC/DIP matching.

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

3.12.2 Port Policing

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

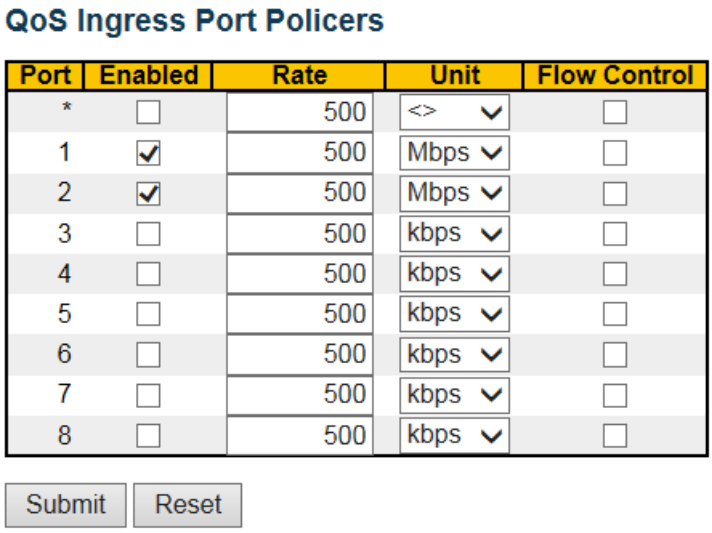


Figure 62 QoS Ingress port policer

Object	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.

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

3.12.3 Port Scheduler

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

QoS Egress Port Schedulers

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

Figure 63 QoS Egress Port Schedulers

Object	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.

3.12.4 Port Shaping

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

QoS Egress Port Shapers

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

Figure 64 QoS Egress Port Shapers

Object	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".

3.12.5 Port Tag Remarking

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

QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified

Figure 65 QoS Egress Port Tag Remarking

Object	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.

3.12.6 Port DSCP

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

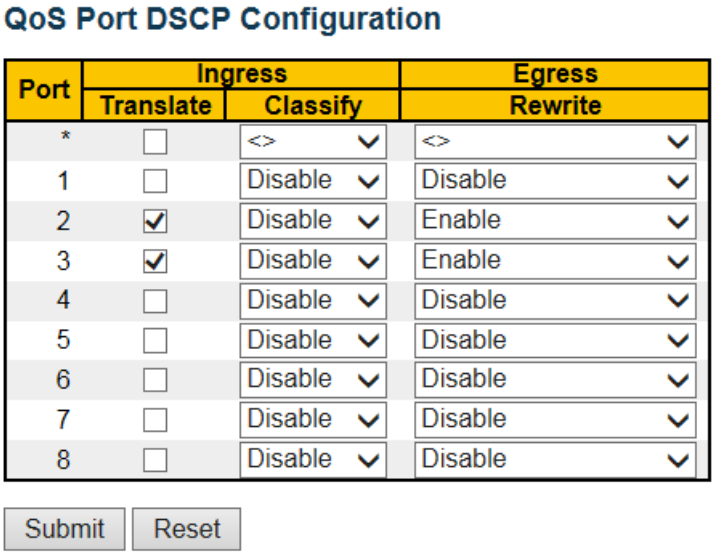


Figure 66 QoS Port DSCP Configuration

Object	Description
Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
Ingress	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: Translate Classify
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	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.

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

3.12.7 DSCP-Based QoS

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

DSCP-Based QoS Ingress Classification

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

Figure 67 QoS DSCP based QoS Ingress Classification

Object	Description
DSCP	Maximum number of supported DSCP values are 64.
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
Qos Class	QoS class value can be any of (0-7)

DPL	Drop Precedence Level (0-1)

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

3.12.8 DSCP Translation

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

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap 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)

Figure 68 QoS DSCP Translation

Object	Description
DSCP	Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
Ingress	Ingress side DSCP can be first translated to new DSCP before using the

	DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation - Translate Classify
Translation	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 - Remap DP0 Controls the remapping for frames with DP level 0. 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.

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

3.12.9 DSCP Classification

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

DSCP Classification

QoS Class	DPL	DSCP
*	*	<>
0	0	0 (BE)
0	1	0 (BE)
1	0	0 (BE)
1	1	0 (BE)
2	0	0 (BE)
2	1	0 (BE)
3	0	0 (BE)
3	1	0 (BE)
4	0	0 (BE)
4	1	0 (BE)
5	0	0 (BE)
5	1	0 (BE)
6	0	0 (BE)
6	1	0 (BE)
7	0	0 (BE)
7	1	0 (BE)

Submit Reset

Figure 69 DSCP Classification

Object	Description
QoS Class	Actual QoS class.
DPL	Actual Drop Precedence Level.
DSCP	Select the classified DSCP value (0-63).

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

3.12.10 QoS Control List

This page shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the lowest plus sign to add a new QCE to the list.

QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action			
									CoS	DPL	DSCP	
												⊕

Figure 70 QoS Control List configuration

Object	Description
QCE	Indicates the QCE id.
Port	Indicates the list of ports configured with the QCE.
DMAC	Indicates the destination MAC address. Possible values are: Any: Match any DMAC. Unicast: Match unicast DMAC. Multicast: Match multicast DMAC. Broadcast: Match broadcast DMAC. The default value is 'Any'.
SMAC	Match specific source MAC address or 'Any'. If a port is configured to match on DMAC/DIP, this field indicates the DMAC.
Tag Type	Indicates tag type. Possible values are: Any: Match tagged and untagged frames. Untagged: Match untagged frames. Tagged: Match tagged frames. The default value is 'Any'.

VID	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
PCP	Priority Code Point: Valid values of PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
DEI	Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.
Frame Type	Indicates the type of frame. Possible values are: Any: Match any frame type. Ethernet: Match EtherType frames. LLC: Match (LLC) frames. SNAP: Match (SNAP) frames. IPv4: Match IPv4 frames. IPv6: Match IPv6 frames.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are: CoS: Classify Class of Service. DPL: Classify Drop Precedence Level. DSCP: Classify DSCP value.
Modification Buttons	You can modify each QCE (QoS Control Entry) in the table using the following buttons: ⊕: Inserts a new QCE before the current row. ⓔ: Edits the QCE. ⬆: Moves the QCE up the list. ⬇: Moves the QCE down the list. ⊗: Deletes the QCE. ⊕: The lowest plus sign adds a new entry at the bottom of the QCE listings.

The QCE page includes the following fields:

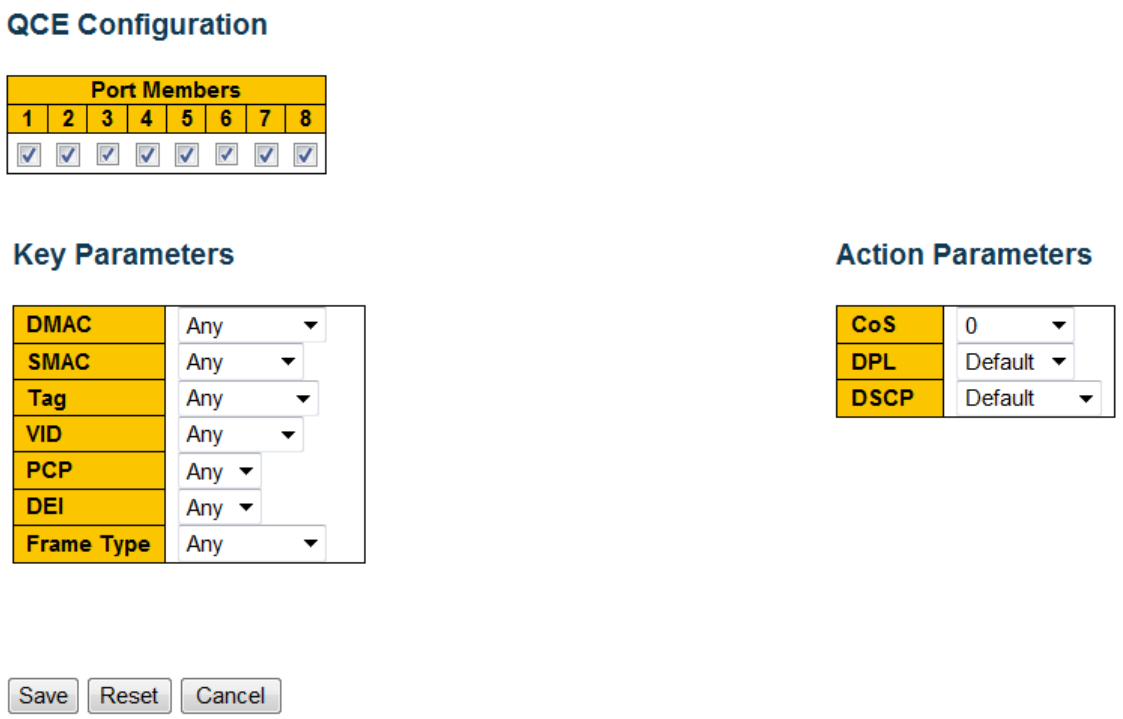


Figure 71 QCE configuration

Object	Description
Port Members	Check the checkbox button to include the port in the QCL entry. By default all ports are included.
Key parameters	Key configuration is described as below: **DMAC** Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast' or 'Any'. **SMAC** Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination MAC address. **Tag** Value of Tag field can be 'Untagged', 'Tagged' or 'Any'. **VID** Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs. **PCP** Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

