



IGR-842PoE

6 port Gigabit PoE with 2 port
SFP industrial ring manage
switch

Web User Manual





Copyright & Disclaimer

No part of this publication may be reproduced in any form or by any means, whether electronic, mechanical, photocopying, or recording without the written consent of OvisLink Corp.

OvisLink Corp. has made the best effort to ensure the accuracy of the information in this user's guide. However, we are not liable for the inaccuracies or errors in this guide. Please use with caution. All information is subject to change without notice

All Trademarks are properties of their respective holders.

Table of Contents

1. Introduction.....	1
1.1 Overview.....	1
1.2 How to Use This Guide	2
1.3 Firmware Upgrade and Tech Support	2
2. Installing the IGR-842POE.....	3
2.1 Before You Start.....	3
2.2 Package Content	3
2.3 Optional Accessory	4
2.4 Knowing your IGR-842POE	5
2.5 Hardware Installation	6
2.6 LED Table	9
3. Introduce the IGR-842POE.....	11
3.1 Important Information.....	11
3.2 Prepare your PC	11
3.3 Management Interface	11
3.4 Introduction to Web Management	12
4. Web Management: Configuration of IGR-842POE.....	15
4.1 System	15
4.2 Green Ethernet	28
4.3 Port.....	30
4.4 DHCP	32
4.5 Security	39
4.6 Aggregation	105
4.7 Loop Protection	109
4.8 Spanning Tree	110
4.9 IPMC Profile	120
4.10 MVR	122
4.11 IPMC.....	125

4.12 LLDP	136
4.13 PoE.....	146
4.14 MAC Address Tables.....	151
4.15 VLANs	154
4.16 Private VLANs	158
4.17 VCL	161
4.18 Voice VLAN	167
4.19 QoS	170
4.20 Mirroring	192
4.21 GVRP	193
4.22 sFlow	194
4.23 RingV2.....	197
4.24 DDMI	199
5. Web Management: Monitor of IGR-842POE.....	200
5.1 Sysytem.....	200
5.2 Green Ethernet	205
5.3 Ports	206
5.4 DHCP	212
5.5 Security	219
5.6 LACP	238
5.7 Loop Protection	241
5.8 Spanning Tree	241
5.9 MVR	244
5.10 IPMC	247
5.11 LLDP.....	255
5.12 PoE.....	264
5.13 MAC Table	265
5.14 VLANs	266
5.15 VCL	269
5.16 sFlow	270

5.17 RingV2.....	271
5.18 DDMI	272
6. Web Management: Diagnostics of IGR-842POE.....	275
6.1 Ping	275
6.2 Ping6	276
6.3 VeriPHY	277
7. Web Management: Maintenance of IGR-842POE	279
7.1 Restart Device	279
7.2 Factory Default	279
7.3 Software	280
7.4 Configuration	282
8. Trouble Shooting	285
8.1 Incorrect Connections.....	285
8.2 Cabling	285
9. Specifications	286
10. Network Glossary	289
10.1 Cabling	294

1

Introduction



1.1 Overview

The IGR-842POE is a 6 port Gigabit with 2-Port Gigabit TP/SFP slots Ring industrial switch. With robust design and wide working temperature from -40 degree to 70 degree , The IGR-842POE is able to work in any demanding environment such as factory or intersection.

IGR-840POE can be power by two power source for power redundancy to prevent power failure for one power supply. Moreover, IGR-842POE provide the H/W network status detection to provide the quick response network backup. Furthermore, with special chain technology, IGR-842POE is allowed to work with existing network without disconnection current network.

IGR-842POE is also a PoE switch which can power on any PoE client such as IP cameras , VoIP phone.

Note:

If the switch is used in outdoor environment or connect with cable to outdoor , it is suggested to add a lightning arrester to protect the switch..

1.2 How to Use This Guide

IGR-842POE is a SNMP and web smart PoE Switch with many functions. It is recommended that you read through the entire user's guide whenever possible. The user guide is divided into different chapters. You should read at least go through the first 2 chapters before attempting to install the device.

Recommended Reading

Chapter 1: This chapter explains the basic information for IGR-842POE. It is a must read.

Chapter 2: This chapter is about hardware installation. You should read through the entire chapter.

Chapter 3:

- **3.1 Important Information:** This section has information of default setting such as IP, Username, and Password.
- **3.3 Management Interface:** This section introduces Web management, and Console management.
- **3.4 Introduction to Web Management:** This section tells you how to get into the WebUI using HTTP.

1.3 Firmware Upgrade and Tech Support

If you encounter a technical issue that cannot be resolved by information on this guide, we recommend that you visit our comprehensive website support at www.airlive.com. The tech support FAQ are frequently updated with latest information.

In addition, you might find new firmware's that either increase software functions or provide bug fixes for IGR-842POE. You can reach our web page <http://www.airlive.com/product/IGR-842PoE>

2

Installing the IGR-842POE

This chapter describes the hardware features and the hardware installation procedure for the IGR-842POE. For software configuration, please go to chapter 3 for more details.

2.1 Before You Start

It is important to read through this section before you install the IGR-842POE

- The maximum cabling distance is 100 meters by Cat5e RJ45 cable.
- Do not create a network loop.
- Always check the LED lights for troubleshooting

2.2 Package Content

Unpack the contents of the IGR-842POE Plus and verify them against the checklist below.

- One unit of IGR-842POE
- Quick Installation Guide
- Wall mount kit



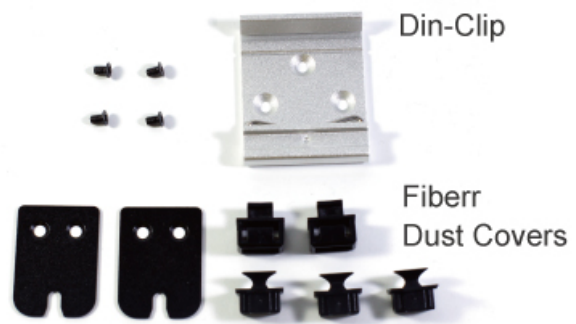
IGR-842POE



Quick Installation Guide



Console Cable



Din-Clip

Fiberr
Dust Covers

Wall Mount Brackets RJ45 Dust Covers

Compare the contents of your IGR-842POE package with the standard checklist above. If any item is missing or damaged, please contact your local dealer for service.

2.3 Optional Accessory

The IGR-842POE has the following optional accessories which you can purchase from AirLive

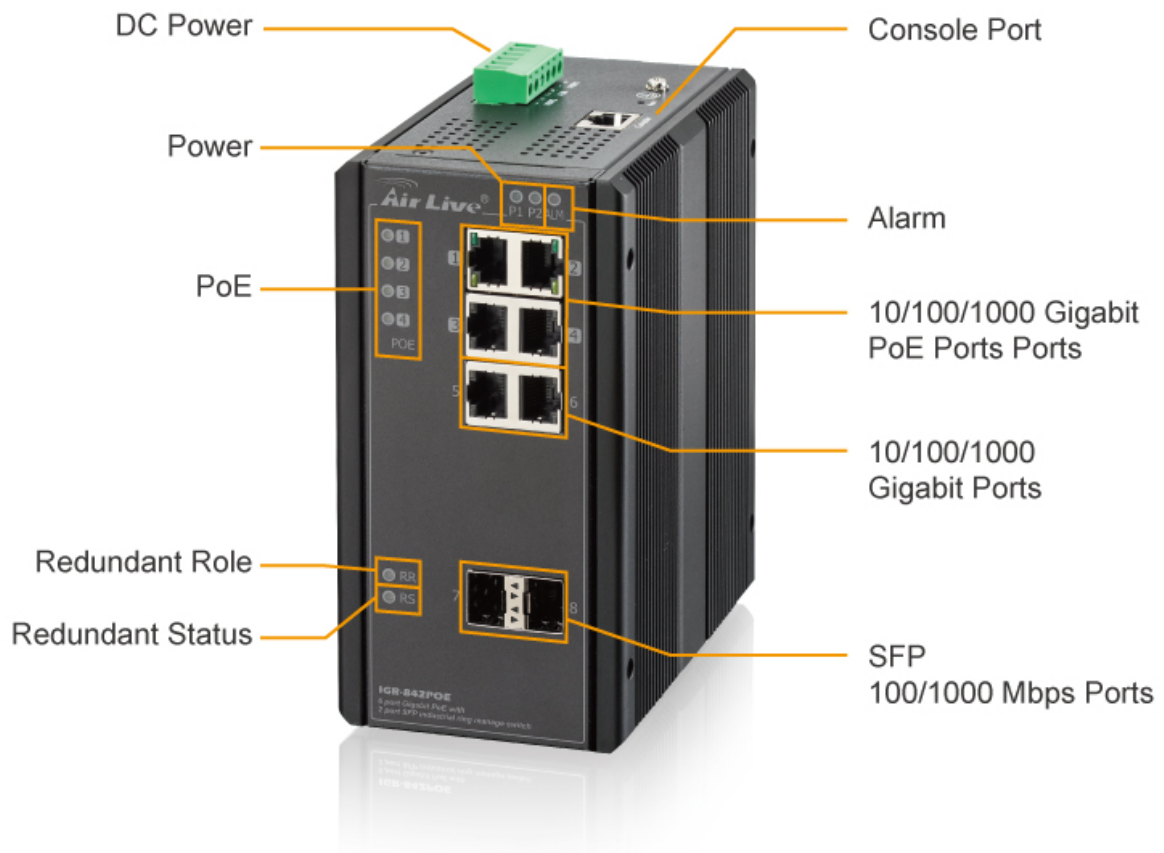
- 1000Base-SX MiniGBIC Transceiver (*Model: SFP-SX v2*) or 1000Base-LX MiniGBIC Transceiver (*Model: SFP-LX v2*) is for your SFP slots of IGR-842POE, it allows you to use fiber cable for extending transmission distance.



Note: While installing MiniGBIC into SFP slot of IGR-842POE, please notice the direction of MiniGBIC is correct, and make sure that MiniGBIC is indeed installed in the IGR-842POE.

2.4 Knowing your IGR-842POE

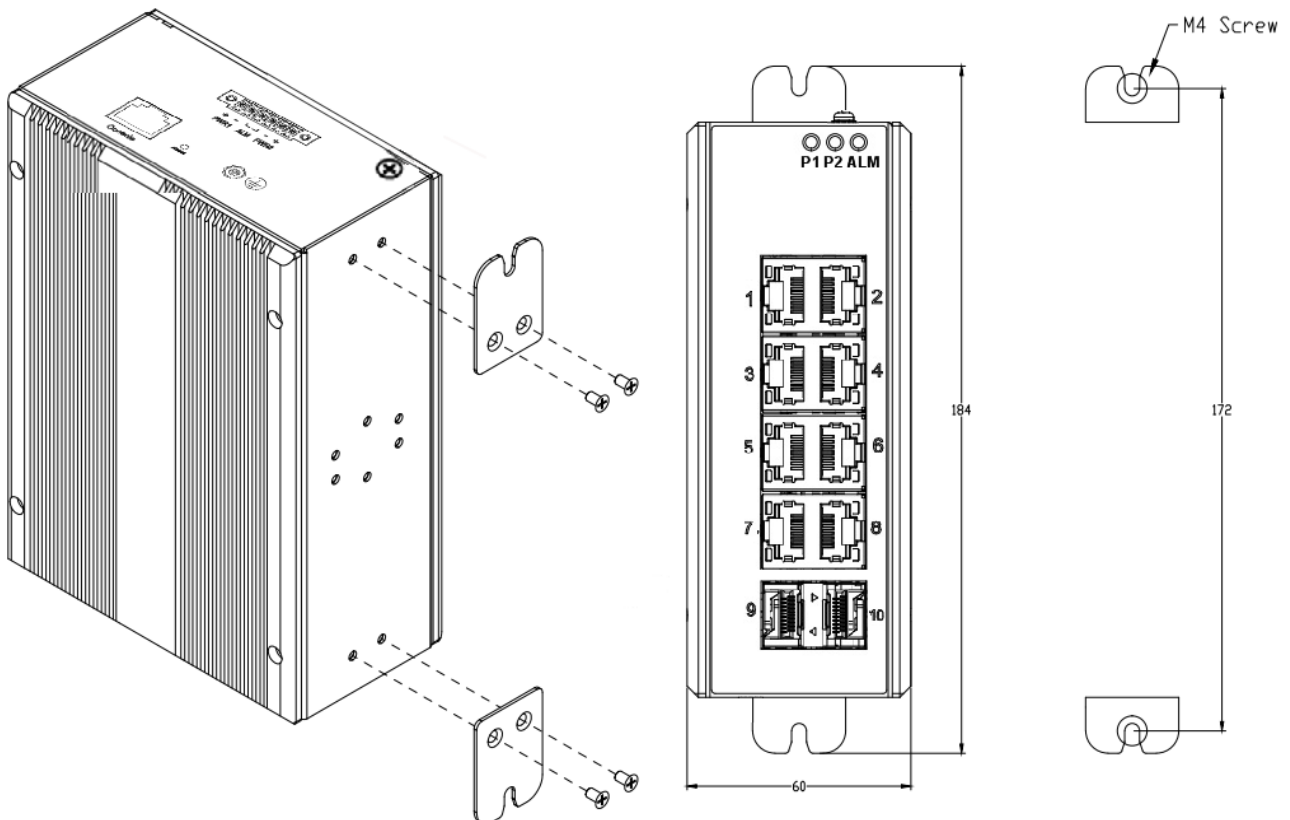
Below are descriptions and diagrams of the product:



2.5 Hardware Installation

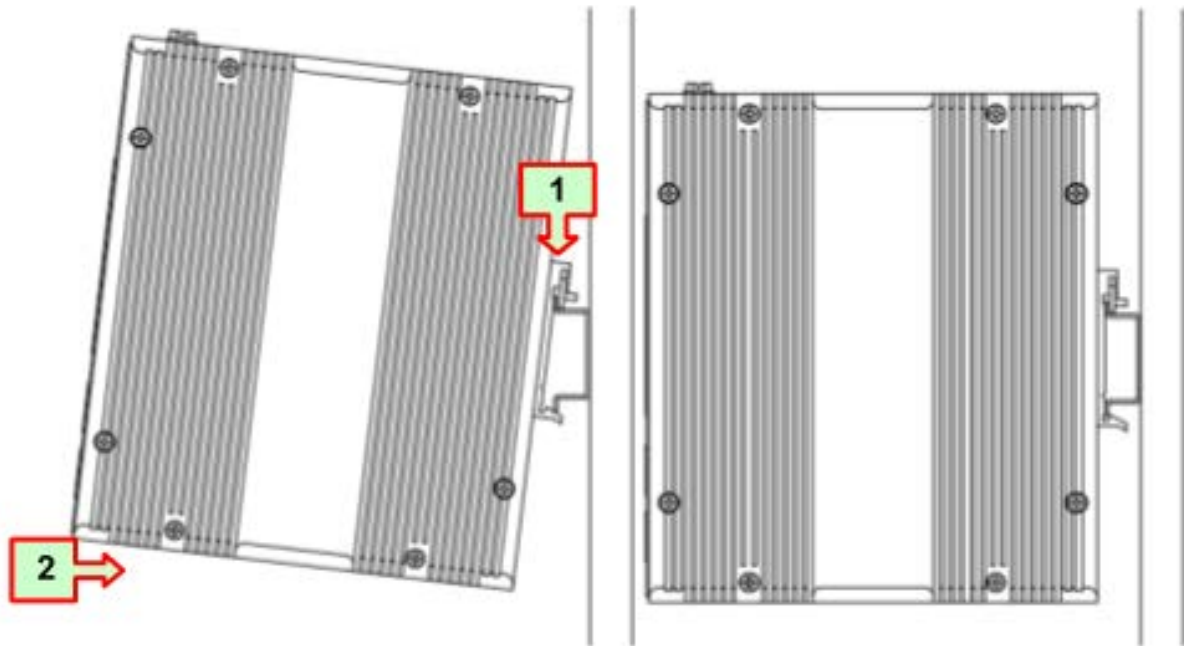
Set the IGR-842POE on a sufficiently large flat space with a power outlet nearby. The surface where you put your IGR-842POE should be clean, smooth, level and sturdy. Make sure there is enough clearance around the IGR-842POE to allow attachment of cables, power cord and allow air circulation.

2.5.1. Wall-mounted Installation



Screw on the wall-mounting plate on with the plate and screws in the accessory kit.

2.5.2. DIN-Rail Mounting

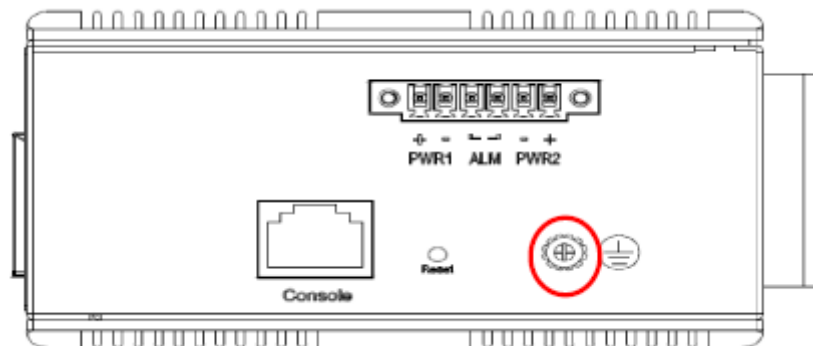


Screw the din-clip with screws in the accessory kit.

Hook the unit onto the din-rail.

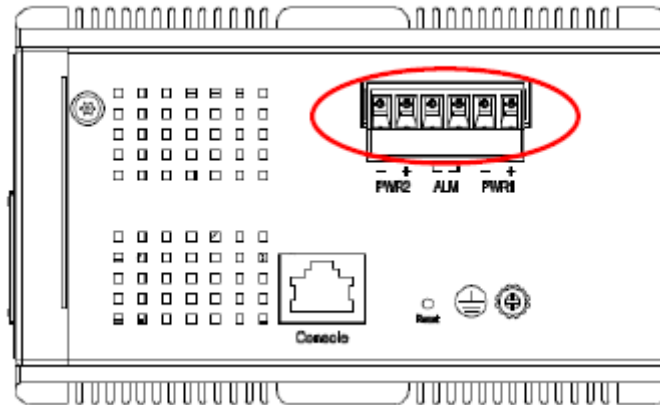
Push the bottom of the unit towards the din-rail until it locks in place.