	DEI Valid value of DEI can be '0', '1' or 'Any'. **Frame Type** Frame Type can have any of the following values: **Any:** Allow all types of frames. **EtherType:** Ether Type Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'. **LLC:** SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'. DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'. Control Valid Control field can vary from 0x00 to 0xFF or 'Any'. **SNAP:** PID Valid PID(a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'. **IPv4:** Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'. Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. If a port is configured to match on DMAC/DIP, this field is the Destination IP address. IP Fragment IPv4 frame fragmented option: 'Yes', 'No' or 'Any'. DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP. Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP. **IPv6:** Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'. Source IP 32 LS bits of IPv6 source address in value/mask format or

	'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination IP address. DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP. Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
Action Parameters	CoS Class of Service: (0-7) or 'Default'. DP Drop Precedence Level: (0-1) or 'Default'. DSCP DSCP: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'. 'Default' means that the default classified value is not modified by this QCE.

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

3.12.11 Storm Control

Storm control for the switch is configured on this page.

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

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

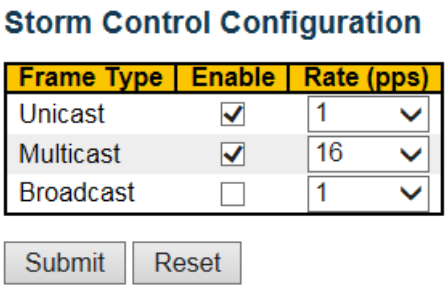


Figure 72 Storm control configuration

Object	Description
Frame Type	The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.
Enable	Enable or disable the storm control status for the given frame type.
Rate	The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K.

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

3.13 Mirror

Configure port Mirroring on this page.

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:

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

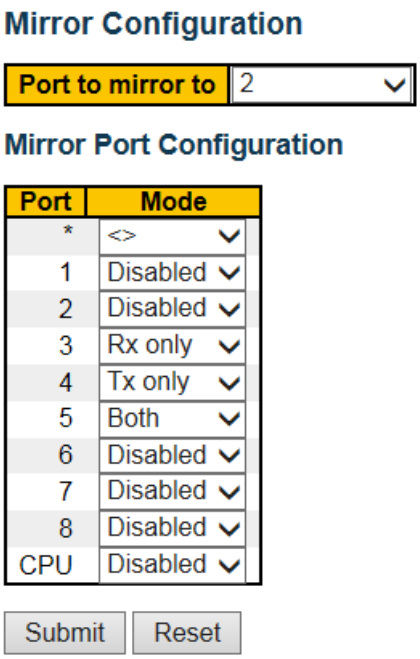


Figure 73 mirror configuration

Object	Description
Port to mirror	**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**.

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

3.14 GVRP

3.14.1 Global Config

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

GVRP Configuration

☐ Enable GVRP

Parameter	Value
Join-timer:	20
Leave-timer:	60
LeaveAll-timer:	1000
Max VLAN:	20

Submit

Figure 74 GVRP configuration

Object	Description
GVRP Protocol timers	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 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 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 number of VLANs	When GVRP is enabled a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off.

Buttons	
Submit	Click to save changes.

3.14.2 Port Config

This page allows you to enable a port for GVRP.

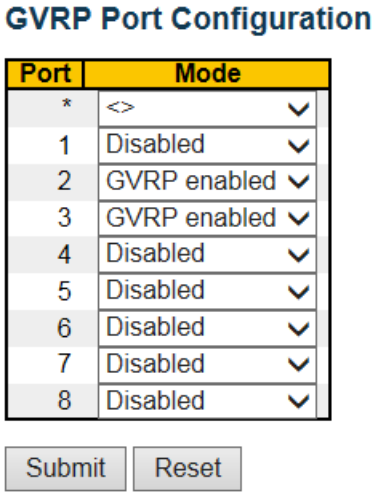


Figure 75 GVRP port configuration

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

3.15 DT-Ring

This page provides Ring related configuration.

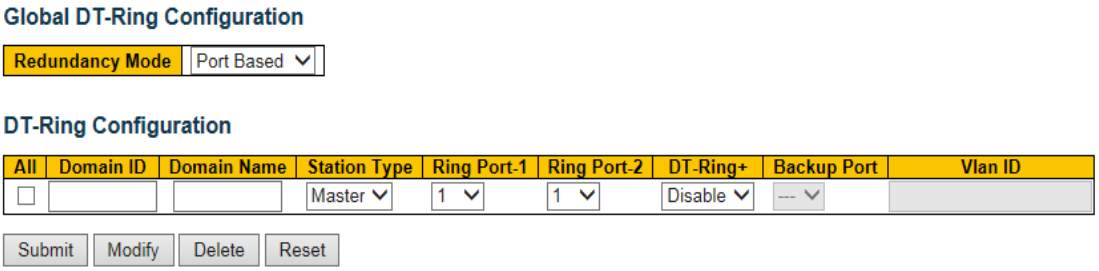


Figure 76 DT-Ring Configuration

Object	Description
Global DT-Ring Configuration	
Redundancy Mode	Configure DT-Ring redundant ring mode, port-based (DT-Ring-Port) or VLAN-based (DT-Ring-VLAN).
DT-Ring Configuration	
Domain ID	The domain ID is used to distinguish different rings. One switch supports a maximum of 16 VLAN-based rings, the number of port-based rings depends on the number of switch ports.
Domain Name	Configure the domain name.
Station Type	Select the switch role in a ring. # Master: One ring has only one master. The master sends DT-Ring protocol packets and detects the status of the ring. When the ring is closed, the two ring ports on the master are in forwarding and blocking state respectively. # Slave: A ring can include multiple slaves. Slaves listen to and forward DT-Ring protocol packets and report fault information to the master.
Ring Port-1/Ring Port-2	Selecting ring port(s). # Each ring port must be unique, CANNOT be configured in different groups; 2 ring ports between ring CANNOT be the same. # When role is ring/master, one ring port is **forward port** and another is **block port**. The block port is redundant port; it is blocking port in normal state. # When role is ring/slave, both ring ports are **forward port**.
DT-Ring+	Enable/disable DT-Ring+. # When role is dual-homing, one ring port is **primary port** and another is

	backup port. This backup port is redundant port; it is blocking port in normal state.
Backup Port	Set a port to backup port. Enable DT-Ring+ before setting backup port.
VLAN ID	Select the VLANs for the ring port. # When there are multiple VLANs, you can separate the VLANs by a comma (,) and an en dash (-), where an en dash is used to separate two consecutive VLAN IDs and a comma is used to separate two inconsecutive VLAN IDs.

Buttons	
Submit	Click to save changes.
Modify	Modify config.
Delete	Delete config.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click a DT-Ring entry in Figure 76 to show DT-Ring and port status, as shown in Figure 77.

DT-Ring Information

Domain ID	1
Domain Name	a
Station Type	Master
Ring State	Close
Ring Port-1	1 | FORWARD
Ring Port-2	2 | BLOCK
Change Time	1 | Clear
Vlan List	---

DT-Ring+ Information

DT-Ring+	Enable
Backup Port	3
Device-0	
Backup Port	3 | BLOCK
Equipment IP	192.168.0.220
Equipment MAC	00-01-c1-01-00-02
Device-1	
Backup Port	6 | BLOCK
Equipment IP	192.168.0.26
Equipment MAC	00-1e-cd-11-01-b1

Figure 77 DT-Ring State

3.16 DRP

This page provides DRP related configuration.

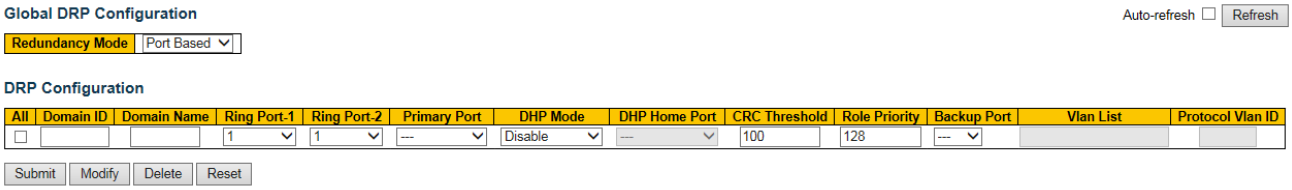


Figure 78 DRP Configuration

Object	Description
Global DRP Configuration	
Redundancy Mode	Configure DRP redundant ring mode, port-based (DRP-Port) or VLAN-based (DRP-VLAN).

	# DRP-Port-Based: forwards or blocks packets based on specific ports. # DRP-VLAN-Based: forwards or blocks packets based on VLANs. If a port is in blocking state, only the data packets of the specified VLAN are blocked. Therefore, multiple VLANs can be configured on tangent ring ports. A port can belong to different DRP rings according to VLAN configurations.
DRP Configuration	
Domain ID	Each ring has a unique domain ID. One switch supports a maximum of 8 VLAN-based rings, the number of port-based rings depends on the number of switch ports.
Domain Name	Configure the domain name.
Ring Port-1/Ring Port-2	Selecting ring port(s). # When role is Root/B-ROOT, one ring port is **forward port** and another is **block port**. The block port is redundant port; it is blocking port in normal state. # When role is Normal, both ring ports are **forward port**.
Primary Port	Configure the primary port. When the ring is closed, the primary port on root is in forwarding state.
DHP Mode	configure the DHP mode. # The implementation of DHP is based on DRP. The role election and assignment mechanism of DHP is the same as that of DRP. DHP provides link backup through the configuration of Home-node, Normal-node, and Home-port.
DHP Home Port	Configure the Home-port for a DHP Home-node. # If there is only one device in DHP link, the both ring ports of the Home-node must be configured as the Home-port.
CRC Threshold	Configure the CRC threshold. # This parameter is used in root election. The system counts the number of received CRCs. If the number of CRCs of one ring port exceeds the threshold, the system considers the port to have CRC degradation. As a result, the CRC degradation value is set to 1 in the vector of the Announce packet of the port.

	# If the two compared devices have the same link status value, the values of CRC degradation status are compared. The device with a larger CRC degradation status value is considered to have a larger vector. If the CRC degradation status value of all compared devices is 1, the device with a larger CRC degradation rate value is elected as the Root.
Role Priority	Configure the priority of a switch. # If the two compared devices have the same link status value and CRC degradation value, the values of role priority, IP addresses, and MAC addresses are compared sequentially. The device with a larger value is elected as the Root.
Backup Port	Configure the backup port.
VLAN List	Select the VLANs managed by current DRP-VLAN-Based ring.
Protocol Vlan ID	The VLAN ID must be one of service VLAN. # DRP packets with the VLAN ID serve as the basis for the diagnosis and maintenance of the DRP-VLAN-Based ring.

Buttons	
Submit	Click to save changes.
Modify	Modify config.
Delete	Delete config.
Reset	Click to undo any changes made locally and revert to previously saved values.

Click a DRP entry in Figure 78 to show DRP and port status, as shown in Figure 79.

DRP Information

Domain ID	1
Domain Name	a
Role State	ROOT
Ring State	Close
Ring Port-1	1 | FORWARD
Ring Port-2	2 | BLOCK
Primary Port	Ring Port-1
DHP Mode	Disable
DHP Home Port	---
CRC Threshold	100
Role Priority	128
Backup Port	3 | INIT

Figure 79 DRP State

4 Monitor

4.1 System

4.1.1 System Information

The switch system information is provided here.

System Information

System	
Contact	86-10-88798888
Name	sicom3008pn-8ge-l15-l15-c
Location	Building No.2,Shixing Avenue 30#,Shijingshan District,Beijing
Hardware	
MAC Address	00-1e-cd-01-f8-b9
Chip ID	VSC7425
Time	
System Date	2000-01-01T20:13:41+00:00
System Uptime	0d 20:13:43
Software	
Software Version	v00.00.10B01
Software Date	2018-06-12T14:52:29+08:00

Figure 80 system information_SICOM3008PN

Object	Description
Contact	The system contact configured in Configuration | System | Information | System Contact.
Name	The system name configured in Configuration | System | Information | System Name.
Location	The system location configured in Configuration | System | Information | System Location.
MAC Address	The MAC Address of this switch.
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.

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

4.1.2 CPU Load

This page displays the CPU load, using line chart.

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 1~256 samples (maximum 256) are graphed, and the last numbers are displayed as text as well.

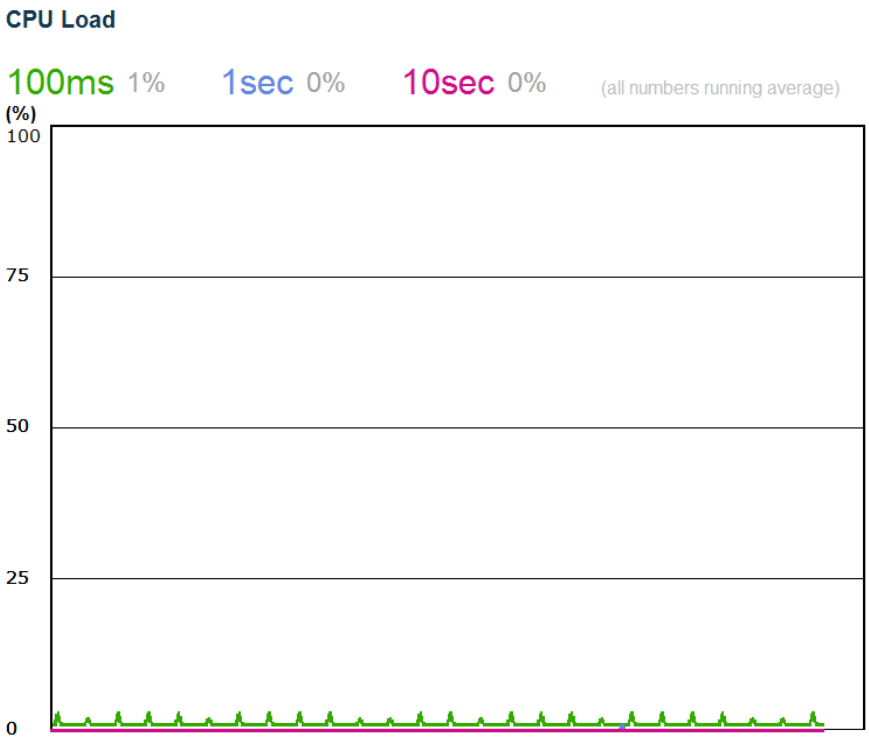


Figure 81 CPU load

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

4.1.3 IP Status

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

IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80:1::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-01-c1-00-00-00	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.2/24	
VLAN1	IPv6	fe80:2::201:c1ff:fe00:0/64	

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>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.0.34	VLAN1:f4-8e-38-a4-fb-67
fe80:2::201:c1ff:fe00:0	VLAN1:00-01-c1-00-00-00

Figure 82 ip status

Object	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 Routes	
Network	The destination IP network or host address of this route.
Gateway	The gateway address of this route.

Status	The status flags of the route.
Neighbor cache	
IP Address	The IP address of the entry.
Link Address	The Link (MAC) address for which a binding to the IP address given exist..

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

4.1.4 System Log

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

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

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

The "Start from ID" input field allow the user to change the starting point in this table.

Clicking the Refresh button will update the displayed table starting from that or the closest next entry match.