2.5.3. Ground Connection



IGR-842POE must be properly grounded for optimum system performance.

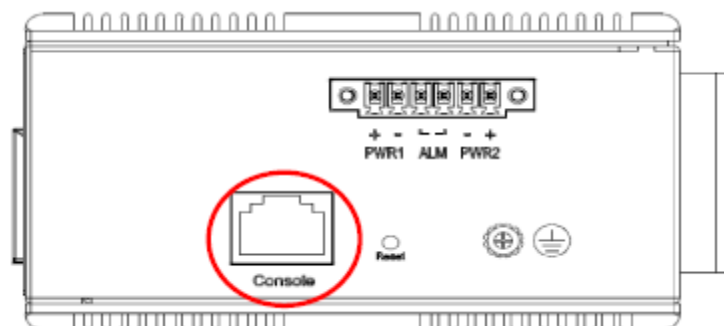
2.5.4. Power On



The DC power interface is a 6-pin terminal block with polarity signs on the top panel. The IGR-842POE can be powered from two power supply (input range 12V – 58V). The DC power connector is a 6-pin terminal block; There is alarm contact on the middle terminal block.

Power Connector (6P Terminal Block)	
Input	DC 12-58V
PWR1 +/-	Power Input 1 +/-
PWR2 +/-	Power Input 2 +/-
ALM	Alarm relay output

2.5.5. Console Connection

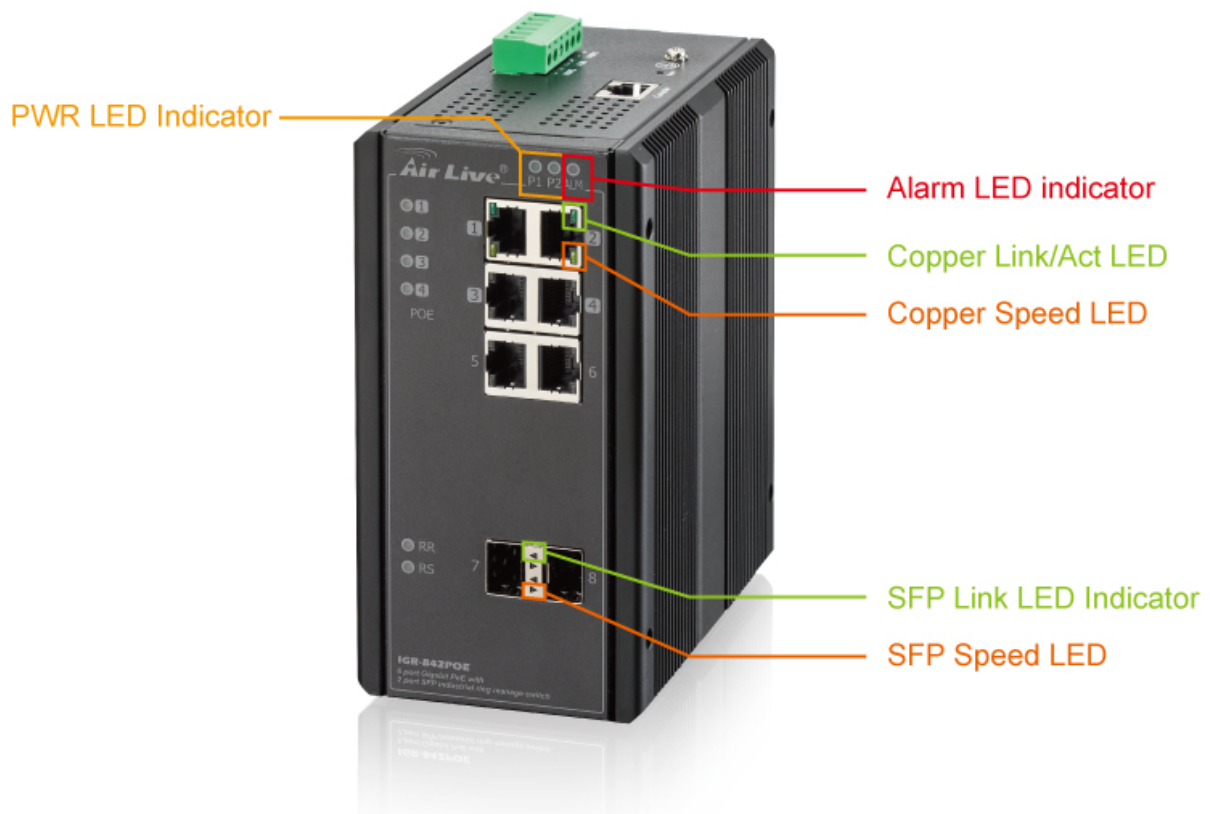


The Console port is for local management by using a terminal emulator or a computer with terminal emulation software.

- DB9 connector connect to computer COM port
- Baud rate: 115200bps
- 8 data bits, 1 stop bit
- None Priority
- None flow control

2.6 LED Table

The LED Indicators gives real-time information of systematic operation status. The following table provides descriptions of LED status and their meaning.



LED	Status	Description
P1	Green	P1 power line has power
	Off	P1 power line disconnect or does not have supply power
P2	Green	P2 power line has power
	Off	P2 power line disconnect or does not have supply power
Alarm	Red	Alarm event occurs
	Off	No alarm

Copper ports Speed	Yellow	A 100 Mbps or a 1000Mbps connection is detected
	Off	No link or a 10 Mbps connection is detected
SFP port Link/Act	Green	Ethernet link up
	Off	Ethernet link down
SFP port Speed	Yellow	SFP port speed 1000Mbps connection is detected.
	Off	No link or a SFP port speed 100Mbps connection is detected

3

Introduce the IGR-842POE

3.1 Important Information

The following information will help you to get start quickly. However, we recommend you to read through the entire manual before you start. Please note the username and password are case sensitive.

- The default IP address is **192.168.2.1**
- The default Subnet Mask is **255.255.255.0**
- The default username is **admin**
- The default password is **airlive**

Note : The default PoE mode is “Disable”

3.2 Prepare your PC

The IGR-842POE can be managed remotely by a PC through RJ-45 cable. The default IP address of the IGR-842POE is **192.168.2.1** with a *subnet mask* of 255.255.255.0. This means the IP address of the PC should be in the range of 192.168.2.2 to 192.168.2.253.

To prepare your PC for management with the IGR-842POE, please do the following:

1. Connect your PC directly to the copper port of IGR-842POE
2. Set your PC's IP address manually to 192.168.2.100 (or other address in the same subnet)

3.3 Management Interface

The IGR-842POE can be configured using on the management interfaces below:

- **Web Management (HTTP):** You can manage your IGR-842POE by simply typing its IP address in the web browser. Most functions of IGR-842POE can be accessed by web management interface. We recommend using this interface for initial configurations. To begin, simply enter IGR-842POE's IP address (**default is 192.168.2.1**) on the web browser. The default username is **admin** and password is **airlive**.

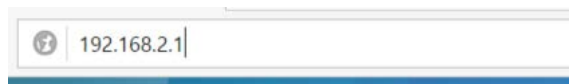
3.4 Introduction to Web Management

The IGR-842POE offers Web Management interfaces for users. Users can easily access and control IGR-842POE via web browsers. The Web-Based Management supports Internet Explorer 10 or later version. If you want to check the cameras' stream, please use Firefox, because other browser does not support the plug-in for video.

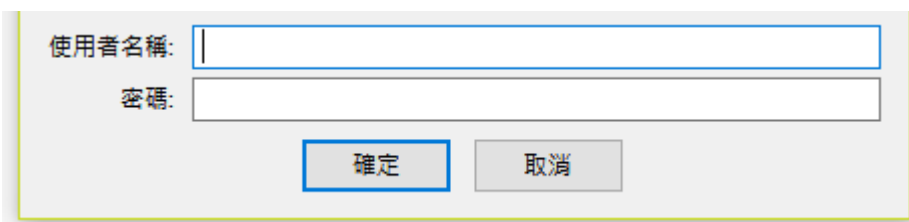
3.4.1. Getting into Web Management

Web Management (HTTP)

1. Launch the Internet Explorer.
2. Type `http://192.168.2.1`. Press "**Enter**".



3. The login screen appears.
4. Key in the user name and password. The default user name is "**admin**" and password is "**airlive**".



使用者名稱:

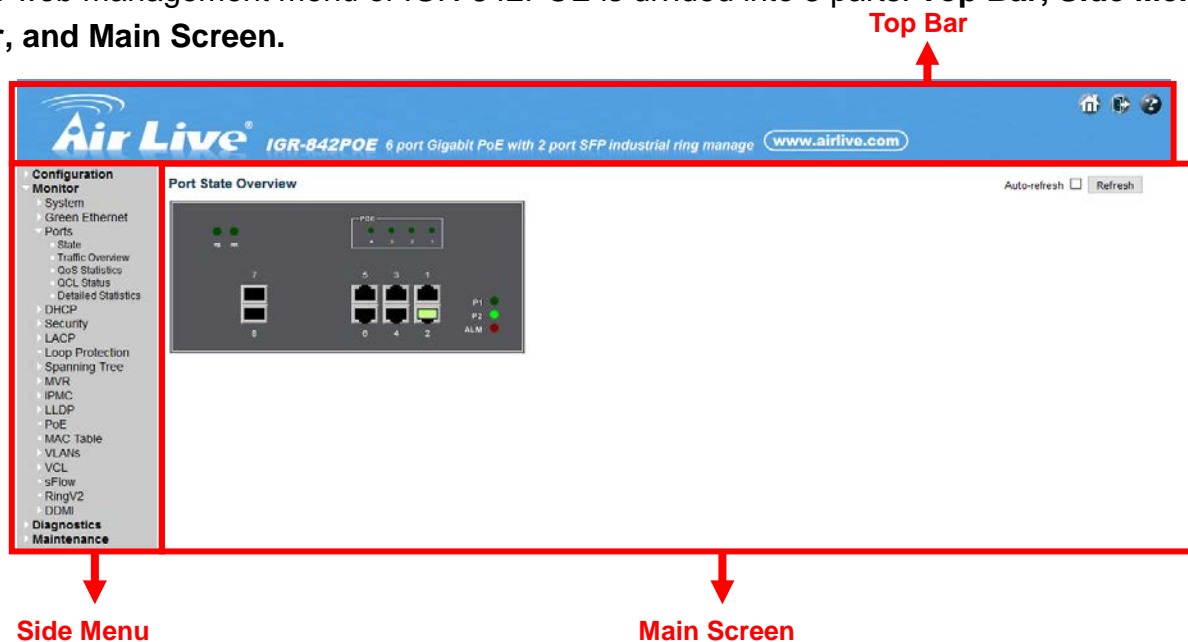
密碼:

5. Click "**Enter**" or "**Login**", then the home screen of the Web-based management appears.



3.4.2. Menu Structure of IGR-842POE

The web management menu of IGR-842POE is divided into 3 parts: **Top Bar**, **Side Menu Bar**, and **Main Screen**.



- **Top Bar:** It display panel GUI. You can direct click the port on the Switch figure on the top of web page. Then, you will see the port information. On the left-top corner, there is a pull-down list for Auto Logout. For the sake of security, we provide auto-logout function to protect you from illegal user as you are leaving. If you do not choose any selection in Auto Logout list, it means you turn on the Auto Logout function and the system will be logged out automatically when no action on the device 3 minutes later. If OFF is chosen, the screen will keep as it is. Default is ON.

- **Side Menu:** All management functions will show in Side Menu, you can choose any one of them to configure its setting. The detailed introduction for all management function will explain in below chapters. The following list is the full function tree for web user interface.
- **Main Screen:** Once choosing any function of Side Menu, the configuration page of the function will show in Main Screen. You can configure the function by instruction of manual.

4

Web Management: Configuration of IGR-842POE

4.1 System

This chapter describes the entire basic configuration tasks which includes the System Information and any manage of the Switch (e.g. Time, Account, IP, Syslog and NTP.)

Please Click Maintenance, Configuration and Save startup-config to save the configuration.

4.1.1. System Information

You can identify the system by configuring the contact information, name, and location of the switch.

The switch system information is provided here.

Web interface

To configure System Information in the web interface:

1. Click Monitor, System and Information.
2. Check the contact information for the system administrator as well as the name and location of the switch. Also indicate the local time zone by configuring the appropriate offset.

System Information Configuration

System Contact	<input type="text"/>
System Name	<input type="text"/>
System Location	<input type="text"/>

Parameter description:

1. Contact

The system contact configured in Configuration | System | Information | System Contact.

2. System Name

Displays the user-defined system name that configured in System | System Information | Configuration | System Name.

3. System Location

The system location configured in Configuration | System | Information | System Location.

4. Button

Save - Click to save changes.

Reset - Click to revert to previously saved values.

4.1.2. System IP

This sector is to provide and config the IP information of the IGR-842POE.

Web Interface

To configure an IP address in the web interface:

1. Click Configuration, System, IP.
2. Click Add Interface then you can create new Interface on the switch.
3. Click Add Route then you can create new Route on the switch
4. Click Save

IP Configuration

Mode	Host <input type="button" value="v"/>
DNS Server	No DNS server <input type="button" value="v"/> <input type="text"/>
DNS Proxy	<input type="checkbox"/>

IP Interfaces

Delete	VLAN	IPv4 DHCP			IPv4		IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		172.16.100.120	24		

Default Gateway

Address
<input type="text"/>

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
--------	---------	-------------	---------	---------------

Parameter description:

IP Configuration

1. Mode

Configure whether the IP stack should act as a Host or a Router :

- Host mode

IP traffic between interfaces will not be routed

- Router

traffic is routed between all interfaces.

2. DNS Sever

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

3. 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

1. Delete

Select this option to delete an existing IP interface.

2. VLAN

The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.

3. 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.

4. 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.

5. IPv4 DHCP Current Lease

For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.

6. IPv4 Address

The IPv4 address of the interface in dotted decimal notation.

If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

7. 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 is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

8. 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.

9. 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

1. Address

The IP address of the gateway valid format is dotted decimal notation.

IP Routes

1. Delete

Select this option to delete an existing IP route.

2. Network

The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or IPv6 :: notation.

3. 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).

4. Gateway

The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.

5. 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

1. Add Interface:

Click to add a new IP interface. A maximum of 8 interfaces is supported.

2. Set Default Gateway

Click to save changes.

3. Add Route:

Click to add a new IP route. A maximum of 32 routes is supported.

4. Save:

Click to save changes.

5. Reset:

Click to revert to previously saved values.

4.1.3. System NTP

Configure NTP on this page

Web Interface

To configure Time in the web interface:

1. Click Configuration, System and Time
2. Specify the Time parameter.

3. Click Save.

NTP Configuration

Mode	Disabled <input type="checkbox"/>
Server 1	<input type="text"/>
Server 2	<input type="text"/>
Server 3	<input type="text"/>
Server 4	<input type="text"/>
Server 5	<input type="text"/>

Parameter description:

1. Mode:

Indicates the NTP mode operation. Possible modes are:

Enabled: Enable NTP client mode operation.

Disabled: Disable NTP client mode operation.

2. 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'.

3. Save:

Click to save changes.

4. Reset:

Click to revert to previously saved values.

4.1.4. System Time

This page allows you to configure the Time Zone.

Web Interface

To configure log configuration in the web interface:

1. Click Configuration, System Time
2. Specify the Time parameter.
3. Click Save.

Time Zone Configuration

Time Zone Configuration	
Time Zone	None ▼
Acronym	<input type="text"/> (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	1 ▼
Hours	20 ▼
Minutes	33 ▼
Seconds	25 ▼

Save Reset

Parameter description:

Time Zone Configuration

1. Time Zone

Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set

2. 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

1. 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)

2. 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).

3. Non 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).

4. Data/Time Configuration**Data/Time settings**

- Week - 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

Save – Click to save changes.

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

4.1.5. System Log

Configure System Log on this page.

Web Interface

To configure log configuration in the web interface:

1. Click Configuration, System Log
2. Specify the Syslog parameters include IP Address of Syslog server and Port number.
3. Evoke the Syslog to enable it.
4. Click Save.

System Log Configuration

Server Mode	Disabled <input type="button" value="v"/>
Server Address	<input type="text"/>
Syslog Level	Info <input type="button" value="v"/>

Parameter description:

1. 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.

2. Acronym :

Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.

3. 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.

4. Buttons

Save – Click to save changes.

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

4.1.6. System Alarm Profile

Alarm Profile is provided here to enable/disable alarm

Web Interface

To configure Alarm Profile in the web interface:

1. Click Configuration, Alarm Profile
2. Enable the Alarm.
3. Click Save

Alarm Profile

ID	Description	Enabled
* *		<input type="checkbox"/>
1	Port 1 Link Down	<input type="checkbox"/>
2	Port 2 Link Down	<input type="checkbox"/>
3	Port 3 Link Down	<input type="checkbox"/>
4	Port 4 Link Down	<input type="checkbox"/>
5	Port 5 Link Down	<input type="checkbox"/>
6	Port 6 Link Down	<input type="checkbox"/>
7	Port 7 Link Down	<input type="checkbox"/>
8	Port 8 Link Down	<input type="checkbox"/>
9	Port 9 Link Down	<input type="checkbox"/>
10	Port 10 Link Down	<input type="checkbox"/>
11	Power Alarm	<input type="checkbox"/>

Parameter description:

1. ID

The identification of the Alarm Profile entry.

2. Description

Alarm Type Description.

3. 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.

4. 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.

Buttons

Save – Click to save changes.

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

Note: When any alarm exists, the Alarm LED will be on (lighted), Alarm Output Relay will also be enabled.

4.2 Green Ethernet

Green Ethernet is a power saving option that reduces the power usage when there is low or no traffic utilization.

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

Green Ethernet works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode.

For ports that are not Green Ethernet -capable the corresponding Green Ethernet checkboxes are grayed out and thus impossible to enable Green Ethernet for.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.

4.2.1.Port Power Saving

This page allows the user to configure the port power savings features.

Web Interface

To configure port power savings in the web interface:

1. Click Green Ethernet, port power savings
2. Specify the ActiPHY, PerfectReach, EEE
3. Click Save

Port Power Savings Configuration

Optimize EEE for Latency

Port Configuration

Port	ActiPHY	PerfectReach	EEE	EEE Urgent Queues									
				1	2	3	4	5	6	7	8		
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Parameter description:

Port Power Saving Configuration

1. Optimize EEE for

The switch can be set to optimize EEE for either best power saving or least traffic latency.

Port Configuration

1. Port

The switch port number of the logical port.

2. ActiPHY

Link down power savings enabled.

ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted.

3. PerfectReach

Cable length power savings enabled.

PerfectReach works by determining the cable length and lowering the power for ports

with short cables.

4. EEE

Controls whether **EEE** is enabled for this switch port.

For maximizing power savings, the circuit isn't started at once transmit data is ready

for a port, but is instead queued until a burst of data is ready to be transmitted.

This

will give some traffic latency.

If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent

queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

5. EEE Urgent Queues

Queues set will activate transmission of frames as soon as data is available.

Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

Buttons

Save – Click to save changes.

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

4.3 Port

4.3.1.Port Configuration

The section describes to configure the Port detail parameters of the switch. Others you could using the Port configure to enable or disable the Port of the switch. Monitor the ports content or status in the function.

Web Interface

To configure Port Configuration in the web interface:

1. Click configuration, Port and Port Configuration
2. Specify the Speed Configured, Flow Control, Maximum Frame size, Excessive Collision mode and Power Control
3. Click Save.

Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>			<input type="checkbox"/>	9600	<>
1	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
2	100fdx		Auto	X	X	<input type="checkbox"/>	9600	Discard
3	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
4	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
5	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
6	Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
7	Down		Auto	X	X	<input type="checkbox"/>	9600	
8	Down		Auto	X	X	<input type="checkbox"/>	9600	
9	Down		Auto	X	X	<input type="checkbox"/>	9600	
10	Down		Auto	X	X	<input type="checkbox"/>	9600	

Parameter description:

1. Port :

This is the logical port number for this row.

2. Link :

The current link state is displayed graphically. Green indicates the link is up and red that it is down.

3. Current Link Speed :

Provides the current link speed of the port.

4. Configuration 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 .

5. 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.

6. **Maximum Frame Size :**

Enter the maximum frame size allowed for the switch port, including FCS.

7. **Excessive Collision :**

Configure port transmit collision behavior.

Discard: Discard frame after 16 collisions (default).

Restart: Restart backoff algorithm after 16 collisions.

Buttons

Apply : 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.

4.4 DHCP

The section describes to configure the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

4.4.1.DHCP Server

A Dynamic Host Configuration Protocol (DHCP) server can provide valuable TCP/IP network services. DHCP can dynamically allocate IP parameters, such as an IP address.

4.4.1.1. DHCP Server Mode

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

Web Interface

To configure DHCP Server in the web interface:

1. Click Configuration DHCP, DHCP Server.
2. Specify DHCP Global Mode
3. Add VLAN Range
4. Specify DHCP Mode
5. Click Save.

DHCP Server Mode Configuration

Global Mode

Mode	Disabled ▼
-------------	------------

VLAN Mode

Delete	VLAN Range	Mode
Delete	<input style="width: 50px;" type="text"/> - <input style="width: 50px;" type="text"/>	Enabled ▼

Add VLAN Range

Save

Reset

Parameter description:

Global VLAN

1. Mode :

Configure the operation mode per system. Possible modes are:

Enabled: Enable DHCP server per system.

Disabled: Disable DHCP server pre system.

VLAN Mode

1. 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 32 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.

2. 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.

Save – Click to save changes.

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

4.4.1.2. DHCP Server Excluded IP

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

Web Interface

To configure DHCP Server in the web interface:

1. Click Configuration DHCP, DHCP Server and Excluded IP.
2. Add VLAN Range
3. Click Save.

DHCP Server Excluded IP Configuration

Excluded IP Address

Delete	IP Range	
Delete	<input type="text"/>	- <input type="text"/>

Parameter description:

1. 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 VLAN Range - Click to add a new VLAN range.

Save – Click to save changes.

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

4.4.1.3. 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.

Web Interface

To configure DHCP Server in the web interface:

1. Click Configuration DHCP, DHCP Server and Pool
2. Add New Pool
3. Add Name
4. Click Save.

DHCP Server Pool Configuration

Pool Setting

Delete	Name	Type	IP	Subnet Mask	Lease Time
Delete	<input type="text"/>	-	-	-	1 days 0 hours 0 minutes

Add New Pool

Save

Reset

Parameter description:

1. 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.

2. 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

3. IP :

Display network number of the DHCP address pool.

If "-" is displayed, it means not defined.

4. Subnet Mask :

Display subnet mask of the DHCP address pool.

If "-" is displayed, it means not defined.

5. Lease Time

Display lease time of the pool.

Buttons

Delete - Click to delete the setting.

Add New Pool - Click to add a new VLAN range.

Save – Click to save changes.

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

4.4.2.DHCP Snooping

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

The section describes to configure the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

Web Interface

To configure DHCP snooping in the web interface:

1. Click Configuration, DHCP, Snooping
2. Select "Enabled" in the Mode of DHCP Snooping Configuration.

3. Select "Trusted" of the specific port in the Mode of Port Mode Configuration.
4. Click Save.

DHCP Snooping Configuration

Snooping Mode | Disabled ▾

Port Mode Configuration

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

Save | Reset

Parameter description:

1. 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.

2. 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

Save – Click to save changes.

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

4.4.3.DHCP Relay

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID(Port VLAN ID) correctly

Web Interface

To monitor an DHCP Relay statistics in the web interface:

1. Click Configuration, DHCP, DHCP Relay

DHCP Relay Configuration

Relay Mode	Disabled	▼
Relay Server	0.0.0.0	
Relay Information Mode	Disabled	▼
Relay Information Policy	Keep	▼

Save Reset

Parameter description:

1. Relay Mode:

Indicates the DHCP relay mode operation.
Possible modes are:

Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

Disabled: Disable DHCP relay mode operation.

2. Relay Server :

Indicates the DHCP relay server IP address.

3. Relay Information Mode :

Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

Possible modes are:

Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

Disabled: Disable DHCP relay information mode operation.

4. Relay Information Policy :

Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:

Replace: Replace the original relay information when a DHCP message that already contains it is received.

Keep: Keep the original relay information when a DHCP message that already contains it is received.

Drop: Drop the package when a DHCP message that already contains relay information is received.

Buttons

Save – Click to save changes.

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

4.5 Security

This section shows you to to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

4.5.1.Switch

4.5.1.1. User

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.

Web Interface

To monitor an Security User in the web interface:

1. Click Configuration, Security and User
2. Add New User
3. Add User Name
4. Add Password
5. Select Privilege level

Users Configuration

User Name	Privilege Level
admin	15

Add New User

Add User

User Settings	
User Name	<input type="text"/>
Password	<input type="password"/>
Password (again)	<input type="password"/>
Privilege Level	1 ▼

Parameter description:

1. 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.

2. Password :

The section will teach user to set the QoS Port DSCP configuration that was allowed you to configure the basic QoS Port DSCP Configuration settings for all switch ports. Others the settings relate to the currently selected stack unit, as reflected by the page header.

3. 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.

Save – 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)

4.5.1.2. Privilege Level

This page provides an overview of the privilege levels.

Web Interface

To monitor an Security Privilege level in the web interface:

1. Click Configuration, Security and Privilege level
2. Select Privilege level
3. Click Save

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5 ▾	10 ▾	5 ▾	10 ▾
Debug	15 ▾	15 ▾	15 ▾	15 ▾
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 ▾
POE	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 ▾

Parameter description:

1. 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.

2. Privilege Level :

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

Save – Click to save changes.

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

4.5.1.3. Auth Method

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

Web Interface

To monitor an Security Auth Method in the web interface:

1. Click Configuration, Security and Auth Method
2. Select Methods
3. Click Save

Authentication Method Configuration

Client	Methods		
console	local ▼	no ▼	no ▼
telnet	local ▼	no ▼	no ▼
ssh	local ▼	no ▼	no ▼
http	local ▼	no ▼	no ▼

Parameter description:

1. Client :

The management client for which the configuration below applies.

2. 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.

3. Buttons

Save – Click to save changes.

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

4.5.1.4. SSH

Configure SSH on this page.

Web Interface

To monitor an Security SSH in the web interface:

1. Click Configuration, Security and SSH

2. Enable SSH Configuration
3. Click Save

SSH Configuration

Mode	Enabled ▼
------	-----------

Save	Reset
------	-------

Parameter description:

1. Mode :

Indicates the SSH mode operation. Possible modes are:

Enabled: Enable SSH mode operation.

Disabled: Disable SSH mode operation.

Buttons

Save – Click to save changes.

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

4.5.1.5. HTTPS

Configure HTTPS on this page.

Web Interface

To configuration an Security HTTPS in the web interface:

1. Click Configuration, Security and HTTPS
2. Enable HTTPS Mode
3. Enable Automatic Redirect
4. Click Save

HTTPS Configuration

Mode	Disabled ▼
Automatic Redirect	Disabled ▼

Save	Reset
------	-------

Parameter description:

1. Mode :

Indicates the SSH mode operation. Possible modes are:
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.

2. 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

Save – Click to save changes.

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

4.5.1.6. 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.

Access Management Configuration

Mode

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
--------	---------	------------------	----------------	------------	------	------------

Add New Entry

Save Reset



Access Management Configuration

Mode Disabled ▾

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	1	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add New Entry

Save Reset

Parameter description:
1. Mode :

Indicates the access management mode operation. Possible modes are:

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation.

2. Delete :

Check to delete the entry. It will be deleted during the next save

3. VLAN ID :

Indicates the VLAN ID for the access management entry.

4. Start IP address :

Indicates the start IP address for the access management entry.

5. End IP address :

Indicates the end IP address for the access management entry.

6. 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.

7. 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.

8. 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 :

Save – Click to save changes.

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

4.5.1.7. SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP “Enable”, SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set “Disable”, SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

4.5.1.7.1. System

This section describes how to configure SNMP System on the switch. This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click <Apply> button, the setting takes effect.

Web Interface

To configuration SNMP System in the web interface:

1. Click Configuration, SNMP and System
2. Evoke SNMP State to enable or disable the SNMP function
3. Specify the Engine ID
4. Click Save

SNMP System Configuration

Mode	Enabled <input type="button" value="v"/>
Version	SNMP v2c <input type="button" value="v"/>
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Parameter description:

1. Mode :

Indicates the SNMP mode operation. Possible modes are:

Enabled: Enable SNMP mode operation.

Disabled: Disable SNMP mode operation.

2. Version :

Indicates the SNMP supported version. Possible versions are:

SNMP v1: Set SNMP supported version 1.

SNMP v2c: Set SNMP supported version 2c.

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.

4. 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.

5. 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 :

Save – Click to save changes.

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

4.5.1.7.2. Trap

Configure SNMP trap on this page.

Web Interface

To display the configuration SNMP Trap in the web interface:

1. Click Configuration, SNMP and Trap
2. Click Add New Entry then you can create new SNMP Trap on the switch
3. Click Save

Trap Configuration

Global Settings

Mode ▾

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
--------	------	--------	---------	---------------------	------------------

Add New Entry

Save Reset

Trap Config Name	<input type="text"/>
Trap Mode	Disabled ▾
Trap Version	SNMP v2c ▾
Trap Community	Public
Trap Destination Address	<input type="text"/>
Trap Destination Port	162
Trap Inform Mode	Disabled ▾
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled ▾
Trap Security Engine ID	<input type="text"/>
Trap Security Name	None ▾

SNMP Trap Event

System	<input type="checkbox"/> * <input type="checkbox"/> Warm Start <input type="checkbox"/> Cold Start
Interface	<input type="checkbox"/> * Link up <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches <input type="checkbox"/> * Link down <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches LLDP <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches
AAA	<input type="checkbox"/> * <input type="checkbox"/> Authentication Fail
Switch	<input type="checkbox"/> * <input type="checkbox"/> STP <input type="checkbox"/> RMON

Parameter description:

Global Setting

1. Mode :

Indicates the trap mode operation. Possible modes are:

Enabled: Enable SNMP trap mode operation.

Disabled: Disable SNMP trap mode operation.

Trap Destination Configurations

1. Name:

Indicates the trap Configuration's name. Indicates the trap destination's name.

2. Enable :

Indicates the trap destination mode operation. Possible modes are:

Enabled: Enable SNMP trap mode operation.

Disabled: Disable SNMP trap mode operation.

3. 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.

4. 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'.

5. Destination port :

Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

6. Trap Mode :

Indicates the SNMP trap mode operation. Possible modes are:

Enabled: Enable SNMP trap mode operation.

Disabled: Disable SNMP trap mode operation.

7. Trap 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.

8. 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.

9. 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

10. Trap Destination IPv6 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'.

11. 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.

12. 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.

13. 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.

14. Trap Inform Timeout(seconds) :

Indicates the SNMP trap inform timeout. The allowed range is **0** to **2147**.

15. Trap Inform Retry Time :

Indicates the SNMP trap inform retry times. The allowed range is **0** to **255**.

16. 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.

17. Trap 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.

18. 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.

Button :

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.

4.5.1.7.3. Communities

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

Web Interface

To display the configuration SNMP Communities in the web interface:

1. Click SNMP, Communities
2. Click Add new community
3. Specify the SNMP communities parameters
4. Click Save
5. If you want to modify or clear the setting then click Reset

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Parameter description:

1. **Delete :**

Check to delete the entry. It will be deleted during the next save.

2. 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.

3. 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.

4. Source Mask :

Indicates the SNMP access source address mask.

Button :

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.

4.5.1.7.4. User

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

Web Interface

To display the configuration SNMP Users in the web interface:

1. Click SNMP, Users
2. Specify the Privilege parameters
3. Click Save

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
--------	-----------	-----------	----------------	-------------------------	-------------------------	------------------	------------------

Parameter description:

1. Delete :

Check to delete the entry. It will be deleted during the next save.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

Button :

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.

4.5.1.7.5. Group

The function is used to configure SNMPv3 group. The Entry index key are Security Model and Security Name. To create a new group account, please check <Add new group> button, and enter the group information then check <Save>. Max Group Number: v1: 2, v2: 2, v3:10.

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

Web Interface

To display the configuration SNMP Group in the web interface:

1. Click SNMP, Group
2. Specify the Privilege parameters
3. Click Save

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group

Parameter description:

1. Delete :

Check to delete the entry. It will be deleted during the next save.

2. 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).

3. 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.

4. 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.

Button :

Add New Entry - Click to add a new group entry.

Save – Click to save changes.

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

4.5.1.7.6. Views

The function is used to configure SNMPv3 view. The Entry index keys are OID Subtree and View Name. To create a new view account, please check <Add new view> button, and enter the view information then check <Save>. Max Group Number: 28.

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

Web Interface

To display the configuration SNMP Views in the web interface:

1. Click SNMP, Views
2. Click Add new View
3. Specify the SNMP View parameters
4. Click Save
5. If you want to modify or clear the setting then click Reset

SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included ▼	.1

Parameter description:

1. Delete :

Check to delete the entry. It will be deleted during the next save.

2. 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.

3. 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 its OID subtree should overstep the 'excluded' view entry.

4. 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(*).

Button :

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.

4.5.1.7.7. Access

The function is used to configure SNMPv3 accesses. The Entry index key are Group Name, Security Model and Security level. To create a new access account, please check <Add new access> button, and enter the access information then check <Save>. Max Group Number : 14

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

Web Interface

To display the configuration SNMP Access in the web interface:

1. Click SNMP, Access
2. Click Add new Access
3. Specify the SNMP Access parameters
4. Click Save
5. If you want to modify or clear the setting then click Reset

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view ▾	None ▾
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view ▾	default_view ▾

Parameter description:

1. Delete :

Check to delete the entry. It will be deleted during the next save.

2. 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.

3. 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).

4. 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.

5. 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.

6. 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.

Button :

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

4.5.1.8.RMON

An RMON implementation typically operates in a client/server model. Monitoring devices contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients.

4.5.1.8.1. Statistics

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

Web Interface

To display the configuration RMON in the web interface:

1. Click RMON, Statistics
2. Click Add New Entry
3. Specify the ID parameters
4. Click Save

RMON Statistics Configuration

Delete	ID	Data Source
<input type="checkbox"/>		
<input type="checkbox"/>		

Parameter description:

1. Delete :

Check to delete the entry. It will be deleted during the next save.

2. ID :

Indicates the index of the entry. The range is from 1 to 65535.

3. 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

Button :

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

4.5.1.8.2. History

This section 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. The "Start from History Index and Sample Index" allows the user to select the starting point in the History table.

The "Start from History Index and Sample Index" allows the user to select the starting point in the History table. Clicking the button will update the displayed table starting from that or the next closest History table match.

The will use the last entry of the currently displayed entry as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

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

Web Interface

To display the configuration RMON History in the web interface:

1. Click RMON, History
2. Click Security, Switch, RMON ,then History
3. Checked "Auto-refresh"
4. Click " Refresh" to refresh the port detailed statistics or clear all information when you click " Clear".

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
--------	----	-------------	----------	---------	-----------------

Parameter description:

1. Delete :

Check to delete the entry. It will be deleted during the next save

2. ID :

Indicates the index of the entry. The range is from 1 to 65535.

3. 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.

4. Interval :

Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.

5. 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.

6. Buckets Granted :

The number of data shall be saved in the RMON.

Button :

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

4.5.1.8.3. 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. The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the button will update the displayed table starting from that or the next closest Alarm table match.