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

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

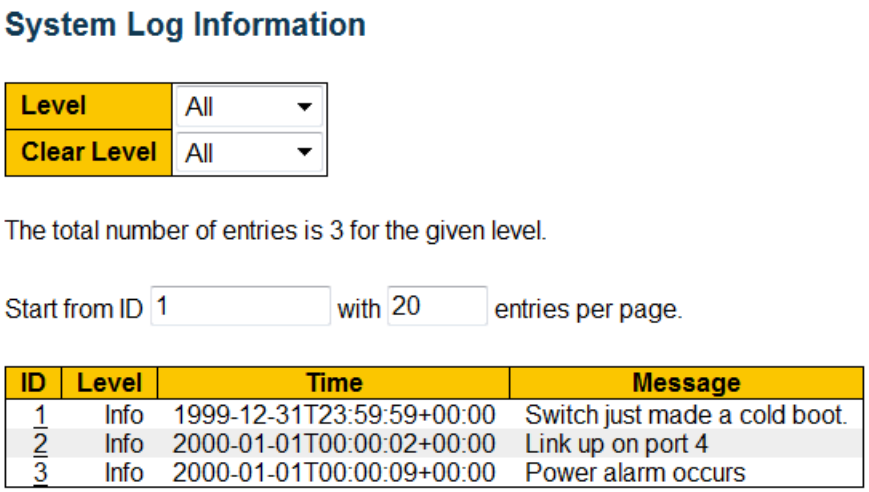


Figure 83 System Log information

Object	Description

ID	The identification of the system log entry.
Level	The level of the system log entry. Info: The system log entry is belonged information level. Warning: The system log entry is belonged warning level. Error: The system log entry is belonged error level.
Time	The occurred time of the system log entry.
Message	The detail message of the system log entry.

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

4.1.5 System Detailed Log

The switch system detailed log information is provided here.

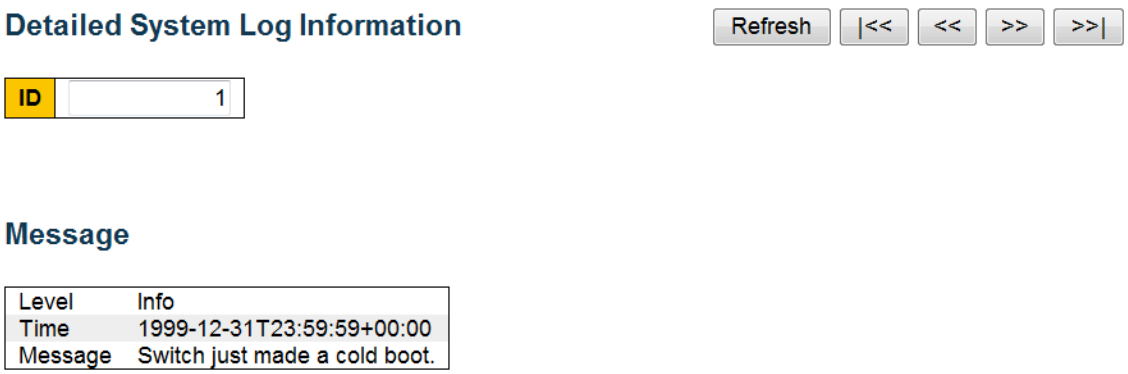


Figure 84 detailed log information

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

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

4.1.6 System Alarm

Current Alarm is provided on this page.

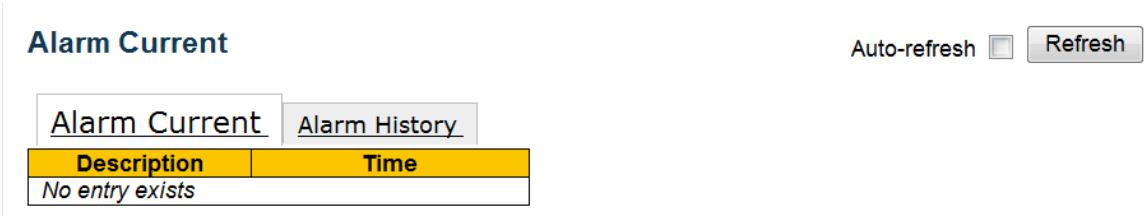


Figure 85 Alarm Current

Object	Description
Description	Alarm Type Description..
Time	Alarm occurrence date time.

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

4.2 Ports

4.2.1 Ports State

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

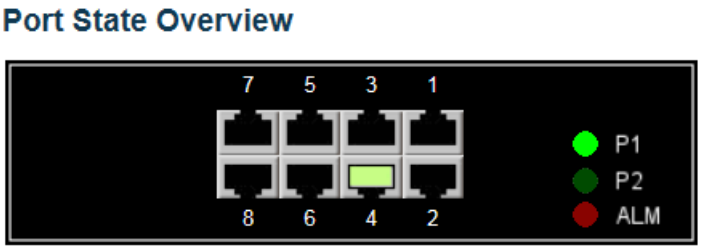


Figure 86 port state overview _SICOM3008PN

The port states are illustrated as follows:

RJ45 ports			
SFP ports			
State	Disabled	Down	Link

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

4.2.2 Trafice Overview

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

Port Statistics Overview

Auto-refresh ☐ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	4	0	384	0	0	0	0	0
2	548	285	72008	201076	0	0	0	0	38
3	0	4	0	384	0	0	0	0	0
4	3798	958	445085	264270	0	0	0	0	431
5	0	4	0	384	0	0	0	0	0
6	0	4	0	384	0	0	0	0	0
7	0	4	0	384	0	0	0	0	0
8	0	4	0	384	0	0	0	0	0

Figure 87 port traffic statistics

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

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

4.2.3 QoS Statistics

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

Queuing Counters

Auto-refresh Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	3836	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1624
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

Figure 88 QoS statistics

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

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

4.2.4 QCL Status

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

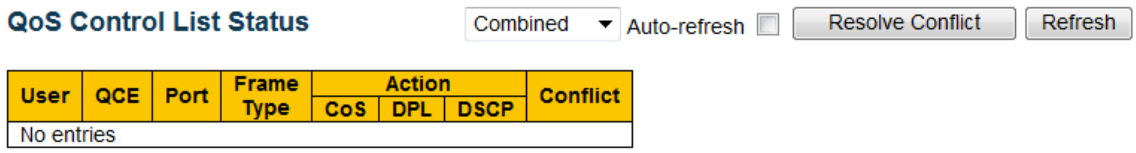


Figure 89 QCL Status

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

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

4.2.5 Detailed Statistics

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

The selected port belongs to the currently selected stack unit, as reflected by the page header.

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

Detailed Port Statistics Port 1 Port 1 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Figure 90 detailed port statistics

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

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.	
Receive and Transmit Queue Counters	
The number of received and transmitted packets per input and output queue.	
Receive Error Counters	
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short [1] frames received with valid CRC.
Rx Oversize	The number of long [2] frames received with valid CRC.
Rx Fragments	The number of short [1] frames received with invalid CRC.
Rx Jabber	The number of long [2] frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process. [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.

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

4.3 DHCP

4.3.1 DHCP Server

4.3.1.1 Statistics

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

DHCP Server Statistics

Auto-refresh Refresh Clear

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

Figure 91 DHCP server

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

DISCOVER	Number of DHCP DISCOVER messages received.
REQUEST	Number of DHCP REQUEST messages received.
DECLINE	Number of DHCP DECLINE messages received.
RELEASE	Number of DHCP RELEASE messages received.
INFORM	Number of DHCP INFORM messages received.
DHCP Message Sent Counters	
OFFER	Number of DHCP OFFER messages sent.
ACK	Number of DHCP ACK messages sent.
NAK	Number of DHCP NAK messages sent.

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

4.3.1.2 Binding

This page displays bindings generated for DHCP clients.

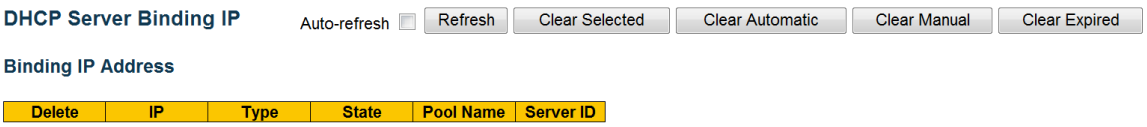


Figure 92 DHCP server binding ip

Object	Description
IP	IP address allocated to DHCP client.
Type	Type of binding. Possible types are Automatic, Manual, Expired.
State	State of binding. Possible states are Committed, Allocated, Expired.

Pool Name	The pool that generates the binding.
Server ID	Server IP address to service the binding.

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

4.3.1.3 Declined IP

This page displays declined IP addresses.

Figure 93 DHCP server declined IP

Object	Description
Declined IP	List of IP addresses declined.

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

Refresh	Click to refresh the page immediately.

4.3.2 DHCP Snooping Table

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

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

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

Use the |<< button to start over.

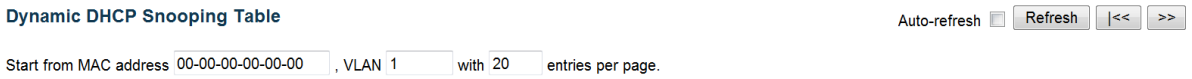


Figure 94 DHCP Snooping Table

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

Buttons

Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Refreshes the displayed table starting from the input fields.
Clear	Flushes all dynamic entries.
|<<	Updates the table starting from the first entry in the Dynamic DHCP snooping Table.
>>	Updates the table, starting with the entry after the last entry currently displayed.