The will use the last entry of the currently displayed entry as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

Web Interface

To display the configuration RMON Alarm in the web interface:

1. Specify Port which wants to check
2. Click Security, Switch, RMON ,then Alarm
3. Checked "Auto-refresh"
4. Click " Refresh" to refresh the port detailed statistics

RMON Alarm Configuration

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

Parameter description:

1. Delete :

Indicates the index of Alarm control entry.

2. ID :

Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

3. Interval :

Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to $2^{31}-1$.

4. 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).

5. 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).

6. Value :

The value of the statistic during the last sampling period.

7. Starup Alarm :

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

Rising Trigger alarm when the first value is larger than the rising threshold.

Falling Trigger alarm when the first value is less than the falling threshold.

RisingOrFalling Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

8. Rising Threshold :

Rising threshold value (-2147483648-2147483647).

9. Rising Index :

Rising event index (1-65535).

10. Falling Threshold :

Falling threshold value (-2147483648-2147483647)

11. Falling Index :

Falling event index (1-65535).

Button :

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

4.5.1.8.4. 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 .

The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the button will update the displayed table starting from that or the next closest Event table match.

The will use the last entry of the currently displayed entry as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

Web Interface

To display the configuration RMON Alarm in the web interface:

1. Click Security, Switch, RMON ,then Event
2. Checked "Auto-refresh"
3. Click " Refresh" to refresh the port detailed statistics
4. Specify Port which wants to check

RMON Event Configuration

Delete	ID	Desc	Type	Community	Event Last Time
<input type="button" value="Add New Entry"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>					

Parameter description:

1. Delete :

Indicates the index of Alarm control entry.

2. ID :

Indicates the index of the entry. The range is from 1 to 65535.

3. Desc :

Indicates this event, the string length is from 0 to 127, default is a null string.

4. 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.

5. Community :

Specify the community when trap is sent, the string length is from 0 to 127, default is "public".

6. Event Last Time :

Indicates the value of sysUpTime at the time this event entry last generated an event.

Button :

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

4.5.2. Network

4.5.2.1. Limit Control

This page allows you to configure the Port Security Limit Control system and port settings. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC

address and VLAN ID. If Limit Control is enabled on a port, the **limit** specifies the maximum number of

users on the port. If this number is exceeded, an **action** is taken. The action can be one of the four

different actions as described below.

The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC

addresses learnt on the port.

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

Web Interface

To configure a Configuration of Limit Control in the web interface:

1. Select "Enabled" in the Mode of System Configuration.
2. Checked Aging Enabled
3. Set Aging Period(Default is 3600 seconds)

To configure a Port Configuration of Limit Control in the web interface:

1. Select "Enabled" in the Mode of Port Configuration
2. Specify the maximum number of MAC addresses in the Limit of Port Configuration.
3. Set Action (None, Trap, Shutdown, Trap & Shutdown)
4. Click Apply

Port Security Limit Control Configuration

System Configuration

Mode	Disabled ▾
Aging Enabled	<input type="checkbox"/>
Aging Period	3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<> ▾	4	<> ▾		
1	Disabled ▾	4	None ▾	Disabled	Reopen
2	Disabled ▾	4	None ▾	Disabled	Reopen
3	Disabled ▾	4	None ▾	Disabled	Reopen
4	Disabled ▾	4	None ▾	Disabled	Reopen
5	Disabled ▾	4	None ▾	Disabled	Reopen
6	Disabled ▾	4	None ▾	Disabled	Reopen
7	Disabled ▾	4	None ▾	Disabled	Reopen
8	Disabled ▾	4	None ▾	Disabled	Reopen

Parameter description:

System Configuration

1. Mode :

Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

2. Aging Enabled :

If checked, secured MAC addresses are subject to aging as discussed under [Aging Period](#) .

3. Aging Period :

If [Aging Enabled](#) is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The Aging Period can be set to a number between 10 and 10,000,000 seconds. To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is

connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

1. Port :

The port number to which the configuration below applies.

2. Mode :

Controls whether Limit Control is enabled on this port. Both this and the [Global Mode](#) must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

3. Limit :

The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding [action](#) is taken.

The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

4. Action :

If [Limit](#) is reached, the switch can take one of the following actions:

None: Do not allow more than [Limit](#) MAC addresses on the port, but take no further action.

Trap: If [Limit](#) + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.

Shutdown: If [Limit](#) + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

1. Boot the switch,
2. Disable and re-enable Limit Control on the port or the switch,
3. Click the [Reopen](#) button.

Trap & Shutdown: If [Limit](#) + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

5. State :

This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:

Disabled: Limit Control is either globally disabled or disabled on the port.

Ready: The limit is not yet reached. This can be shown for all [actions](#).

Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if [Action](#) is set to **None** or **Trap**.

Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if [Action](#) is set to **Shutdown** or **Trap & Shutdown**.

6. Re-open Button :

If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to **Shutdown** in the [Action](#) section.

Note that clicking the reopen button causes the page to be refreshed, so noncommitted changes will be lost.

Button :

Refresh - Click to refresh the page. Note that non-committed changes will be lost

Save – Click to save changes.

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

4.5.2.2.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.

This section provides an overview of f QoS Ingress Port Policers for all switch ports The Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic

Web Interface

To configure a Configuration of Limit Control in the web interface:

1. Select “Enabled” in the Mode of Network Access Server Configuration.
2. Checked Reauthentication Enabled.
3. Set Reauthentication Period (Default is 3600 seconds).
4. Set EAPOL Timeout (Default is 30 seconds).
5. Set Aging Period (Default is 300 seconds).
6. Set Hold Time (Default is 10 seconds).
7. Checked RADIUS-Assigned QoS Enabled.
8. Checked RADIUS-Assigned VLAN Enabled.
9. Checked Guest VLAN Enabled.
10. Specify Guest VLAN ID.
11. Specify Max. Reauth. Count.
12. Checked Allow Guest VLAN if EAPOL Seen.
13. .Click Apply.

Network Access Server Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	<input type="checkbox"/>
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>
Guest VLAN Enabled	<input type="checkbox"/>
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
*	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize

Save Reset

Parameter description:

System Configuration

1. Mode:

Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

2. 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).

3. 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.

4. 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.

5. AgingPeriod :

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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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].

11. 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].

12. Allow Guest VLAN if EAPOL Seen

To set the Rate limit value for this port, the default is 500.

Port Configuration

1. Port :

The port number for which the configuration below applies.

2. 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.

3. 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

RADIUS attributes used in identifying a QoS Class:

The User-Priority-Table attribute defined in [RFC4675](#) forms the basis for identifying the QoS Class in an Access-Accept packet.

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

All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

4. 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 RADIUSassigned).

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].

5. 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.

6. 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.

7. 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.

Button :

Refresh - Click to refresh the page. Note that non-committed changes will be lost

Save – Click to save changes.

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

4.5.2.3. ACL

It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into Ether Types. IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number is 1-8, however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

4.5.2.3.1. Port

The section describes how to configure the ACL parameters (ACE) of the each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE

Web Interface

To configure the ACL Ports Configuration in the web interface:

1. Click Configuration, ACL, then Ports
2. To scroll the specific parameter value to select the correct value for port ACL setting.
3. Click the save to save the setting.
4. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.
5. After you configure complete then you could see the Counter of the port. Then you could click refresh to update the counter or Clear the information.

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	280014
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	0
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
9	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Parameter description:
1. Port :

The logical port for the settings contained in the same row.

2. Policy ID :

Select the policy to apply to this port. The allowed values are **0** through **255**. The default value is 0.

3. Action :

Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

4. 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".

5. 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".

6. 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".

7. Logging :

Controls the rate for the port shaper. The default value is ?. This value is restricted to ?-1000000 when the "Unit" is "kbps", and it is restricted to 1-? when the "Unit" is "Mbps".

8. 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).

9. 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".

10. Counter :

Counts the number of frames that match this ACE.

Buttons:

Save – 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.

4.5.2.3.2. Rate Limiters

The section describes how to configure the switch's ACL Rate Limiter parameters. The Rate Limiter Level from 1 to 16 that allow user to set rate limiter value and units with pps or kbps.

Web Interface

To configure ACL Rate Limiter in the web interface:

1. Click Configuration, ACL, then Rate Limiter.
2. To specific the Rate field and the range from 0 to 3276700.
3. To scroll the Unit with pps or kbps.
4. Click the Apply to save the setting.

5. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

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 ▼

Parameter description:

1. Rate Limiter ID :

The rate limiter ID for the settings contained in the same row.

2. Rate :

The rate range is located **0-3276700** in pps.
Or **0, 100, 200, 300, ..., 1000000** in kbps.

3. 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.

4.5.2.3.3. Access Control List

The section describes how to configure Access Control List rule. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port. 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 the priority is highest

Web Interface

To configure Access Control List in the web interface:

1. Click Configuration, ACL, then Access Control List.
2. Click the  button to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list.)
3. To specific the parameter of the ACE.
4. Click the save to save the setting.
5. If you want to cancel the setting then you need to click the reset button.It will revert to previously saved values.
6. When editing an entry on the ACE Configuration page, note that the Items displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched (such as Rate Limiter, Port Copy, Logging, and Shutdown).

Access Control List Configuration Auto-refresh Refresh Clear Remove All

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

ACE Configuration

Ingress Port	All
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

Parameter description:**1. 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.

2. Policy/Bitmask :

Indicates the policy number and bitmask of the ACE.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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".

8. Counter :

The counter indicates the number of times the ACE was hit by a frame.

9. 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

Refresh – Click to refresh the page; any changes made locally will be undone.

Clear – Click to clear the counters.

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

Parameter description:

1. 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.

2. 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.

3. Policy Value :

When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is **0** to **255**.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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".

10. 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.

11. 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).

12. Counter :

The counter indicates the number of times the ACE was hit by a frame.

MAC Parameters

1. 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.

2. 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.

3. DMAC Filter :

Select the ingress port for which this ACE applies.

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.

4. DMAC Value :

Select the ingress port for which this ACE applies.

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

1. 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".

2. 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.

3. 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.

4. 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'tcare".)

VLAN Parameters

1. 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.

2. 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.

3. 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.

4. 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](#).

5. Sender IP Mask :

When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in [dotted decimal notation](#).

6. 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.

7. 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](#).

8. Target IP Mask :

When "Network" is selected for the target IP filter, you can enter a specific target IP mask in [dotted decimal notation](#).

9. ARP Sender MAC Match :

Specify the target IP filter for this specific ACE.

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").

10. 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").

11. IP :

Specify whether frames can hit the action according to their target hardware

12. Ethernet :

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").

IP Parameters

1. 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.

2. 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.

3. 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").

4. 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").

5. 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").

6. 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.

7. SIP Address :

When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in [dotted decimal notation](#).

8. SIP Mask :

When "Network" is selected for the source IP filter, you can enter a specific SIP mask in [dotted decimal notation](#).

9. 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.

10. DIP Address :

When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in [dotted decimal notation](#).

11. DIP Mask :

When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in [dotted decimal notation](#).

IPv6 Parameters

1. 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.

2. 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.

3. 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.

4. 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.

5. 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 0xFFFFFFF0 (bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

6. 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

1. 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.

2. 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.

3. 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.

4. 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

1. 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'tcare").

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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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").

8. 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").

9. 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").

10. 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").

11. 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").

12. 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

1. Ethernet Type 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.

2. Ethernet Type Value :

Specify the TCP/UDP source filter for this ACE.
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:

Save – Click to save changes.

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

Cancel – Return to the previous page

4.5.2.4. IP Source Guard

4.5.2.4.1. Configuration

The section describes to configure the IP Source Guard detail parameters of the switch. You could use the IP Source Guard configure to enable or disable with the Port of the switch.

Web Interface

To configure an IP Source Guard Configuration in the web interface:

1. Select "Enabled" in the Mode of IP Source Guard Configuration.
2. Select "Enabled" of the specific port in the Mode of Port Mode Configuration.
3. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port in the Mode of Port Mode Configuration.
4. Click Apply.

IP Source Guard Configuration

Mode

Port Mode Configuration

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

Parameter description:

1. Mode of IP Source Guard Configuration :

Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

2. Port Mode Configuration :

Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port..

3. Max Dynamic Clients :

Controls the unit of measure for the storm control rate as kbps, Mbps, fps or kfps . The default value is "kbps".

4. Buttons:

Save – Click to save changes.

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

Translate dynamic to static – Click to translate all dynamic entries to static entries

4.5.2.4.2. Static Table

The section describes to configure the IP Source Guard Static Table parameters of the switch. You could use the Static IP Source Guard Table configure to manage the entries.

Web Interface

To configure an IP Source Guard Statics Table in the web interface:

1. Click "Add new entry".
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click Apply.

Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
<input type="button" value="Add New Entry"/>				
<input type="button" value="Save"/>		<input type="button" value="Reset"/>		

Parameter description:

1. Delete :

Check to delete the entry. It will be deleted during the next save.

2. Port :

The logical port for the settings.

3. VLAN ID :

The vlan id for the settings.

4. IP Address :

Allowed Source IP address.

5. MAC Address :

Allowed Source MAC address.

Buttons:

Add New Entry – Click to add a new entry to the Static IP Source Guard table.

Save – Click to save changes.

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

4.5.2.5. ARP Inspection

The section describes to configure the ARP Inspection parameters of the switch. You could use the ARP Inspection configure to manage the ARP table.

4.5.2.5.1. Port Configuration

This section describes how to configure ARP Inspection setting including :
Mode (Enabled and Disabled)

Port (Enabled and Disabled)

Web Interface

To display the QoS Port Schedulers in the web interface:

1. Select "Enabled" in the Mode of ARP Inspection Configuration.
2. Select "Enabled" of the specific port in the Mode of Port Mode Configuration
3. Click Apply.

ARP Inspection Configuration

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None
7	Disabled	Disabled	None
8	Disabled	Disabled	None

Parameter description:

1. Mode of ARP Inspection Configuration :

Enable the Global ARP Inspection or disable the Global ARP Inspection.

2. Port Mode Configuration :

Shows the scheduling mode for this port.

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

Possible modes are:

Enabled: Enable ARP Inspection operation.

Disabled: Disable ARP Inspection operation.

If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting.

And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:

Enabled: Enable check VLAN operation.

Disabled: Disable check VLAN operation.

Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting.

There are four log types and possible types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons :

Save – Click to save changes.

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

Translate dynamic to static – Click to translate all dynamic entries to static entries

4.5.2.5.2. VLAN Configuration

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

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

Clicking the button will update the displayed table starting from that or the closest next VLAN Table match. The will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the button to start over.

Web Interface

To configuration a VLAN Mode Configuration in the web interface:

1. Click "Add new entry".
2. Specify the VLAN ID, Log Type.
3. Click Apply.

VLAN Mode Configuration

Start from VLAN with entries per page.

Delete	VLAN ID	Log Type
--------	---------	----------

Add New Entry

Save Reset

Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1 ▾			

Add New Entry

Save Reset

Parameter description:

1. VLAN Mode Configuration :

Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.

Possible types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries

Buttons :

Save – Click to save changes.

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

Add New Entry – Click to add a new VLAN to the ARP Inspection VLAN table.

4.5.2.5.3. Static Table

The section describes to configure the Static ARP Inspection Table parameters of the switch. You could use the Static ARP Inspection Table configure to manage the ARP entries.

Web Interface

To configuration a VLAN Mode Configuration in the web interface:

1. Click “Add new entry”.
2. Specify the VLAN ID, Log Type.
3. Click Apply.

Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
<input type="button" value="Add New Entry"/>				
<input type="button" value="Save"/>		<input type="button" value="Reset"/>		

Parameter description:

1. **Delete :**
Check to delete the entry. It will be deleted during the next save.
2. **Port :**
Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode
3. **VLAN ID :**
The vlan id for the settings.
4. **MAC Address :**
Allowed Source MAC address in ARP request packets.
5. **IP Address :**
Allowed Source IP address in ARP request packets.

Buttons :

Add New Entry – Click to add a new entry to the Static ARP Inspection table.

Save – Click to save changes.

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

4.5.2.5.4. Dynamic Table

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

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a 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.

Web Interface

To configuration a Dynamic ARP Inspection Table Configuration in the web interface:

1. Click Security, Network, ARP Inspection.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statics..
4. Specify the Start from port, VLAN ID, MAC Address, IP Address, and entries per page..

Dynamic ARP Inspection Table

 Auto-refresh Refresh |<< >>

Start from Port 1, VLAN 1, MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address	Translate to static
No more entries				

Save Reset

Parameter description:
Navigating the ARP Inspection Table :

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table. The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a 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.

1. **Port :**
Switch Port Number for which the entries are displayed.
2. **VLAN ID :**
VLAN-ID in which the ARP traffic is permitted.
3. **MAC Address :**
User MAC address of the entry.
4. **IP Address :**
User IP address of the entry.
5. **Translate to static :**
Select the checkbox to translate the entry to static 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.

Save – Click to save changes.

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

|<< – Updates the system log entries to the first available entry ID.

>> – Updates the system log entry to the next available entry ID.

4.5.3.AAA

4.5.3.1.RADIUS

This section shows you to use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

Web Interface

To configure a Common Configuration of AAA, RADIUS in the web interface:

RADIUS Server Configuration

Global Configuration

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

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
--------	----------	-----------	-----------	---------	------------	-----

Add New Server

Save Reset

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Delete		1812	1813			

Add New Server

Save Reset

Parameter description:

Global Configuration

1. 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.

2. (QoS class, DP level) to (PCP, DEI) Mapping :

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.

3. 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.

4. Key :

The secret key - up to 63 characters long - shared between the RADIUS server and the switch.

5. NAS-IP-Address(Attribute4) :

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.

6. NAS-IPv6-Address(Attribute95) :

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.

7. 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.

Global Configuration**1. Delete :**

To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

2. Hoshname :

The IP address or hostname of the RADIUS server.

3. Auth Port :

The **UDP** port to use on the RADIUS server for authentication.

4. Acct Port :

The **UDP** port to use on the RADIUS server for accounting.

5. Retransmit :

This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

6. 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.

4.5.3.2. TACACS+

This page allows you to configure the [TACACS+](#) servers.

Web Interface

To configure a Common Configuration of AAA, TACACS+ in the web interface:

TACACS+ Server Configuration

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key	<input type="text"/>	

Server Configuration

Delete	Hostname	Port	Timeout	Key
--------	----------	------	---------	-----

Parameter description:

Global Configuration

1. 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.

2. 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.

3. Key :

The secret key - up to 63 characters long - shared between the RADIUS server and the switch.

Server Configuration

1. Delete :

To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.

2. Hostname :

The IP address or hostname of the TACACS+ server.

3. Port :

The **TCP** port to use on the TACACS+ server for authentication.

4. Timeout :

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

5. 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.

4.6 Aggregation

The Aggregation is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment's to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

4.6.1. Static Aggregation

Ports using Static Trunk as their trunk method can choose their unique Static GroupID to form a logic "trunked port". The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a "logic trunked port". Using Static Trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in "not ready" state when using static trunk to aggregate with high speed links.

Web Interface

To configure the Trunk Aggregation Hash mode and Aggregation Group in the web interface:

1. Click Configuration, Aggregation, Static and then Aggregation Mode Configuration.
2. Evoke to enable or disable the aggregation mode function. Evoke Aggregation Group ID and Port members
3. Click the save to save the setting.
4. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

Aggregation Group Configuration

Group ID	Port Members							
	1	2	3	4	5	6	7	8
Normal	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Parameter description:

Hash Code Contributors

1. 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.

2. 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.

3. 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.

4. 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

1. 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.

2. Port Member :

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.

4.6.2.LACP Aggregation

This page allows the user to inspect the current LACP port configurations, and possibly change them as well. An LACP trunk group with more than one ready member-ports is a "real trunked" group. An LACP trunk group with only one or less than one ready member-ports is not a "real trunked" group.

Web Interface

To configure the Trunk Aggregation LACP parameters in the web interface:

1. Click Configuration, LACP, Configuration.
2. Evoke to enable or disable the LACP on the port of the switch.
Scroll the Key parameter with Auto or Specific Default is Auto.
3. Scroll the Role with Active or Passive. Default is Active.
4. Click the save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

LACP Port Configuration

Port	LACP Enabled	Key	Role	Timeout	Prio
*	<input type="checkbox"/>	<> ▼	<> ▼	<> ▼	32768
1	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
2	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
3	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
4	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
5	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
6	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
7	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
8	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768

Parameter description:

1. Port :

The switch port number.

2. 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.

3. 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.

4. 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).

5. 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.

6. 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

Save – Click to save changes.

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

4.7 Loop Protection

The loop Protection is used to detect the presence of traffic. When switch receives packet's (looping detection frame) MAC address the same as oneself from port, show Loop Protection happens. The port will be locked when it received the looping Protection frames. If you want to resume the locked port, please find out the looping path and take off the looping path, then select the resume the locked port and click on "Resume" to turn on the locked ports.

Web Interface

To display the Loop Protection status in the web interface:

1. Click Monitor, Loop Protection

Loop Protection Configuration

General Settings

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

Port Configuration

Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<> ▾	<> ▾
1	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
2	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
3	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
4	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
5	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
6	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
7	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
8	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾

Save Reset

Parameter description:

General Setting

1. **Enable Loop Protection :**

Controls whether loop protections is enabled (as a whole).

2. **Transmission Time :**

The interval between each loop protection PDU sent on each port, valid values are 1 to 10 seconds.

3. 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

1. Port :

The switch port number of the port.

2. Enable :

Controls whether loop protection is enabled on this switch port.

3. 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**.

4. 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.

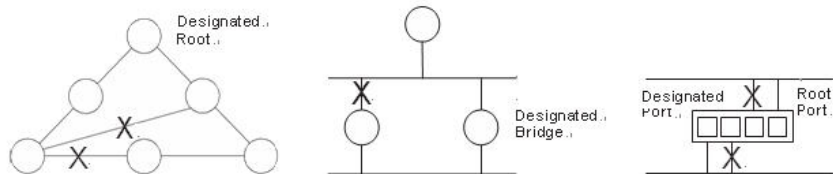
Reset- Click to undo any changes made locally and revert to previously saved values.

4.8 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP - STP uses a distributed algorithm to select a bridging device (STP- compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables

all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDUs after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

4.8.1. Bridge Settings

The section describes that how to configure the Spanning Tree Bridge and STP System settings. It allows you to configure STP System settings are used by all STP Bridge instance in the switch.

Web Interface

To display the Loop Protection status in the web interface:

1. Click Configuration, Spanning Tree, Bridge Settings.
2. Scroll to select the parameters and write down available value of parameters in blank field in Basic Settings.
3. Evoke to enable or disable the parameters and write down available value of parameters in blank field in Advanced settings.
4. Click the apply to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

STP Bridge Configuration

Basic Settings	
Protocol Version	MSTP ▼
Bridge Priority	32768 ▼
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings	
Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	<input type="text"/>

Parameter description:

Basic Setting

1. Enable Loop Protection :

The **MSTP** / **RSTP** / **STP** protocol version setting. Valid values are **STP**, **RSTP** and **MSTP**.

2. 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

3. 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.

4. 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.

5. 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.

6. 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 Setting

1. Edge Port BPDU Filtering :

Control whether a port *explicitly* configured as **Edge** will transmit and receive BPDUs.

2. 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.

3. 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.

4. 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

Save – Click to save changes.

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

4.8.2.MSTI Mapping

When you implement an Spanning Tree protocol on the switch that the bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. Due to the reason that you need to set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) This section describes it allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree MSTI Mapping parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Mapping
2. Specify the configuration identification parameters in the field. Specify the VLANs Mapped blank field.

3. Click the save to save the setting
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	00-05-65-73-c5-90
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Parameter description:

Configuration Identification

1. Configuration Name :

The **MSTP** / **RSTP** / **STP** protocol version setting. Valid values are **STP**, **RSTP** and **MSTP**.

2. Configuration Revision :

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

1. MSTI :

The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

2. 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.

4.8.3.MATI Priorities

When you implement a Spanning Tree protocol on the switch that the bridge instance. The CIST is the default instance which is always active. For 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. The section describes it allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree MSTI Priorities parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Priorities.
2. Scroll the Priority maximum is 240. Default is 128.
3. Click the save to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<> ▼
CIST	32768 ▼
MSTI1	32768 ▼
MSTI2	32768 ▼
MSTI3	32768 ▼
MSTI4	32768 ▼
MSTI5	32768 ▼
MSTI6	32768 ▼
MSTI7	32768 ▼

Parameter description:

1. MSTI :

The bridge instance. The CIST is the default instance, which is always active.

2. 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*.

Buttons

Save – Click to save changes.

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

4.8.4.CIST Ports

When you implement an Spanning Tree protocol on the switch that the bridge instance. You need to configure the CIST Ports. The section describes it allows the user to inspect the to inspect the current STP CIST port configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree CIST Ports parameters in the web interface:

1. Click Configuration, Spanning Tree, CIST Ports
2. Scroll and evoke to set all parameters of CIST Aggregated Port Configuration.
3. Evoke to enable or disable the STP, then scoll and evoke to set all parameters of the CIST normal Port configuration.
4. Click the apply to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

STP CIST Port Configuration

CIST Aggregated Port Configuration										
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point	
						Role	TCN			
-	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True	

CIST Normal Port Configuration										
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point	
						Role	TCN			
*	<input checked="" type="checkbox"/>	<>	<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>	
1	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
2	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
3	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
4	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
5	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
6	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
7	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
8	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	

Save Reset

Parameter description:

1. Port :

The switch port number of the logical STP port.

2. STP Enabled :

Controls whether STP is enabled on this switch port.

3. 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.

4. Priority :

Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

5. 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.

6. AdminEdge :

Controls whether the *operEdge* flag should start as set or cleared. (The initial *operEdge* state when a port is initialized).

7. 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.

8. 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**.

9. 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.

10. 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.

11. 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.

4.8.5.MSTI Ports

The section describes it 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. It contains MSTI port settings for physical and aggregated ports.

Web Interface

To configure the Spanning Tree MSTI Port Configuration parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Ports
2. Scroll to select the MST1 or other MSTI Port
3. Click Get to set the detail parameters of the MSTI Ports.
4. Scroll to set all parameters of the MSTI Port configuration.
5. Click the save to save the setting
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

MSTI Port Configuration

Select MSTI

MST1 ▾

Get

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto ▾	128 ▾

MSTI Normal Ports Configuration

Port	Path Cost	Priority
*	<> ▾	<> ▾
1	Auto ▾	128 ▾
2	Auto ▾	128 ▾
3	Auto ▾	128 ▾
4	Auto ▾	128 ▾
5	Auto ▾	128 ▾
6	Auto ▾	128 ▾
7	Auto ▾	128 ▾
8	Auto ▾	128 ▾

Save

Reset

Parameter description:

1. Port :

The switch port number of the corresponding STP CIST (and MSTI) port.

2. 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.

3. 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.

Save – Click to save changes.

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

4.9 IPMC Profile

4.9.1.Profile Table

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

Web Interface

To configure the Profile Table in the web interface:

1. Click Configuration, IPMC Profile, Profile Table.

IPMC Profile Configurations

Global Profile Mode	Disabled ▼
---------------------	------------

IPMC Profile Table Setting

Delete	Profile Name	Profile Description	Rule
--------	--------------	---------------------	------

Add New IPMC Profile

Save Reset

Parameter description:

1. Global Profile Mode :

Enable/Disable the Global IPMC Profile.

System starts to do filtering based on profile settings only when the global profile mode is enabled.

2. Delete :

Check to delete the entry.

The designated entry will be deleted during the next save.

3. Profile Name :

The name used for indexing the profile table.

Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.


4. Profile Description :

Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile.

No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.

5. Rule :

When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:

 : List the rules associated with the designated profile.

 : Adjust the rules associated with the designated profile.

Buttons :

Add New IPMC Profile – Click to add new IPMC profile. Specify the name and configure the new entry.

Click "Save".

Save – Click to save changes.

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

4.9.2.Address Entry

The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create at maximum 128 address entries in the system.

Web Interface

To configure the Profile Table in the web interface:

1. Click Configuration, IPMC Profile, Address Entry.

IPMC Profile Address Configuration

Refresh | << >>

 Navigate Address Entry Setting in IPMC Profile by entries per page.

Delete	Entry Name	Start Address	End Address
--------	------------	---------------	-------------

Parameter description:
1. Delete :

Enable/Disable the Global IPMC Profile.
 Check to delete the entry.
 The designated entry will be deleted during the next save.

2. Entry :

The name used for indexing the address entry table.
 Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

3. Star Address :

The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

4. End Address :

The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons :

Add New Address(Range) Entry – Click to add new address range. Specify the name and configure the addresses.

Click "Save"

Save – Click to save changes.

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

Refresh – Refreshes the displayed table starting from the input fields.

|<< – Updates the table starting from the first entry in the IPMC Profile Address Configuration.

>> – Updates the table, starting with the entry after the last entry currently displayed.

4.10 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLANs. In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

It is allowed to create at maximum 4 MVR VLANs with corresponding channel profile for each Multicast VLAN.

The channel profile is defined by the IPMC Profile which provides the filtering conditions.

Web Interface

To configure the Profile Table in the web interface:

1. Click Configuration, MVR.

MVR Configurations

MVR Mode

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

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

Immediate Leave Setting

Port	Immediate Leave
*	<input type="text" value="<>"/>
1	<input type="text" value="Disabled"/>
2	<input type="text" value="Disabled"/>
3	<input type="text" value="Disabled"/>
4	<input type="text" value="Disabled"/>
5	<input type="text" value="Disabled"/>
6	<input type="text" value="Disabled"/>
7	<input type="text" value="Disabled"/>
8	<input type="text" value="Disabled"/>

Parameter description:

1. MVR Mode :

Enable/Disable the Global IPMC Profile.
Check to delete the entry.

2. Delete :

Check to delete the entry. The designated entry will be deleted during the next save.

3. MVR VID :

Specify the Multicast [VLAN ID](#).

Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

4. MVR Name :

MVR Name is an optional attribute to indicate the name of the specific MVR VLAN.

Maximum length of the MVR VLAN Name string is 16. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

5. IGMP Address :

Define the IPv4 address as source address used in IP header for **IGMP** control frames.

The default IGMP address is not set (0.0.0.0).

When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address.

Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

6. Mode :

Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.

7. Tagging :

Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.

8. Priority :

Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

9. LLQI :

Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.

10. Interface Channel Profile :

When the MVR VLAN is created, select the **IPMC Profile** as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profile selected for designated interface channel is not allowed to have overlapped permit group address.

11. Profile Management Button :

You can inspect the rules of the designated profile by using the following button:



List the rules associated with the designated profile.

12. Port :

The logical port for the settings.

13. Port Role :

Configure an MVR port of the designated MVR VLAN as one of the following roles.

Inactive: The designated port does not participate MVR operations.

Source: Configure uplink ports that receive and send multicast data as source ports.

Subscribers cannot be directly connected to source ports.

Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

Select the port role by clicking the Role symbol to switch the setting.

I indicates Inactive; S indicates Source; R indicates Receiver

The default Role is Inactive.

14. Immediate Leave :

Enable the [fast leave](#) on the port.

15. Buttons :

Add New Address(Range) Entry – Click to add new address range. Specify the name and configure the addresses.

Click "Save"

Save – Click to save changes.

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

4.11 IPMC

4.11.1. IGMP Snooping

The function, is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

4.11.1.1. Basic Configuration

The section describes how to set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP

Web Interface

To configure the IGMP Snooping parameters in the web interface:

1. Click Configuration, IPMC,IGMP Snooping, Basic Configuration
2. Evoke to select enable or disable which Global configuration
3. Evoke which port wants to become a Router Port or enable/ disable the Fast Leave function..
4. Scroll to set the Throtting parameter.
5. Click the apply to save the setting
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throtting
*	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Parameter description:

1. Snooping Enabled :

Enable the Global IGMP Snooping.

2. 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.

3. 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.

4. Leave Proxy Enabled :

Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

5. Proxy Enabled :

Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

6. 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.

7. Fast Leave :

Enable the fast leave on the port.

8. Throttling :

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons :

Save – Click to save changes.

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

4.11.1.2. VLAN Configuration

The section describes the VLAN configuration setting process integrated with IGMP Snooping function. For Each setting 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. Clicking the button will update the displayed table starting from that or the next closest VLAN Table match.

Web Interface

To configure the IGMP Snooping VLAN Configuration in the web interface:

1. Click Configuration, IPMC, IGMP Snooping, VLAN Configuration
2. Evoke to select enable or disable Snooping , IGMP Querier. Specify the parameters in the blank field.
3. Click the refresh to update the data or click << or >> to display previous entry or next entry.
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

IGMP Snooping VLAN Configuration Refresh | << | >>

Start from VLAN with entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Add New IGMP VLAN											
Save Reset											

Parameter description:

1. Delete :

Check to delete the entry. The designated entry will be deleted during the next save.

2. VLAN ID :

The VLAN ID of the entry.

3. IGMP Snooping Enabled :

Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.

4. Querier Election :

Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

5. 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 192.162.2.1.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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).

11. 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).

12. 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.

Save – Click to save changes.

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

4.11.1.3. Port Filtering Profile

The section describes how to set the IGMP Port Group Filtering? With the IGMP filtering feature, an user can exert this type of control. In some network Application environments, as like the metropolitan or multiple-dwelling unit (MDU) installations, an user might want to control the multicast groups to which a user on a switch port can belong. It allows the user to control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.









With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing. IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

Web Interface

To configure the IGMP Snooping Port Group Configuration in the web interface:

1. Click Configuration, IPMC, IGMP Snooping, Port Filtering Profile.
2. Click Add new Filtering Group.
3. Scroll the Port to enable the Port Group Filtering. Specify the Filtering Groups in the blank field.
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

IGMP Snooping Port Filtering Profile Configuration

Port	Filtering Profile
1	 - ▾
2	 - ▾
3	 - ▾
4	 - ▾
5	 - ▾
6	 - ▾
7	 - ▾
8	 - ▾

Parameter description:**1. Port :**


The logical port for the settings.

2. Filtering Profile :

Select the [IPMC Profile](#) as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

3. Profile Management Button :

You can inspect the rules of the designated profile by using the following button:

 : List the rules associated with the designated profile.

Buttons :

Save – Click to save changes.

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

4.11.2. MLD Snooping**4.11.2.1. Basic Configuration**

This page provides MLD Snooping related configuration.

Web Interface

To configure the IGMP Snooping parameters in the web interface:

1. Click Configuration, IPMC,MLD Snooping, Basic Configuration
2. Evoke to select enable or disable which Global configuration
3. Evoke which port wants to become a Router Port or enable/ disable the Fast Leave function..
4. Scroll to set the Throtting parameter.
5. Click the apply to save the setting
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

MLD Snooping Configuration

Global Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv6 Flooding Enabled	<input checked="" type="checkbox"/>
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Parameter description:

1. Snooping Enabled :

Enable the Global MLD Snooping.

2. Unregistered IPMCv4 Flooding Enabled :

Enable unregistered IPMCv6 traffic flooding.

The flooding control takes effect only when MLD Snooping is enabled.

When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

3. MLD SSM Range :

SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

4. Leave Proxy Enabled :

Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

5. Proxy Enabled :

Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

6. Router Port :

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

7. Fast Leave :

Enable the fast leave on the port.

8. Throttling :

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons :

Save – Click to save changes.

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

4.11.2.2. VLAN Configuration

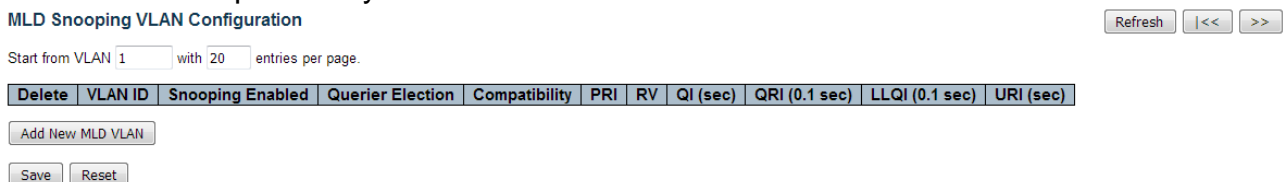
Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN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

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

Web Interface

To configure the MLD Snooping VLAN Configuration in the web interface:

1. Click Configuration, IPMC, MLD Snooping, VLAN Configuration
2. Evoke to select enable or disable Snooping , MLD Querier. Specify the parameters in the blank field.
3. Click the refresh to update the data or click << or >> to display previous entry or next entry.
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values



Parameter description:

1. Delete :

Check to delete the entry. The designated entry will be deleted during the next save.