4.4 Security

4.4.1 Accessment Management Statistics

This page provides statistics for access management.

Access Management Statistics

Auto-refresh Refresh Clear

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

Figure 95 Access Management Statistics

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

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

4.4.2 Network

4.4.2.1 NAS

4.4.2.1.1 Switch

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

Network Access Server Switch Status

Auto-refresh ☐ Refresh

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			-	

Figure 96 NAS switch port states

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

	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.

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

4.4.2.1.2 Port

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

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

Figure 97 NAS statistics port

Object	Description
Port State	
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
QoS Class	The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. 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.
Port Counters	
EAPOL Counters	These supplicant frame counters are available for the following

	administrative states: • Force Authorized • Force Unauthorized • Port-based 802.1X • Single 802.1X • Multi 802.1X
Backend Server Counters	These backend (RADIUS) frame counters are available for the following administrative states: • Port-based 802.1X • Single 802.1X • Multi 802.1X • MAC-based Auth.
Last Supplicant/Client Info	Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states: • Port-based 802.1X • Single 802.1X • Multi 802.1X • MAC-based Auth.
Selected Counters	
Selected Counters	The Selected Counters table is visible when the port is in one of the following administrative states: • Multi 802.1X • MAC-based Auth. The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.
Attached MAC Addresses	

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

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

Clear	This button is available in the following modes: • Force Authorized • Force Unauthorized • Port-based 802.1X • Single 802.1X Click to clear the counters for the selected port.
Clear All	This button is available in the following modes: • Multi 802.1X • MAC-based Auth.X Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.
Clear This	This button is available in the following modes: • Multi 802.1X • MAC-based Auth.X Click to clear only the currently selected client's counters.

4.4.3 ACL Status

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

ACL Status

Combined Auto-refresh Refresh

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	Counter	Conflict
arp	All	EType- 0x154e	Filter	Disabled	Disabled	Enabled	Yes	0	No
Profinet_dcp	All	EType- 0x8892	Permit	Disabled	Disabled	Disabled	Yes	0	No
Profinet_mrp	All	EType- 0x88e3	Deny	Disabled	Disabled	Disabled	Yes	0	No
Profinet	All	EType- 0x8892	Permit	Disabled	Disabled	Disabled	Yes	0	No
LLDP	All	EType- 0x88cc	Deny	Disabled	Disabled	Disabled	Yes	0	No
Static	All	EType	Deny	Disabled	Disabled	Disabled	No	0	No
Static	All	EType- 0x8892	Deny	Disabled	Disabled	Disabled	No	0	No
Static	All	EType- 0x8892	Deny	Disabled	Disabled	Disabled	No	0	No
Static	All	EType- 0x8892	Deny	Disabled	Disabled	Disabled	No	0	No
Static	All	EType- 0x8892	Deny	Disabled	Disabled	Disabled	No	0	No

Figure 98 ACL status

Object	Description
User	Indicates the ACL user.
Ingress Port	Indicates the ingress port of the ACE. Possible values are: All: The ACE will match all ingress port. Port: The ACE will match a specific ingress port.
Frame Type	Indicates the frame type of the ACE. Possible values are: Any: The ACE will match any frame type. EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP: The ACE will match ARP/RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/**ICMP**: The ACE will match IPv4 frames with ICMP protocol. IPv4/**UDP**: The ACE will match IPv4 frames with UDP protocol. IPv4/**TCP**: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. IPv6: The ACE will match all IPv6 standard frames.

Action	Indicates the forwarding action of the ACE. Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped. Filter: Frames matching the ACE are filtered.
Rate limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
Mirror	Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled".
CPU	Forward packet that matched the specific ACE to CPU.
CPU Once	Forward first packet that matched the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Conflict	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

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

4.4.4 AAA

4.4.4.1 RADIUS Overview

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

RADIUS Authentication Server Status Overview Auto-refresh Refresh

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

Figure 99 RADIUS servers status

Object	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.

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

4.4.4.2 RADIUS Details

This page provides detailed statistics for a particular RADIUS server.

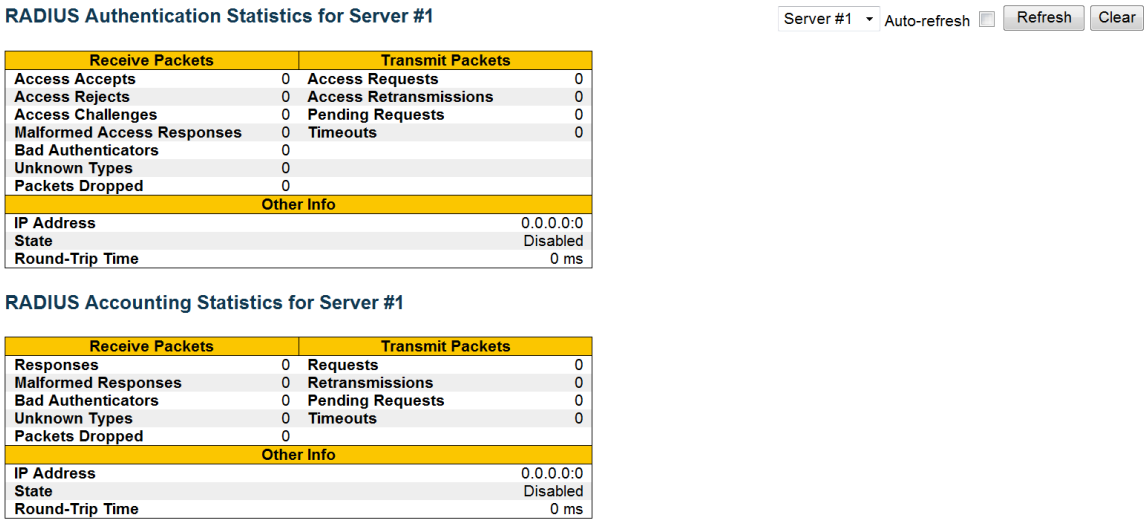


Figure 100 RADIUS Details

Object	Description
RADIUS Authentication Statistics	
Packet Counters	RADIUS authentication server packet counter. There are seven receive and four transmit counters.
Other Info	This section contains information about the state of the server and the latest round-trip time.
RADIUS Accounting Statistics	
Packet Counters	RADIUS accounting server packet counter. There are five receive and four transmit counters.
Other Info	This section contains information about the state of the server and the latest round-trip time.

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

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

4.4.5 Switch

4.4.5.1 RMON

4.4.5.1.1 Statistics

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

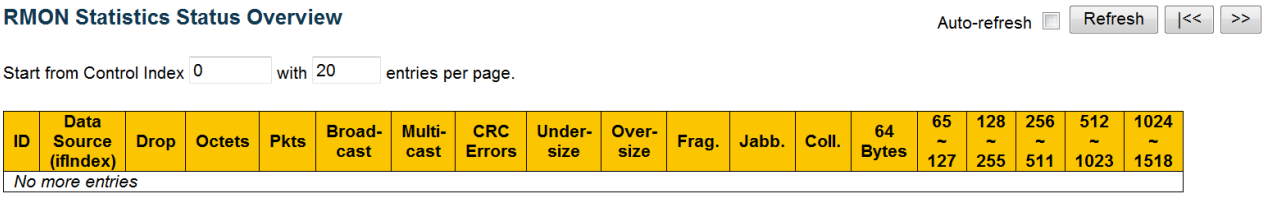


Figure 101 RMON Statistics status

Object	Description
ID	Indicates the index of Statistics entry.
Data Source(ifIndex)	The port ID which wants to be monitored.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broad-cast	The total number of good packets received that were directed to the broadcast address.
Multi-cast	The total number of good packets received that were directed to a multicast address.
CRC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Under-Size	The total number of packets received that were less than 64 octets.
Over-size	The total number of packets received that were longer than 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.