2. VLAN ID :

The VLAN ID of the entry.

3. MLD Snooping Enabled :

Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.

4. Querier Election :

Enable to join MLD Querier election in the VLAN. Disable to act as an MLD Non-Querier.

5. 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 **MLD-Auto, Forced MLDv1, Forced MLDv2, Forced MLDv3**, default compatibility value is MLD-Auto.

6. PRI :

Priority of Interface.

It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

The allowed range is **0** (best effort) to **7** (highest), default interface priority value is 0.

7. 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.

8. 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.

9. 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).

10. LLQI :

Last Listener Query Interval.

The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum

Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages.

The allowed range is **0** to **31744** in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).

11. URI :

Unsolicited Report Interval.

The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address.

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 MLD VLAN. Specify the VID and configure the new entry. Click "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.

Save – Click to save changes.

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

4.11.2.3. Port Filtering Profile

The section describes how to set the MLD Port Group Filtering? With the MLD filtering feature, an user can exert this type of control. In some network Application environments, as like the metropolitan or multiple-dwelling unit (MDU) installations, an user might want to control the multicast groups to which a user on a switch port can belong. It allows the user to control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An MLD profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an MLD profile denying access to a multicast group is applied to a switch port, the MLD join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the MLD report from the port is forwarded for normal processing. MLD filtering controls only MLD membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.









Web Interface

To configure the MLD Snooping Port Group Configuration in the web interface:

1. Click Configuration, IPMC, MLD Snooping, Port Filtering Profile.
2. Click Add new Filtering Group.
3. Scroll the Port to enable the Port Group Filtering. Specify the Filtering Groups in the blank field.
4. Click the save to save the setting

- If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

MLD Snooping Port Filtering Profile Configuration

Port	Filtering Profile
1	 - ▼
2	 - ▼
3	 - ▼
4	 - ▼
5	 - ▼
6	 - ▼
7	 - ▼
8	 - ▼

Parameter description:

1. Port :

The logical port for the settings.

2. Filtering Profile :

Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

3. Profile Management Button :

You can inspect the rules of the designated profile by using the following button:

 : List the rules associated with the designated profile.

Buttons :

Save – Click to save changes.

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

4.12 LLDP

The switch supports the LLDP. For current information on your switch model, The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity

Discovery specified in standards document IEEE 802.1AB.

4.12.1. LLDP

You can per port to do the LLDP configuration and the detail parameters, the settings will take effect immediately. This page allows the user to inspect and configure the current LLDP port settings.

Web Interface

To configure the LLDP in the web interface:

1. Click Configuration, LLDP.
2. Modify LLDP timing parameters
3. Set the required mode for transmitting or receiving LLDP messages
4. Specify the information to include in the TLV field of advertised messages
5. Click Apply

LLDP Configuration

LLDP Parameters

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

LLDP Port Configuration

Port	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Save Reset

Parameter description:

LLDP Parameters

1. 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.

2. 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.

3. 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.

4. 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 Configuration

1. Port :

The switch port number of the logical LLDP port.

2. 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.

3. 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.

4. Port Descr :

Optional TLV: When checked the "port description" is included in LLDP information transmitted.

5. Sys Name :

Optional TLV: When checked the "system name" is included in LLDP information transmitted.

6. Sys Descr :

Optional TLV: When checked the "system description" is included in LLDP information transmitted.

7. Sys Capa :

Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

8. Mgmt Addr :

Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons :

Save – Click to save changes.

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

4.12.2. LLDP-MED

Media Endpoint Discovery is an enhancement of LLDP, known as LLDP-MED that provides the following facilities:

Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services (Diffserv) settings) enabling plug and play networking.

Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.

Extended and automated power management of Power over Ethernet (PoE) end points.

Inventory management, allowing network administrators to track their network devices, and

determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

Web Interface

To configure the LLDP-MED in the web interface:

1. Click Configuration, LLDP-MED.
2. Modify Fast start repeat count parameter, default is 4
3. Modify Coordinates Location parameters
4. Fill Civic Address Location parameters
5. Add new policy
6. Click Apply, will show following Policy Port Configuration
7. Select Policy ID for each port
8. Click Apply

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count	<input type="text" value="4"/>
-------------------------	--------------------------------

Coordinates Location

Latitude	<input type="text" value="0"/>	°	North	▼	Longitude	<input type="text" value="0"/>	°	East	▼	Altitude	<input type="text" value="0"/>	Meters	▼	Map Datum	WGS84	▼
----------	--------------------------------	---	-------	---	-----------	--------------------------------	---	------	---	----------	--------------------------------	--------	---	-----------	-------	---

Civic Address Location

Country code	<input type="text"/>	State	<input type="text"/>	County	<input type="text"/>
City	<input type="text"/>	City district	<input type="text"/>	Block (Neighborhood)	<input type="text"/>
Street	<input type="text"/>	Leading street direction	<input type="text"/>	Trailing street suffix	<input type="text"/>
Street suffix	<input type="text"/>	House no.	<input type="text"/>	House no. suffix	<input type="text"/>
Landmark	<input type="text"/>	Additional location info	<input type="text"/>	Name	<input type="text"/>
Zip code	<input type="text"/>	Building	<input type="text"/>	Apartment	<input type="text"/>
Floor	<input type="text"/>	Room no.	<input type="text"/>	Place type	<input type="text"/>
Postal community name	<input type="text"/>	P.O. Box	<input type="text"/>	Additional code	<input type="text"/>

Emergency Call Service

Emergency Call Service	<input type="text"/>
------------------------	----------------------

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

Parameter description:

Fast start repeat count

1. Fast start repeat count :

Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to

permitted voice-capable devices), both in order to conserve the limited LLDPDU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDPMED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With **Fast start repeat count** it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN

infrastructure elements, including Network Connectivity Devices, or other types of links.

Coordinates Location

1. Latitude :

Rapid startup and Emergency Call Service Location Identification Discovery of

2. Longitude :

Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.

It is possible to specify the direction to either **East** of the prime meridian or **West** of the prime meridian.

3. Altitude :

Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits.

It is possible to select between two altitude types (floors or meters).

Meters: Representing meters of Altitude defined by the vertical datum specified.

Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

4. Map Datum :

The **Map Datum** is used for the coordinates given in these options:

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Coordinates Location

1. Country code :

The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

2. State :

National subdivisions (state, canton, region, province, prefecture).

3. County :

County, parish, gun (Japan), district.

4. City :

City, township, shi (Japan) - Example: Copenhagen.

5. City district :

City division, borough, city district, ward, chou (Japan).

6. Block (Neighborhood) :

Neighborhood, block.

7. Street :

Street - Example: Poppelvej.

8. Leading street direction :

Leading street direction - Example: N.

9. Trailing street suffix :

Trailing street suffix - Example: SW.

10. Street suffix :

Street suffix - Example: Ave, Platz.

11. House no. :

House number - Example: 21.

12. House no. suffix :

House number suffix - Example: A, 1/2.

13. Landmark :

Landmark or vanity address - Example: Columbia University.

14. Additional location info :

Additional location info - Example: South Wing.

15. Name :

Name (residence and office occupant) - Example: Flemming Jahn.

16. Zip code :

Postal/zip code - Example: 2791.

17. Building :

Building (structure) - Example: Low Library.

18. Apartment :

Unit (Apartment, suite) - Example: Apt 42.

19. Floor :

Floor - Example: 4.

20. Room no. :

Room number - Example: 450F.

21. Place type :

Place type - Example: Office.

22. Postal community name :

Postal community name - Example: Leonia.

23. P.O. Box :

Post office box (P.O. BOX) - Example: 12345.

24. Additional code :

Additional code - Example: 1320300003.

Emergency Call Service**1. Emergency Call Service :**

Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunkbased PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

1. Delete :

Check to delete the policy. It will be deleted during the next save.

2. Policy ID :

ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific ports.

3. Application Type :

Intended use of the application types:

1. **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. **Voice Signalling** (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the **Voice** application policy.
3. **Guest Voice** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. **Guest Voice Signalling** (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the **Guest Voice** application policy.
5. **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.
6. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. **Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. **Video Signalling** (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the **Video Conferencing** application policy.

4. Tag :

Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.

Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

5. VLAN ID :

VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.

6. L2 Priority :

L2 Priority is the Layer 2 priority to be used for the specified application type. **L2 Priority** may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

7. DSCP :

DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. **DSCP** may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

8. Adding a new policy :

Click "Add New Policy" to add a new policy. Specify the **Application type, Tag, VLAN ID, L2 Priority** and **DSCP** for the new policy. Click "Save".

The number of policies supported is 32.

Port Policies Configuration

1. Port :

The port number to which the configuration applies.

2. Policy ID :

The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons :

Save – Click to save changes.

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

4.13 PoE

Power over Ethernet or **PoE** describes any of several standardized or ad-hoc systems which pass electric power along with data on twisted pair Ethernet cabling. This allows a single cable to provide both data connection and electric power to devices such as wireless access points, IP cameras, and VoIP phones.

4.13.1. PoE

This page allows the user to inspect and configure the current PoE port settings and show all PoE Supply.

Web Interface

To configure Power Over Ethernet in the web interface:

1. Click configuration, PoE, and configuration
2. Specify the Reserved Power determined and Power Management mode. Specify the PoE or PoE++ and Priority.
3. Click Apply.

Power Over Ethernet Configuration

Reserved Power determined by	<input checked="" type="radio"/> Class	<input type="radio"/> Allocation	<input type="radio"/> LLDP-MED
Power Management Mode	<input type="radio"/> Actual Consumption	<input checked="" type="radio"/> Reserved Power	

PoE Power Supply Configuration

Primary Power Supply [W]	120
--------------------------	-----

PoE Port Configuration

Port	Mode	Operation	Priority	Maximum Power [W]
*	<>	<>	<>	15.4
1	Enable	802.3at	Low	15.4
2	Enable	802.3at	Low	15.4
3	Enable	802.3at	Low	15.4
4	Enable	802.3at	Low	15.4

Parameter description:

Reserved Power determined by

1. Allocated mode :

In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.

2. Class Mode :

In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect.

3. LLDP-MED mode :

This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode. In this mode the Maximum Power fields have no effect.

Power Management Mode

1. Actual Consumption :

In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.

2. Reserved Power :

In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.

Power Supply Configuration

1. Power Source :

For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver. Valid values are in the range 0 to 240 Watts.

Port Configuration

1. Port :

This is the logical port number for this row. Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.

PoE Mode

1. Disable :

PoE disabled for the port.

2. Enable :

Enables PoE for the port.

3. Schedule :

Enables PoE for the port by scheduling.

Operation Mode**1. 802.3af :**

Sets PoE protocol to IEEE 802.3af.

2. 802.3at :

Sets PoE protocol to IEEE 802.3at.

4Pairs**1. Enable :**

Enable 4Pairs to support 60W.

The option is only available when following rules are applied.

- High power model supports.
- Only port1 or port2 supports
- Current operation mode is 802.3at.

2. Disable :

Disable 4Pairs to limit 30W of power.

Priority

The priority is used in the case where the remote devices require more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

1. Low :

Enable 4Pairs to support 60W.

The option is only available when following rules are applied.

- High power model supports.
- Only port1 or port2 supports
- Current operation mode is 802.3at.

2. High :

The medium priority

3. Critical :

The highest priority

Maximum Power

The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.

For port support 4Pairs mode, the maximum allowed value is 60 W; others are 30 W.

Buttons :

Save – Click to save changes.

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

4.13.2. Power Scheduler

This page allows the user to make a perfect schedule of PoE power supply. PoE Scheduling not only makes PoE management easier but also saves more energy

Web Interface

To Display Power Over Ethernet Scheduler in the web interface:

1. Click Configuration, PoE, and Scheduler
2. Select the local port and enable.
3. Select time and day to supply power.
4. Click Apply to apply the change.

PoE Power Scheduling Control on Port 1

Power Scheduling Interval Configuration

Day							Interval	Action
Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.	Start - End	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	00:00 - 00:29	<input checked="" type="radio"/> Power ON <input type="radio"/> Power OFF

Apply

Power Scheduling During 00:00 - 05:59

Time Interval	Day						
	Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.
00:00 - 00:29	●	●	●	●	●	●	●
00:30 - 00:59	●	●	●	●	●	●	●
01:00 - 01:29	●	●	●	●	●	●	●
01:30 - 01:59	●	●	●	●	●	●	●
02:00 - 02:29	●	●	●	●	●	●	●
02:30 - 02:59	●	●	●	●	●	●	●
03:00 - 03:29	●	●	●	●	●	●	●
03:30 - 03:59	●	●	●	●	●	●	●
04:00 - 04:29	●	●	●	●	●	●	●
04:30 - 04:59	●	●	●	●	●	●	●
05:00 - 05:29	●	●	●	●	●	●	●
05:30 - 05:59	●	●	●	●	●	●	●

Save Reset

Parameter description:

Power Scheduling Interval Configuration

1. Day :

In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.

2. Interval :

Start - Select the start hour and minute.

End - Select the end hour and minute.

3. Action

Power On - Select the radio button to apply power on during the interval.

Power Off - Select the radio button to apply power off during the interval.

Power Scheduling Interval Configuration

1. Time Interval :

There are 48 time interval one day. Each interval have 30 minutes.

2. Day :

The current scheduling state is displayed graphically during the week.

Green indicates the power is on and red that it is off.

Directly changes checkmarks to indicate which day are members of the time interval.

Check or uncheck as needed to modify the scheduling table.

Buttons :

Apply – Click to apply the power scheduling interval.

Save – Click to save changes.

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

4.13.3. Power Reset

This page provides power reset entry configurations.

The entry is used to control the power reset time on PoE port.

It is allowed to create at maximum 5 entries for each PoE port.

Web Interface

To configure Power Reset in the web interface:

1. Click configuration, PoE, and Power Reset

PoE Power Reset Control on Port 1

Delete	Day							Time (hh:mm)
	Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.	

Add New

Save Reset

Parameter description:

1. Delete :

In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.

2. Day :

Checkmarks indicate which day are members of the entry. Check or uncheck as needed to modify the entry.

3. Time (hh:mm) :

hh - Select the hour.
mm - Select the minute.

Buttons :

Add New – Click to add new reset entry.

Save – Click to save changes.

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

4.14 MAC Address Tables

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time

4.15.1. Configuration

Web Interface

To configure MAC Address Table in the web interface:

Aging Configuration

1. Click configuration .
2. Specify the Disable Automatic Aging and Aging Time.
3. Click Apply.

MAC Table Learning

1. Click configuration .
2. Specify the Port Members(Auto,Disable,Secure).
3. Click Apply.

Static MAC Table Configuration

1. Click configuration and Add new Static entry .
2. Specify the VLAN IP and Mac address ,Port Members.
3. Click Apply.

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	<input type="checkbox"/>
Aging Time	300 seconds

MAC Table Learning

	Port Members							
	1	2	3	4	5	6	7	8
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Static MAC Table Configuration

			Port Members							
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8

Add New Static Entry

Save Reset

Parameter description:

Aging Configuration

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

Configure aging time by entering a value here in seconds; for example, Age time seconds.

The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking Disable automatic aging.

1. Disable Automatic Aging :

Disable the automatic aging of dynamic entries by ticking the item.

2. Disable Automatic Aging :

Enter a value in seconds.

The allowed range is **10** to **1000000** seconds.

MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can do learning based upon the following settings:

1. Auto :

Learning is done automatically as soon as a frame with unknown SMAC is received.

2. Disable :

No learning is done.

3. 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 Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.

1. Delete :

Check to delete the entry. It will be deleted during the next save.

2. VLAN ID :

The VLAN ID of the entry.

3. MAC Address :

The MAC address of the entry.

4. Port Members :

Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

5. Adding a New Static Entry :

Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply".

Buttons:

Apply – Click to save changes.

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

4.15 VLANs

To assign a specific VLAN for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN using the Management VLAN window. Only one management VLAN can be active at a time. When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click configuration VLANs.
2. Specify Existing VLANs, Ethertype for Custom S-ports.
3. Click Apply.

Global VLAN Configuration

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

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

Save Reset

Parameter description:

Global VLAN Configuration

1. 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.

2. EtherType for Custom Sports :

This field specifies the etherType/TPID (specified in hexadecimal) used for Custom Sports.

The setting is in force for all ports whose **Port Type** is set to S-Custom-Port.

Port VLAN Configuration

1. Port :

This is the logical port number of this row.

2. 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

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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:

Apply – Click to save changes.

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

4.16 Private VLANs

The VLAN membership configuration for the selected stack switch unit switch can be monitored and modified here. Up to 4096 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

4.16.1. Membership

The [Private VLAN](#) membership configurations for the switch can be monitored and modified here.

Private [VLANs](#) can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that [VLAN IDs](#) and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click configuration VLANs.

2. Specify Existing VLANs, Ethertype for Custom S-ports.
3. Click Apply.

Private VLAN Membership Configuration

		Port Members							
Delete	PVLAN ID	1	2	3	4	5	6	7	8
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add New Private VLAN

Save Reset

Parameter description:

1. Delete :

To delete a private VLAN entry, check this box. The entry will be deleted during the next save.

2. PVLAN ID :

Indicates the ID of this particular private VLAN.

3. Port Member :

A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

4. Adding a New VLAN :

Click to "add a new VLAN ID". An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled on the selected stack switch unit when you click on "Save". The VLAN is thereafter present on the other stack switch units, but with no port members. The check box is greyed out when VLAN is displayed on other stacked switches, but user can add member ports to it. A VLAN without any port members on any stack unit will be deleted when you click "Save". The "Delete" button can be used to undo the addition of new VLANs.

Button :

Refresh – Click to save changes.

Add New Private VLAN –Click to add a new private VLAN ID

Save – Click to save changes.

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

4.16.2. Port Isolation

Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said

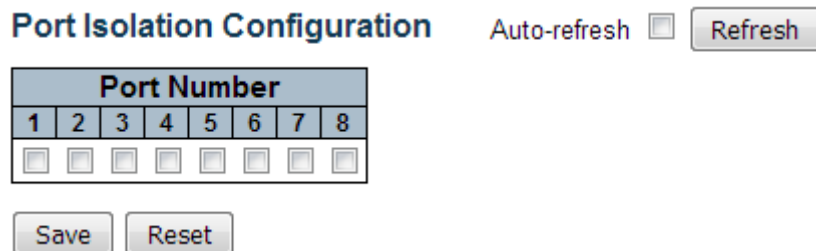
plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map which is responsive to a destination address of a data packet. The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on an data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Web Interface

To configure Port Isolation configuration in the web interface:

1. Click Private VLAN, Port Isolation.
2. Evoke which port want to enable Port Isolation.
3. Click Save.



Port Number							
1	2	3	4	5	6	7	8
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Parameter description:

1. Port Member :

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

Button :

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

Refresh – Click to refresh the page immediately.

Save – Click to save changes.

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

4.17 VCL

4.17.1. MAC-based VLAN

MAC address-based VLAN decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

A most common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure, and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do, which brings security issues. To provide user access and ensure data security in the meantime, the MAC-based VLAN technology is developed.

MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

Web Interface

To configure MAC address-based VLAN configuration in the web interface:

1. Click VCL, MAC-based VLAN configuration and add new entry.
2. Specify the MAC address and VLAN ID.
3. Click Save.

MAC-based VLAN Membership Configuration Auto-refresh Refresh |<< >>|

	Delete	MAC Address	VLAN ID	1	2	3	4	5	6	7	8	Port Members	
Currently no entries present													

Parameter description:

1. Delete :

To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted in the stack.

2. MAC Address :

Indicates the MAC address.

3. VLAN ID :

Indicates the VLAN ID.

4. Port Member :

A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

5. Adding a New Mac-based VLAN :

Click “Add New Entry” to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are **1** through **4095**.

The MAC-based VLAN entry is enabled when you click on "Save". A MAC-based VLAN without any port members will be deleted when you click "Save".

The “Delete” button can be used to undo the addition of new MAC-based VLANs. The maximum possible MAC-based VLAN entries are limited to 256.

Button :

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

Refresh – Click to refresh the page immediately.

Save – Click to save changes.

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

|<< – Updates the table starting from the first entry in the MAC-based VLAN Table.

>> – Updates the table, starting with the entry after the last entry currently displayed.

4.17.2. Protocol-based VLAN

This section describe Protocol -based VLAN, The Switch support Protocol include Ethernet LLC SNAP Protocol,

LLC

The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet and Appletalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP

The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

4.17.2.1. Protocol to Group

This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the selected stack switch unit switch.

Web Interface

To configure Protocol -based VLAN configuration in the web interface:

1. Click VCL, Protocol-based VLAN, Protocol to Group.
2. Specify the Ethernet LLC SNAP Protocol and Group Name.
3. Click Save.

Protocol to Group Mapping Table

Auto-refresh Refresh

Delete	Frame Type	Value	Group Name
No Group entry found!			

Add New Entry

Save Reset

Parameter description:

1. Delete :

To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.

2. Frame Type :

Frame Type can have one of the following values:

Ethernet

LLC

SNAP

Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.

3. Value :

Valid value that can be entered in this text field depends on the option selected from

the preceding Frame Type selection menu.

Below is the criteria for three different Frame Types:

For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff

For LLC: Valid value in this case is comprised of two different sub-values.

a. **DSAP:** 1-byte long string (0x00-0xff)

b. **SSAP:** 1-byte long string (0x00-0xff)

For SNAP: Valid value in this case also is comprised of two different subvalues.

a. **OUI:** OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.

b. **PID:** If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type

(EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

4. Group Name :

A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9).

Note: special character and underscore(_) are not allowed.

Button :

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

Refresh – Click to refresh the page immediately.

Add New Entry – Click to add a new entry in mapping table.

Save – Click to save changes.

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

4.17.2.2. Group to VLAN

This section allows you to map a already configured Group Name to a VLAN for the selected stack switch unit switch .

Web Interface

To Display Group Name to VLAN mapping table configured in the web interface:

1. Click VCL, Group Name VLAN configuration and add new entry.
2. Specify the Group Name and VLAN ID.
3. Click Save.

Group Name to VLAN mapping Table

Auto-refresh Refresh

			Port Members							
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8
No Group entries										

Add New Entry

Save Reset

Parameter description:

1. Delete :

To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save.

2. Group Name :

A valid Group Name is a string of at the most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. whichever Group name you try map to a VLAN must be present in

Protocol to Group mapping table and must not be preused by any other existing mapping entry on this page.

3. VLAN ID :

Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.

4. Port Member :

A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

5. Adding a New Group to VLAN mapping entry :

Click “Add New Entry” to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The “Delete” button can be used to undo the addition of new entry.

Button :

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

Refresh – Click to refresh the page immediately.

Add New Entry – Click to add a new entry in mapping table. Legal values for a VLAN ID are 1 through 4095.

Save – Click to save changes.

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

Delete – The button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 64.

4.17.3. IP Subnet-based VLAN

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

Web Interface

To Display IP subnet-based VLAN Membership to configured in the web interface:

1. Click VCL, Group Name VLAN configuration and add new entry.
2. Specify the VCE ID, IP Address, Mask Length, VLAN ID and select Port Members..
3. Click Save.

IP Subnet-based VLAN Membership Configuration

 Auto-refresh Refresh

Delete	VCE ID	IP Address	Mask Length	VLAN ID	Port Members							
					1	2	3	4	5	6	7	8
Currently no entries present												

Add New Entry

Save Reset

Parameter description:
1. Delete :

To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

2. VCE ID :

Indicates the index of the entry. It is user configurable. It's value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.

3. IP Address :

Indicates the IP address.

4. Mask Length :

Indicates the network mask length.

5. VLAN ID :

Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

6. Port Member :

A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Button :

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

Refresh – Click to refresh the page immediately.

Add New Entry – Click to add a new entry in mapping table. Legal values for a VLAN ID are 1 through 4095.

Save – Click to save changes.

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

Delete – The button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 64.

4.18 Voice VLAN

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

4.18.1. Configuration

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

Web Interface

To configure Voice VLAN in the web interface:

1. Select "Enabled" in the Voice VLAN Configuration.
2. Specify VLAN ID Aging Time Traffic Class.
3. Specify (Port Mode, Security, Discovery Protocol) in the Port Configuration
4. Click Save.

Voice VLAN Configuration

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

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<> ▾	<> ▾	<> ▾
1	Disabled ▾	Disabled ▾	OUI ▾
2	Disabled ▾	Disabled ▾	OUI ▾
3	Disabled ▾	Disabled ▾	OUI ▾
4	Disabled ▾	Disabled ▾	OUI ▾
5	Disabled ▾	Disabled ▾	OUI ▾
6	Disabled ▾	Disabled ▾	OUI ▾
7	Disabled ▾	Disabled ▾	OUI ▾
8	Disabled ▾	Disabled ▾	OUI ▾

Parameter description:

1. Mode :

Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

Enabled: Enable Voice VLAN mode operation.

Disabled: Disable Voice VLAN mode operation.

2. VLAN ID :

Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is **1** to **4095**.

3. Aging Time :

Indicates the Voice VLAN secure learning aging time. The allowed range is **10** to **10000000** seconds. It is used when security mode or auto detect mode is enabled.

In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

4. Traffic Class :

Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

5. Port Mode :

Indicates the Voice VLAN port mode. Possible port modes are:

Disabled: Disjoin from Voice VLAN.

Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.

Forced: Force join to Voice VLAN.

6. Port Security :

Indicates the network mask length.

Indicates the Voice VLAN port security mode. When the function is enabled, all nontelephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds.

Possible port modes are:

Enabled: Enable Voice VLAN security mode operation.

Disabled: Disable Voice VLAN security mode operation.

7. Port Security :

Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:

OUI: Detect telephony device by OUI address.

LLDP: Detect telephony device by LLDP.

Both: Both OUI and LLDP.

Button :

Save – Click to save changes.

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

4.18.2. OUI

The section describes to Configure VOICE VLAN OUI table . The maximum entry number is 16. Modifying the OUI table will restart auto detection of OUI process.

Web Interface

To configure Voice VLAN OUI Table in the web interface:

1. Select "Add new entry" ,"Delete" in the Voice VLAN OUI table.
2. Specify Telephony OUI, Description.
3. Click Save.

Voice VLAN OUI Table

Delete	Telephony OUI	Description
<input type="checkbox"/>	00-01-e3	Siemens AG phones
<input type="checkbox"/>	00-03-6b	Cisco phones
<input type="checkbox"/>	00-0f-e2	H3C phones
<input type="checkbox"/>	00-60-b9	Philips and NEC AG phones
<input type="checkbox"/>	00-d0-1e	Pingtel phones
<input type="checkbox"/>	00-e0-75	Polycom phones
<input type="checkbox"/>	00-e0-bb	3Com phones

Add New Entry

Save

Reset

Parameter description:

1. Delete :

Check to delete the entry. It will be deleted during the next save.

2. Telephony OUI :

A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE.

It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

3. Description :

The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is **0** to **32**.

Button :

Add New Entry – Click to add a new access management entry.

Save – Click to save changes.

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

4.19 QoS

The switch support four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges. High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class. The switch support advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

4.19.1. Port Classification

The section allows you to configure the basic QoS Ingress Classification settings for all switch ports. and the settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the QoS Port Classification parameters in the web interface:

1. Click Configuration, QoS, Port Classification
2. Scroll to select QoS class, DP Level, PCP and DEI parameters
3. Click the save to save the setting
4. If you want to cancel the setting then you need to click the Reset button.
It will revert to previously saved values

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<> ▾	<> ▾	<> ▾	<> ▾		<input type="checkbox"/>	<> ▾
1	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	Source ▾
2	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	Source ▾
3	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	Source ▾
4	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	Source ▾
5	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	Source ▾
6	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	Source ▾
7	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	Source ▾
8	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	<input type="checkbox"/>	Source ▾

Parameter description:

1. Port :

The port number for which the configuration below applies.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. DSCP Based :

Click to Enable DSCP Based QoS Ingress Port Classification.

8. 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.

Button :

Save – Click to save changes.

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

4.19.2. Port Policing

This section provides an overview of f QoS Ingress Port Policers for all switch ports The Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic.

Web Interface

To display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Policing
2. Evoke which port need to enable the QoS Ingress Port Policers and type the Rate limit condition.
3. Scroll to select the Rate limit Unit with kbps, Mbps, fps and kfps.
4. Click Apply to save the configuration.

QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<> ▼	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>

Parameter description:

1. Port :

The port number for which the configuration below applies.

2. Enabled :

Controls whether the policer is enabled on this switch port.

3. 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".

4. Unit :

Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".

5. Flow Control :

If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Button :

Save – Click to save changes.

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

4.19.3. Port Scheduler

This section provides an overview of QoS Egress Port Schedulers for all switch ports. and the ports belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Schedulers.
2. Display the QoS Egress Port Schedulers.

QoS Egress Port Schedulers

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

Parameter description:

1. Port :

The logical port for the settings contained in the same row.
Click on the port number in order to configure the schedulers.

2. Mode :

Shows the scheduling mode for this port.

3. Qn :

Shows the weight for this queue and port.

4.19.4. Port Shaping

This section provides an overview of QoS Egress Port Shapers for all switch ports. Others the user could get all detail information of the ports belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Shoapers.
2. Display the QoS Egress Port Shapers.

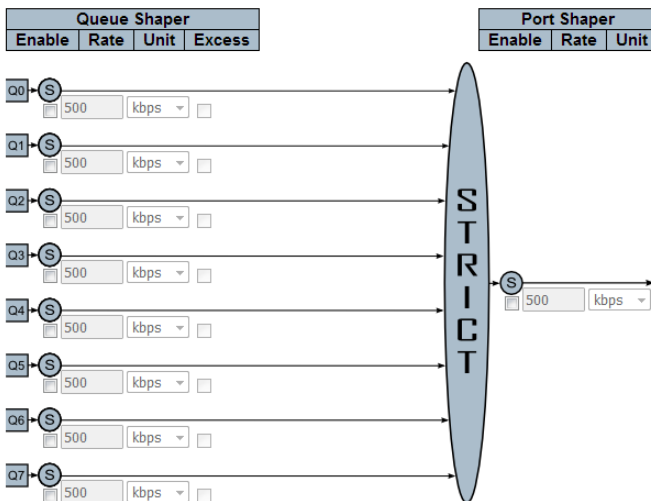
QoS Egress Port Shapers

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

QoS Egress Port Scheduler and Shapers Port 1

Port 1

Scheduler Mode: Strict Priority



Parameter description:

1. Port :

The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.

2. Qn :

Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".

3. Port # :

Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".

4.19.5. Port Tag Remarking

The Section provides user to get an overview of QoS Egress Port Tag Remarking for all switch ports. Others the ports belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To display the QoS Port Tag Remarking in the web interface:

1. Click Configuration, QoS, Tag Remarking .

QoS Egress Port Tag Remarking

Port	Mode
<u>1</u>	Classified
<u>2</u>	Classified
<u>3</u>	Classified
<u>4</u>	Classified
<u>5</u>	Classified
<u>6</u>	Classified
<u>7</u>	Classified
<u>8</u>	Classified

Parameter description:

1. Port :

The logical port for the settings contained in the same row.
Click on the port number in order to configure the shapers.

2. Qn :

Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".

4.19.6. Port DSCP

The section will teach user to set the QoS Port DSCP configuration that was allowed you to configure the basic QoS Port DSCP Configuration settings for all switch ports. Others the settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the QoS Port DSCP parameters in the web interface:

1. Click Configuration, QoS, Tag Remarking .
2. Click Configuration, QoS, Port DSCP.
3. Evoke to enable or disable the Ingress Translate and Scroll the Classify Parameter configuration.
4. Scroll to select Egress Rewrite parameters.
5. Click the save to save the setting.
6. you want to cancel the setting then you need to click the Reset button.
It will revert to previously saved values.

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<>	<>
1	<input type="checkbox"/>	Disable	Disable
2	<input type="checkbox"/>	Disable	Disable
3	<input type="checkbox"/>	Disable	Disable
4	<input type="checkbox"/>	Disable	Disable
5	<input type="checkbox"/>	Disable	Disable
6	<input type="checkbox"/>	Disable	Disable
7	<input type="checkbox"/>	Disable	Disable
8	<input type="checkbox"/>	Disable	Disable

Parameter description:

1. Port :

The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.

2. 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

3. Translate :

To Enable the Ingress Translation click the checkbox.

4. 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.

5. Egress :

To Enable the Ingress Translation click the checkbox.

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.

Button :

Save – Click to save changes.

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

4.19.7. DSCP-Based QoS

The section will teach user to configure the DSCP-Based QoS mode that This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

Web Interface

To configure the DSCP –Based QoS Ingress Classification parameters in the web interface:

1. Click Configuration, QoS, DSCP-Based QoS
2. Evoke to enable or disable the DSCP for Trust
3. Scroll to select QoS Class and DPL parameters
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	<input type="checkbox"/>	<> ▾	<> ▾
0 (BE)	<input type="checkbox"/>	0 ▾	0 ▾
1	<input type="checkbox"/>	0 ▾	0 ▾
2	<input type="checkbox"/>	0 ▾	0 ▾
3	<input type="checkbox"/>	0 ▾	0 ▾
4	<input type="checkbox"/>	0 ▾	0 ▾
5	<input type="checkbox"/>	0 ▾	0 ▾
6	<input type="checkbox"/>	0 ▾	0 ▾
7	<input type="checkbox"/>	0 ▾	0 ▾
8 (CS1)	<input type="checkbox"/>	0 ▾	0 ▾
9	<input type="checkbox"/>	0 ▾	0 ▾
10 (AF11)	<input type="checkbox"/>	0 ▾	0 ▾
11	<input type="checkbox"/>	0 ▾	0 ▾
12 (AF12)	<input type="checkbox"/>	0 ▾	0 ▾
13	<input type="checkbox"/>	0 ▾	0 ▾
14 (AF13)	<input type="checkbox"/>	0 ▾	0 ▾
15	<input type="checkbox"/>	0 ▾	0 ▾
16 (CS2)	<input type="checkbox"/>	0 ▾	0 ▾
17	<input type="checkbox"/>	0 ▾	0 ▾
18 (AF21)	<input type="checkbox"/>	0 ▾	0 ▾

19	<input type="checkbox"/>	0 ▾	0 ▾
20 (AF22)	<input type="checkbox"/>	0 ▾	0 ▾
21	<input type="checkbox"/>	0 ▾	0 ▾
22 (AF23)	<input type="checkbox"/>	0 ▾	0 ▾
23	<input type="checkbox"/>	0 ▾	0 ▾
24 (CS3)	<input type="checkbox"/>	0 ▾	0 ▾
25	<input type="checkbox"/>	0 ▾	0 ▾
26 (AF31)	<input type="checkbox"/>	0 ▾	0 ▾
27	<input type="checkbox"/>	0 ▾	0 ▾
28 (AF32)	<input type="checkbox"/>	0 ▾	0 ▾
29	<input type="checkbox"/>	0 ▾	0 ▾
30 (AF33)	<input type="checkbox"/>	0 ▾	0 ▾
31	<input type="checkbox"/>	0 ▾	0 ▾
32 (CS4)	<input type="checkbox"/>	0 ▾	0 ▾
33	<input type="checkbox"/>	0 ▾	0 ▾
34 (AF41)	<input type="checkbox"/>	0 ▾	0 ▾
35	<input type="checkbox"/>	0 ▾	0 ▾
36 (AF42)	<input type="checkbox"/>	0 ▾	0 ▾
37	<input type="checkbox"/>	0 ▾	0 ▾
38 (AF43)	<input type="checkbox"/>	0 ▾	0 ▾
39	<input type="checkbox"/>	0 ▾	0 ▾
40 (CS5)	<input type="checkbox"/>	0 ▾	0 ▾

41	<input type="checkbox"/>	0 ▾	0 ▾
42	<input type="checkbox"/>	0 ▾	0 ▾
43	<input type="checkbox"/>	0 ▾	0 ▾
44	<input type="checkbox"/>	0 ▾	0 ▾
45	<input type="checkbox"/>	0 ▾	0 ▾
46 (EF)	<input type="checkbox"/>	0 ▾	0 ▾
47	<input type="checkbox"/>	0 ▾	0 ▾
48 (CS6)	<input type="checkbox"/>	0 ▾	0 ▾
49	<input type="checkbox"/>	0 ▾	0 ▾
50	<input type="checkbox"/>	0 ▾	0 ▾
51	<input type="checkbox"/>	0 ▾	0 ▾
52	<input type="checkbox"/>	0 ▾	0 ▾
53	<input type="checkbox"/>	0 ▾	0 ▾
54	<input type="checkbox"/>	0 ▾	0 ▾
55	<input type="checkbox"/>	0 ▾	0 ▾
56 (CS7)	<input type="checkbox"/>	0 ▾	0 ▾
57	<input type="checkbox"/>	0 ▾	0 ▾
58	<input type="checkbox"/>	0 ▾	0 ▾
59	<input type="checkbox"/>	0 ▾	0 ▾
60	<input type="checkbox"/>	0 ▾	0 ▾
61	<input type="checkbox"/>	0 ▾	0 ▾
62	<input type="checkbox"/>	0 ▾	0 ▾
63	<input type="checkbox"/>	0 ▾	0 ▾

Parameter description:

1. DSCP :

Maximum number of supported DSCP values are 64.