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

4.4.5.1.2 History

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

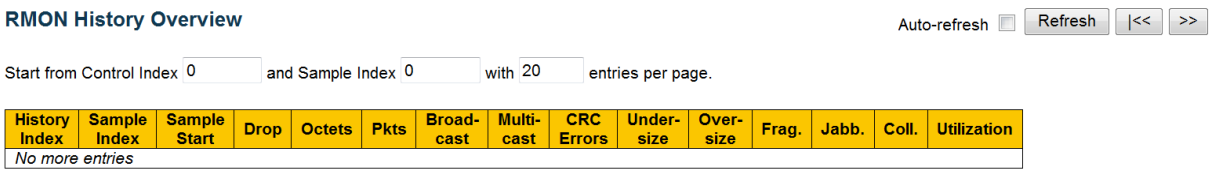


Figure 102 RMON History

Object	Description
History Index	Indicates the index of History control entry.
Sample Index	Indicates the index of the data entry associated with the control entry.
Sample Start	The value of sysUpTime at the start of the interval over which this sample was measured.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	The total number of good packets received that were directed to the broadcast address.
Multicast	The total number of good packets received that were directed to a multicast address.
CRCErrors	The total number of packets received that had a length (excluding framing

	bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	The total number of packets received that were less than 64 octets.
Oversize	The total number of packets received that were longer than 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.

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

4.4.5.1.3 Alarm

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

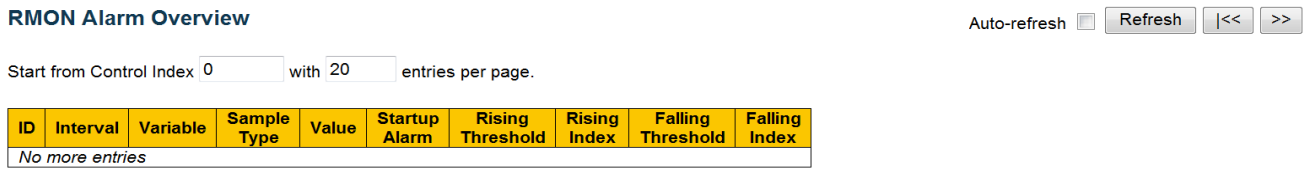


Figure 103 RMON Alarm

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

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

Refresh	Click to refresh the page immediately.
|<<	Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.
>>	Updates the table, starting with the entry after the last entry currently displayed.

4.4.5.1.4 Event

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

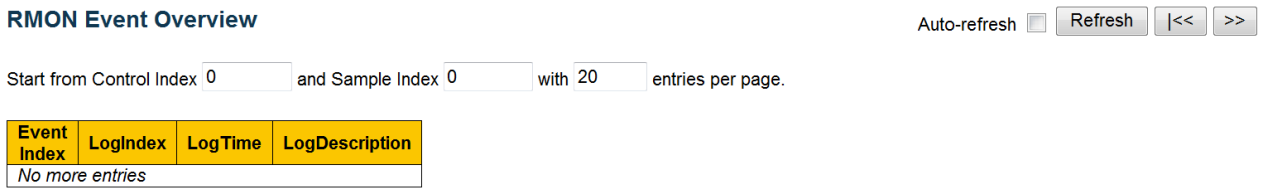


Figure 104 RMON Event

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

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

Refresh	Click to refresh the page immediately.
|<<	Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.
>>	Updates the table, starting with the entry after the last entry currently displayed.

4.5 LACP

4.5.1 System Status

This page provides a status overview for all LACP instances.

LACP System Status

Auto-refresh ☐ Refresh

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

Figure 105 LACP System Status

Object	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.

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

4.5.2 Port Status

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

LACP Status

Auto-refresh ☐ Refresh

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

Figure 106 LACP status

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

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

4.5.3 Port Statistics

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

LACP Statistics

Auto-refresh ☐ Refresh Clear

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

Figure 107 LACP statistics

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

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

4.6 Loop Protection

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

Loop Protection Status

Auto-refresh ☐ Refresh

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

Figure 108 loop protection status

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

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

4.7 Spanning Tree

4.7.1 Bridge Status

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

STP Bridges

Auto-refresh ☐ Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-01-C1-00-00-00	32768.00-01-C1-00-00-00	-	0	Steady	-

Figure 109 STP bridges

Object	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.

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

4.7.2 Port Status

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

STP Port Status

Auto-refresh ☐ Refresh

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	DesignatedPort	Forwarding	0d 05:39:38
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-

Figure 110 STP port status

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

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

4.7.3 Port Statistics

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

STP Statistics

Auto-refresh Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
4	10204	0	0	0	0	0	0	0	0	0

Figure 111 STP statistics

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

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

4.8 IPMC

4.8.1 IGMP Snooping

4.8.1.1 IGMP Snooping Status

This page provides IGMP Snooping 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	-

Figure 112 IGMP Snooping status

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

	querier. 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.

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

4.8.1.2 Groups Information

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

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

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

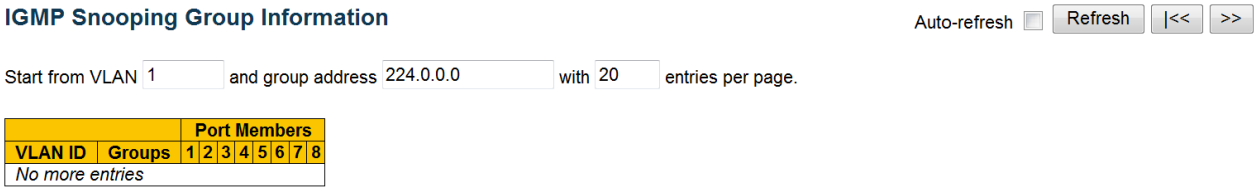


Figure 113 IGMP snooping Groups Information

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

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

|<<	Updates the table, starting with the first entry in the IGMP Group Table.
>>	Updates the table, starting with the entry after the last entry currently displayed.

4.8.1.3 IPv4 SFM Information

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

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

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

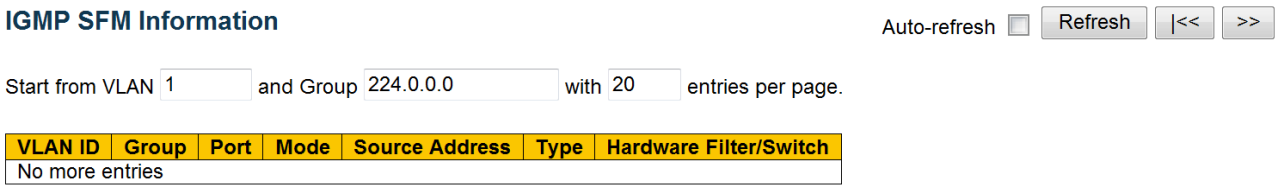


Figure 114 IPv4 SFM Information

Object	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
Type	Indicates the Type. It can be either Allow or Deny.

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

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

4.9 LLDP

4.9.1 Neighbors

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

LLDP Neighbor Information

Auto-refresh Refresh

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

Figure 115 LLDP neighbor information

Object	Description
Local Port	The port on which the LLDP frame was received.
Chassis ID	The **Chassis ID** is the identification of the neighbor's LLDP frames.
Port ID	The **Port ID** is the identification of the neighbor port.
Port Description	**Port Description** is the port description advertised by the neighbor unit.
System Name	**System Name** is the name advertised by the neighbor unit.
System Capabilities	**System Capabilities** describes the neighbor unit's capabilities. The possible capabilities are: 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.

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

4.10 MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

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

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

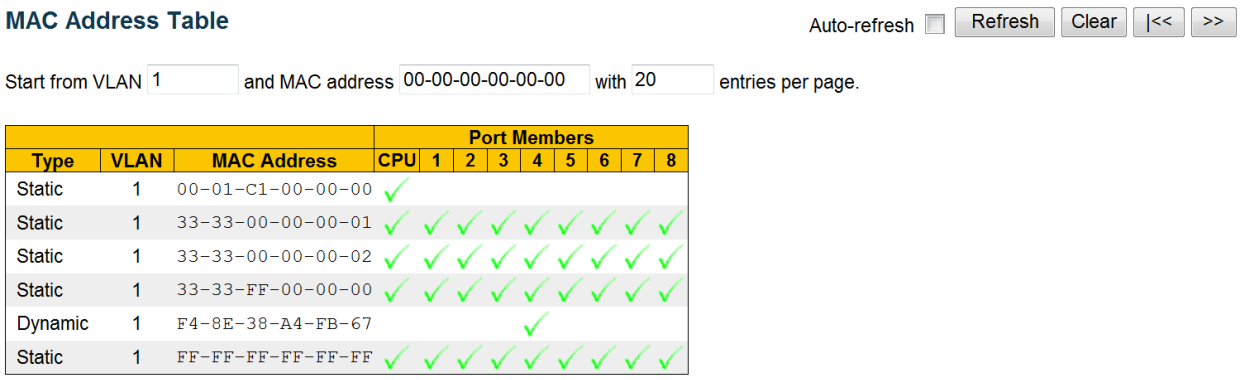


Figure 116 MAC address table

Object	Description
Switch (stack only)	The stack unit where the entry is learned.
Type	Indicates whether the entry is a static or a dynamic entry.
MAC Address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.

Port Members	The ports that are members of the entry.

Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.
Clear	Flushes all dynamic entries.
|<<	Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.
>>	Updates the table, starting with the entry after the last entry currently displayed.

4.11 VLANs

4.11.1 VLANs Membership

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

The "VLAN" input field allows the user to select the starting point in the VLAN Table.

Clicking the Refresh button will update the displayed table starting from that or the closest next VLAN Table match.

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

Figure 117 VLAN Membership status

Object	Description
VLAN User	Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is

	actually configured in hardware.
VLAN ID	VLAN ID for which the Port members are displayed.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. If a port is included in a VLAN, the following image will be displayed: ✓. If a port is in the forbidden port list, the following image will be displayed: ✗. If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed: ✗c. The port will not be a member of the VLAN in this case.

Buttons	
Combined ⌄	Select VLAN Users from this drop down list.
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.

4.11.2 VLANs Ports

This page provides VLAN Port Status.

VLAN Port Status for Combined users Combined Auto-refresh Refresh

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag PVID		No
2	C-Port	☑	All	1	Untag PVID		No
3	C-Port	☑	All	1	Untag PVID		No
4	C-Port	☑	All	1	Untag PVID		No
5	C-Port	☑	All	1	Untag PVID		No
6	C-Port	☑	All	1	Untag PVID		No
7	C-Port	☑	All	1	Untag PVID		No
8	C-Port	☑	All	1	Untag PVID		No

Figure 118 VLAN Port Status

Object	Description
VLAN User	Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware. If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.
Port	The logical port for the settings contained in the same row.
Port Type	Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
Ingress Filtering	Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user.

Frame Type	Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
Port VALN ID	Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user.
Tx Tag	Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port. The field is empty if not overridden by the selected user.
Untagged VLAN ID	If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress. The field is empty if not overridden by the selected user.
Conflicts	Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress. Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority. If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module. The "Combined" user reflects what is actually configured in hardware.

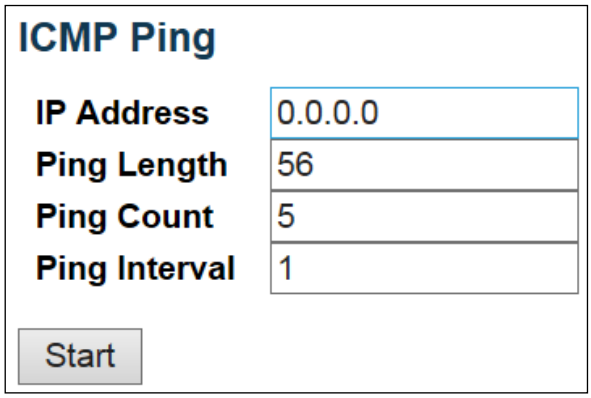
Buttons	
Combined	Select VLAN Users from this drop down list.
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh	Click to refresh the page immediately.

5 Diagnostics

5.1 Ping

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



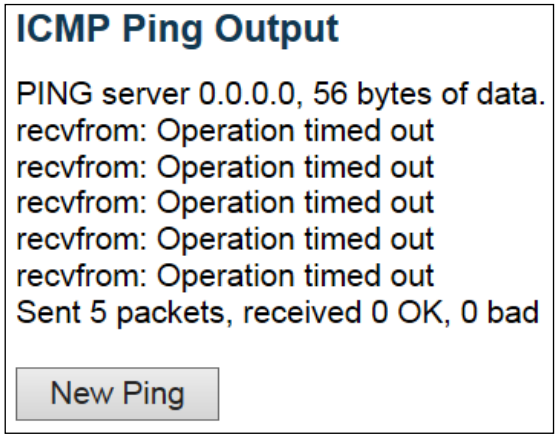


Figure 119 ping

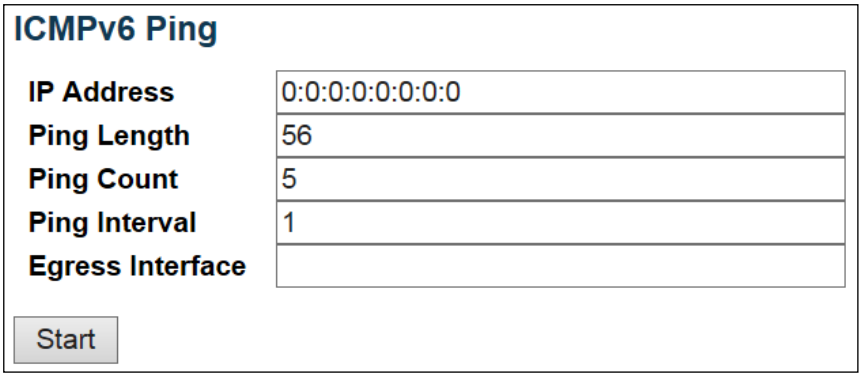
Object	Description
IP Address	The destination IP Address.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Egress Interface (only for IPv6)	The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination. Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.

Buttons	
Start	Click to start transmitting ICMP packets.
New Ping	Click to re-start diagnostics with PING.

5.2 Ping6

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.



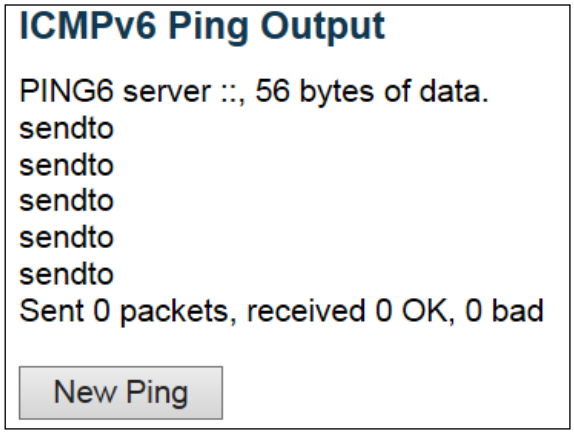


Figure 120 ICMPv6 Ping

Object	Description
IP Address	The destination IP Address.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.
Egress Interface (only for IPv6)	The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes.

	The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination. Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.

Buttons	
Start	Click to start transmitting ICMP packets.
New Ping	Click to re-start diagnostics with PING.

6 Maintenance

6.1 Restart Device

You can restart the switch on this page. After restart, the switch will boot normally.

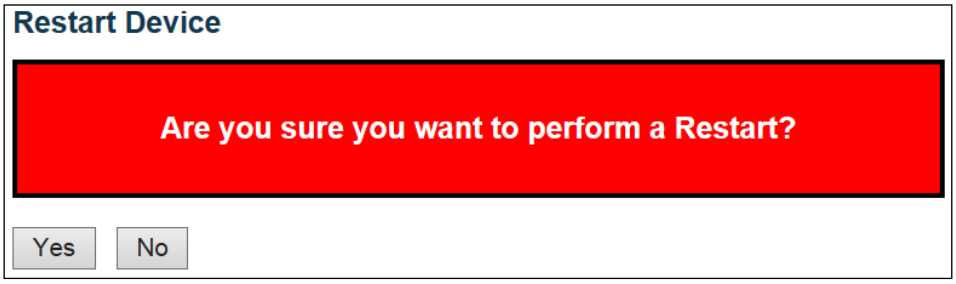


Figure 121 Restart device

Buttons	
Yes	Click to restart device.
No	Click to return to the Port State page without restarting.

6.2 Factory Default

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

The new configuration is available immediately, which means that no restart is necessary.

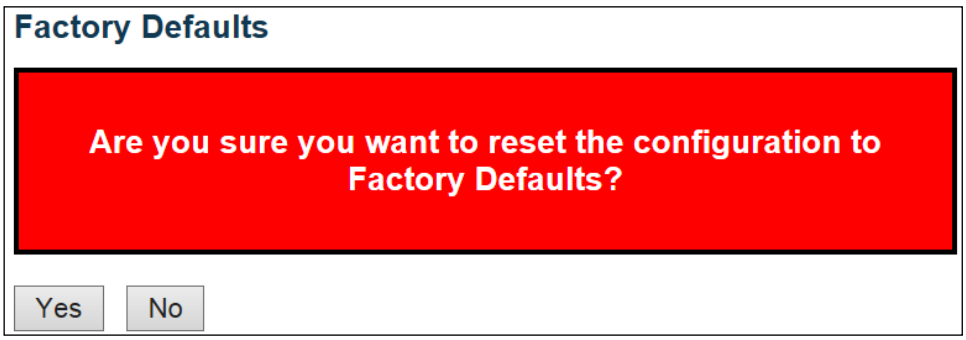


Figure 122 Factory default

Buttons	
Yes	Click to reset the configuration to Factory Defaults.
No	Click to return to the Port State page without resetting the configuration.

6.3 Software

6.3.1 Software Upload

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

Figure 123 Software Upload

Buttons	
Browse	Go to find the software image and click Upload .
Upload	After finding the software image, click the button to update firmware. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

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

6.3.2 Image select

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

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

Note:

In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.

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.

The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

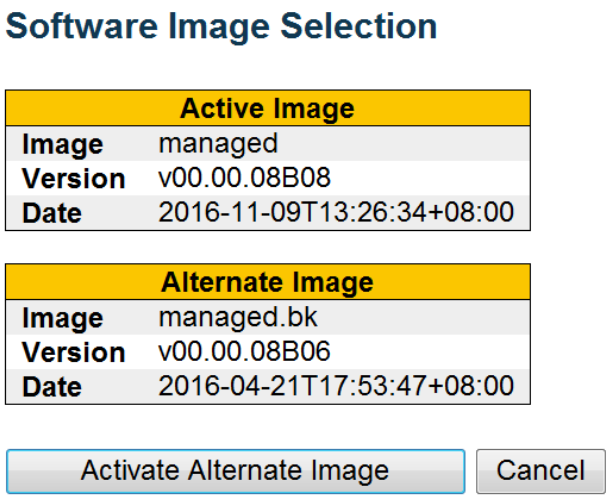


Figure 124 software Image selection

Object	Description
Image	The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named image.bk.
Version	The version of the firmware image.
Data	The date where the firmware was produced.

Buttons	
Activate Alternate Image	Click to use the alternate image. This button may be disabled depending on system state.
Cancel	Cancel activating the backup image. Navigates away from this page.

6.4 Configuration

6.4.1 Save startup-config

Copy running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.

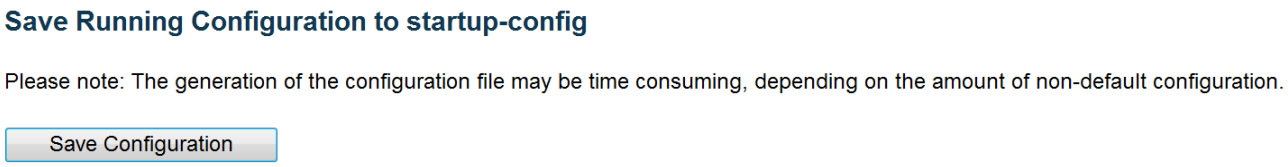


Figure 125 Save startup-config

6.4.2 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 running-config may take a little while to complete, as the file must be prepared for download.

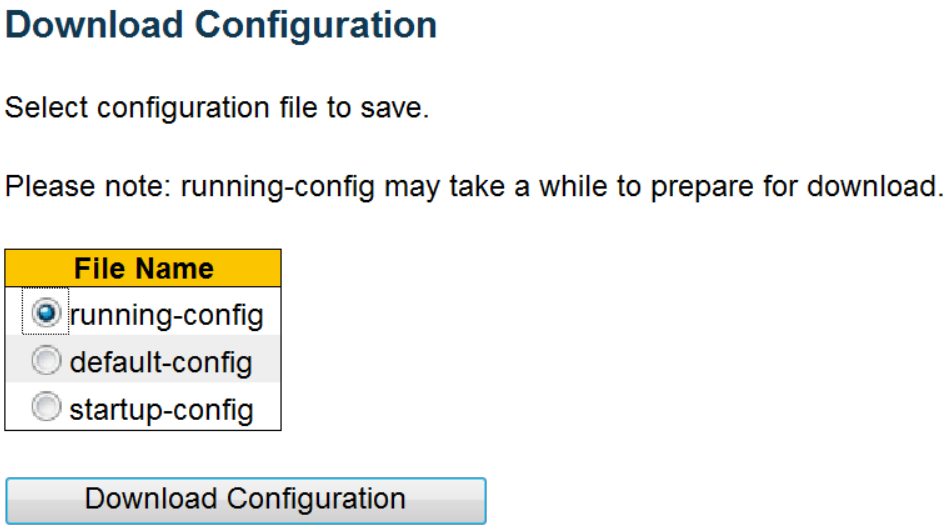


Figure 126 download configuration

6.4.3 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.

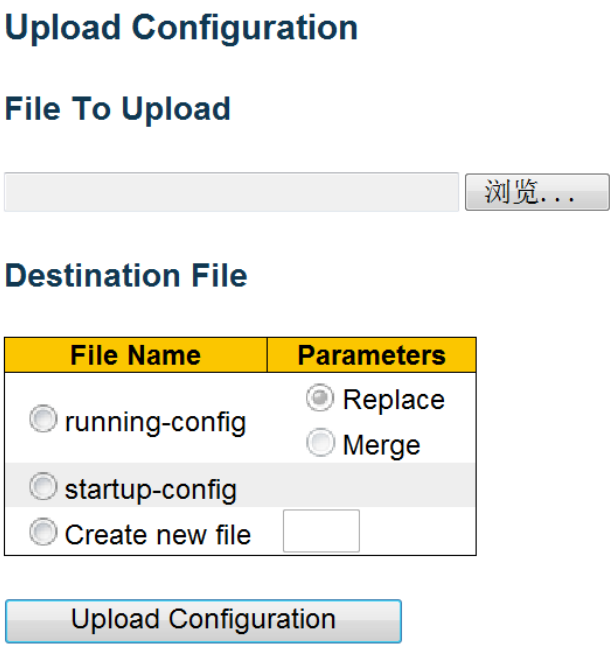


Figure 127 upload configuration

6.4.4 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.

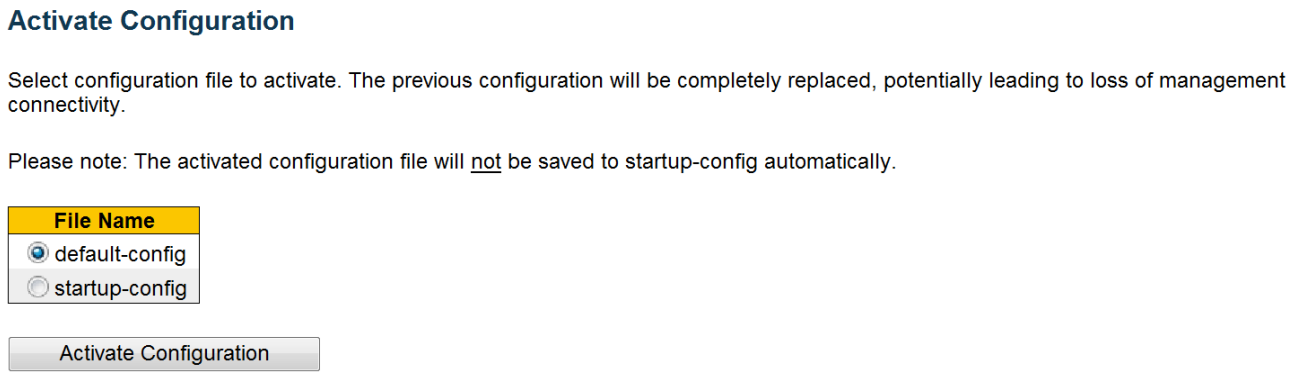


Figure 128 Activate configuration

6.4.5 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.

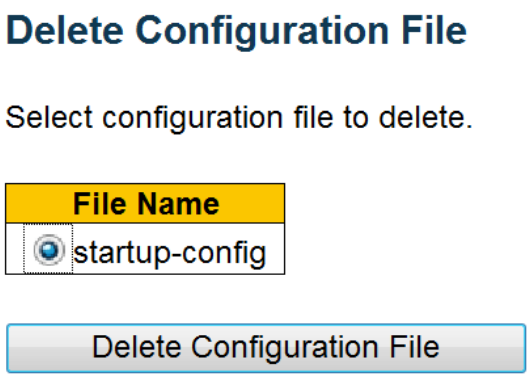


Figure 129 delete configuration file

FAX: +86-10-88796678

Website: http://www.kyland.com

Email: support@kyland.com

For more information about KYLAND products, please visit our website:

http://www.kyland.com