2. Trust :

Click to check if the DSCP value is trusted.

3. QoS Class :

QoS Class value can be any of (0-7)

4. DPL :

Drop Precedence Level (0-3)

Button :

Save – Click to save changes.

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

4.19.8. DSCP-Translation

The section describes to teach user to configure and allows you to map DSCP value to a QoS Class and DPL value. Others the settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the DSCP Classification parameters in the web interface:

1. Click Configuration, QoS, DSCP Translation
2. Scroll to set the DSCP Parameters
3. Click the save to save the setting
4. If you want to cancel the setting then you need to click the Reset button.
It will revert to previously saved values

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<> ▾	<input type="checkbox"/>	<> ▾	<> ▾
0 (BE)	0 (BE) ▾	<input type="checkbox"/>	0 (BE) ▾	0 (BE) ▾
1	1 ▾	<input type="checkbox"/>	1 ▾	1 ▾
2	2 ▾	<input type="checkbox"/>	2 ▾	2 ▾
3	3 ▾	<input type="checkbox"/>	3 ▾	3 ▾
4	4 ▾	<input type="checkbox"/>	4 ▾	4 ▾
5	5 ▾	<input type="checkbox"/>	5 ▾	5 ▾
6	6 ▾	<input type="checkbox"/>	6 ▾	6 ▾
7	7 ▾	<input type="checkbox"/>	7 ▾	7 ▾
8 (CS1)	8 (CS1) ▾	<input type="checkbox"/>	8 (CS1) ▾	8 (CS1) ▾
9	9 ▾	<input type="checkbox"/>	9 ▾	9 ▾
10 (AF11)	10 (AF11) ▾	<input type="checkbox"/>	10 (AF11) ▾	10 (AF11) ▾
11	11 ▾	<input type="checkbox"/>	11 ▾	11 ▾
12 (AF12)	12 (AF12) ▾	<input type="checkbox"/>	12 (AF12) ▾	12 (AF12) ▾
13	13 ▾	<input type="checkbox"/>	13 ▾	13 ▾
14 (AF13)	14 (AF13) ▾	<input type="checkbox"/>	14 (AF13) ▾	14 (AF13) ▾
15	15 ▾	<input type="checkbox"/>	15 ▾	15 ▾
16 (CS2)	16 (CS2) ▾	<input type="checkbox"/>	16 (CS2) ▾	16 (CS2) ▾
17	17 ▾	<input type="checkbox"/>	17 ▾	17 ▾
18 (AF21)	18 (AF21) ▾	<input type="checkbox"/>	18 (AF21) ▾	18 (AF21) ▾
19	19 ▾	<input type="checkbox"/>	19 ▾	19 ▾
20 (AF22)	20 (AF22) ▾	<input type="checkbox"/>	20 (AF22) ▾	20 (AF22) ▾
21	21 ▾	<input type="checkbox"/>	21 ▾	21 ▾
22 (AF23)	22 (AF23) ▾	<input type="checkbox"/>	22 (AF23) ▾	22 (AF23) ▾

22 (AF23)	22 (AF23) ▼	<input type="checkbox"/>	22 (AF23) ▼	22 (AF23) ▼
23	23 ▼	<input type="checkbox"/>	23 ▼	23 ▼
24 (CS3)	24 (CS3) ▼	<input type="checkbox"/>	24 (CS3) ▼	24 (CS3) ▼
25	25 ▼	<input type="checkbox"/>	25 ▼	25 ▼
26 (AF31)	26 (AF31) ▼	<input type="checkbox"/>	26 (AF31) ▼	26 (AF31) ▼
27	27 ▼	<input type="checkbox"/>	27 ▼	27 ▼
28 (AF32)	28 (AF32) ▼	<input type="checkbox"/>	28 (AF32) ▼	28 (AF32) ▼
29	29 ▼	<input type="checkbox"/>	29 ▼	29 ▼
30 (AF33)	30 (AF33) ▼	<input type="checkbox"/>	30 (AF33) ▼	30 (AF33) ▼
31	31 ▼	<input type="checkbox"/>	31 ▼	31 ▼
32 (CS4)	32 (CS4) ▼	<input type="checkbox"/>	32 (CS4) ▼	32 (CS4) ▼
33	33 ▼	<input type="checkbox"/>	33 ▼	33 ▼
34 (AF41)	34 (AF41) ▼	<input type="checkbox"/>	34 (AF41) ▼	34 (AF41) ▼
35	35 ▼	<input type="checkbox"/>	35 ▼	35 ▼
36 (AF42)	36 (AF42) ▼	<input type="checkbox"/>	36 (AF42) ▼	36 (AF42) ▼
37	37 ▼	<input type="checkbox"/>	37 ▼	37 ▼
38 (AF43)	38 (AF43) ▼	<input type="checkbox"/>	38 (AF43) ▼	38 (AF43) ▼
39	39 ▼	<input type="checkbox"/>	39 ▼	39 ▼
40 (CS5)	40 (CS5) ▼	<input type="checkbox"/>	40 (CS5) ▼	40 (CS5) ▼
41	41 ▼	<input type="checkbox"/>	41 ▼	41 ▼
42	42 ▼	<input type="checkbox"/>	42 ▼	42 ▼
43	43 ▼	<input type="checkbox"/>	43 ▼	43 ▼
44	44 ▼	<input type="checkbox"/>	44 ▼	44 ▼
45	45 ▼	<input type="checkbox"/>	45 ▼	45 ▼
46 (EF)	46 (EF) ▼	<input type="checkbox"/>	46 (EF) ▼	46 (EF) ▼
47	47 ▼	<input type="checkbox"/>	47 ▼	47 ▼
48 (CS6)	48 (CS6) ▼	<input type="checkbox"/>	48 (CS6) ▼	48 (CS6) ▼
49	49 ▼	<input type="checkbox"/>	49 ▼	49 ▼

50	50	<input type="checkbox"/>	50	50
51	51	<input type="checkbox"/>	51	51
52	52	<input type="checkbox"/>	52	52
53	53	<input type="checkbox"/>	53	53
54	54	<input type="checkbox"/>	54	54
55	55	<input type="checkbox"/>	55	55
56 (CS7)	56 (CS7)	<input type="checkbox"/>	56 (CS7)	56 (CS7)
57	57	<input type="checkbox"/>	57	57
58	58	<input type="checkbox"/>	58	58
59	59	<input type="checkbox"/>	59	59
60	60	<input type="checkbox"/>	60	60
61	61	<input type="checkbox"/>	61	61
62	62	<input type="checkbox"/>	62	62
63	63	<input type="checkbox"/>	63	63

Parameter description:

1. DSCP :

Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

2. 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

3. Translation :

DSCP at Ingress side can be translated to any of (0-63) DSCP values.

4. Classify :

Click to enable Classification at Ingress side.

5. 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.

6. Remap DP0 :

Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

7. Remap DP1 :

Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

Button :

Save – Click to save changes.

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

4.19.9. DSCP-Classification

The section describes to teach user to configure and allows you to map DSCP value to a QoS Class and DPL value. Others the settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the DSCP Classification parameters in the web interface:

1. Click Configuration, QoS, DSCP Classification
2. Scroll to set the DSCP Parameters
3. Click the save to save the setting
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

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)

Save Reset

Parameter description:

1. QoS Class :

Actual QoS class.

2. DPL :

Actual Drop Precedence Level.

3. Classify :

Select the classified DSCP value (0-63).

Button :

Save – Click to save changes.


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

4.19.10. QoS Control List


The section 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.

Web Interface

To configure the QoS Control List parameters in the web interface:

1. Click Configuration, QoS, QoS Control List.
2. Click the to  add a new QoS Control List.
3. Scroll all parameters and evoke the Port Member to join the QCE rules.
4. Click the save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

QoS Control List Configuration

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



QCE Configuration

Port Members							
1	2	3	4	5	6	7	8
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Key Parameters

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

Action Parameters

CoS	0
DPL	Default
DSCP	Default

Parameter description:

1. QCE :

Indicates the QCE id.

2. Port :

Indicates the list of ports configured with the QCE.

3. 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'.

4. SMAC :

Match specific source MAC address or 'Any'.

If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

5. Tag Type :

Select the classified DSCP value (0-63).

6. VID :

Indicates ([VLAN ID](#)), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

7. 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'.

8. DEI :

Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

9. 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.

10. Action :

Actual Drop Precedence Level.

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.


11. Modification :


Select the classified DSCP value (0-63).


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.

Parameter description:**1. Port Members :**

Check the checkbox button to include the port in the QCL entry. By default all ports are included.

2. Key parameters :

Indicates the list of ports configured with the QCE.

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.

3. 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.

Button :

Save – Click to save changes.

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.

4.19.11. Storm Control

The section allows user to configure the Storm control for the switch. 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.

Web Interface

To configure the Storm Control Configuration parameters in the web interface:

1. Click Configuration, QoS, Storm Control Configuration
2. Evoke to select the frame type to enable storm control
3. Scroll to set the Rate Parameters
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

Storm Control Configuration

Frame Type	Enable	Rate (pps)
Unicast	<input type="checkbox"/>	1 ▼
Multicast	<input type="checkbox"/>	1 ▼
Broadcast	<input type="checkbox"/>	1 ▼

Save Reset

Parameter description:

1. Frame Type :

The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.

2. Enable :

Enable or disable the storm control status for the given frame type.

3. 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.**

Button :

Save – Click to save changes.

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

4.20 Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

Web Interface

To configure the Mirror in the web interface:

1. Click Configuration, Mirroring
2. Scroll to select Port to mirror on which port
3. Scroll to disabled, enable, TX Only and RX Only to set the Port mirror mode
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button.
It will revert to previously saved values

Mirror Configuration

Port to mirror to	Disabled ▼
-------------------	------------

Mirror Port Configuration

Port	Mode
*	<> ▼
1	Disabled ▼
2	Disabled ▼
3	Disabled ▼
4	Disabled ▼
5	Disabled ▼
6	Disabled ▼
7	Disabled ▼
8	Disabled ▼
CPU	Disabled ▼

Save	Reset
------	-------

Parameter description:

1. 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.

2. Port :

The logical port for the settings contained in the same row.

3. 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**.

Button :

Save – Click to save changes.

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

4.21 GVRP

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices.

4.21.1. Global config

Web Interface

To configure the Mirror in the web interface:

1. Click Configuration, GVRP, Global config.

GVRP Configuration

Refresh

Enable GVRP

Parameter	Value
Join-time:	20
Leave-time:	60
LeaveAll-time:	1000
Max VLANs:	20

Save

Parameter description:

1. GVRP Protocol timers :

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.

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.

2. Max number of VLANs :

The logical port for the settings contained in the same row.

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.

Button :

Save – Click to save changes.

4.21.2. Port config

Web Interface

To configure the Mirror in the web interface:

1. Click Configuration, GVRP, Port config.

GVRP Port Configuration

Port	Mode
*	<> ▼
1	Disabled ▼
2	Disabled ▼
3	Disabled ▼
4	Disabled ▼
5	Disabled ▼
6	Disabled ▼
7	Disabled ▼
8	Disabled ▼

Save Reset

Parameter description:

1. **Button :**

Save – Click to save changes.

4.22 sFlow

This page allows for configuring sFlow. The configuration is divided into two parts:

Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers. sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.

Web Interface

To configure the GVRP in the web interface:

1. Click Configuration, sFlow.

sFlow Configuration

Agent Configuration

IP Address

Receiver Configuration

Owner	<input type="text" value="<none>"/>	Release
IP Address/Hostname	<input type="text" value="0.0.0.0"/>	
UDP Port	<input type="text" value="6343"/>	
Timeout	<input type="text" value="0"/>	seconds
Max. Datagram Size	<input type="text" value="1400"/>	bytes

Port Configuration

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
1	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
2	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
3	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
4	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
5	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
6	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
7	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
8	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0

Parameter description:

Agent Configuration

1. IP Address :

The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time.

Both IPv4 and IPv6 addresses are supported.

Agent Configuration

1. Owner :

The logical port for the settings contained in the same row.

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.

2. IP Address/Hostname :

The logical port for the settings contained in the same row.

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.

3. UDP Port:

The logical port for the settings contained in the same row.

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.

4. Timeout :

Save – Click to save changes.

5. Max. Datagram Size :

Save – Click to save changes.

Port Configuration

1. Port :

The port number for which the configuration below applies.

2. Flow Sample Enabled :

Enables/disables flow sampling on this port.

3. Flow Sampler Sampling Rate :

The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port.

Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.

4. Flow Sample Max. Header :

Save – Click to save changes.

The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

5. Counter Poller Enabled :

Enables/disables counter polling on this port.

6. Counter Poller Interval :

With counter polling enabled, this specifies the interval - in seconds – between counter poller samples.

Button :

Release – See description under Owner.

Refresh – Click to refresh the page. Note that unsaved changes will be lost.

Save – Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.

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

4.23 RingV2

This page provides Ring related configuration.

Web Interface

To configure the RingV2 in the web interface:

1. Click Configuration, RingV2.

sFlow Configuration

Refresh

Agent Configuration

IP Address

Receiver Configuration

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

Port Configuration

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
1	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
2	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
3	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
4	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
5	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
6	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
7	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
8	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0

Save Reset

Parameter description:

1. Index :

The group index. This parameter is used for easy identifying the ring when user configure it.

Group 1 (Index 1) - It supports configuration of ring.

Group 2 (Index 2) - It supports configuration of ring, coupling and dual-homing.

Group 3 (Index 3) - It supports configuration of chain and balancing-chain.

2. Mode :

Enable Ring on the specific group.

When Group 1 or 2 is enabled, all configuration of Group 3 will be reset to default.

Group 3 all configuration options will be locked.

To configure Group 3, both Group1 and 2 should be disabled first. When Group 3 is enabled, all configuration of Group1 and 2 will be reset to default. Group 1 and 2 all configuration options will be locked.

3. Role :

Configure the Ring group on this switch as specific role.

Group 1 - support option of ring-master and ring-slave.

Ring - it could be master or slave.

Group 2 - support configuration of the ring, coupling and dual-homing.

- # Ring - it could be master or slave.
- # Coupling - it could be primary and backup.
- # Dual-Homing

- Group 3 - support configuration of the chain and balancing-chain.
- # Chain - it could be head, tail or member.
- # Balancing Chain - it could be central-block, terminal-1/2 or member.

Note 1 - Group 1 must be enabled before enable Group 2 to coupling.

Note 2 - When Group 1 or 2 is enabled, the configuration of Group 3 will be disabled.

Note 3 - When Group 3 is enabled, the configuration of Group 1 and 2 will be disabled.

4. Role :

Selecting ring port(s).

Each ring port must be unique, CANNOT be configured in different groups; 2 ring ports between ring/chain 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**.

When role is coupling/primary, only need one ring port named **primary port**.

When role is coupling/backup, only need one ring port named **backup port**.

This backup port is redundant port; it is blocking port in normal state.

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.

When role is chain/head, one ring port is **member port** and another is **head port**.

Both ring ports are forwarding port in normal state.

When role is chain/tail, one ring port is **member port** and another is **tail port**.

The tail port is redundant port; it is blocking port in normal state.

When role is chain/member, both ring ports are **member port**. Both ring ports are forwarding port in normal state.

When role is balancing-chain/central-block, one ring port is **member port** and another is **block port**. The block port is redundant port; it is blocking port in normal state.

When role is balancing-chain/terminal-1/2, one ring port is **member port** and another is **terminal port**. Both ring ports are forwarding port in normal state.

When role is balancing-chain/member, both ring ports are **member port**. Both ring ports are forwarding port in normal state.

Button :

Save – Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.

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

4.24 DDMI

Configure DDMI on this page.

Web Interface

To configure the DDMI in the web interface:

1. Click Configuration, DDMI.

DDMI Configuration

Mode	Enabled ▼
------	-----------

Save	Reset
------	-------

Parameter description:

Mode

1. **Enabled :**

Enable DDMI mode operation.

2. **Disabled :**

Disable DDMI mode operation.

Button :

Save – Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.

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

5

Web Management: Monitor of IGR-842POE

5.1 Sysytem

This chapter describes the entire basic configuration tasks which includes the System Information and any manage of the Switch (e.g. Time, Account, IP, Syslog and NTP.)

5.1.1.Information

You can identify the system by configuring the contact information, name, and location of the switch.

Web Interface

To configure System Information in the web interface:

1. Click Monitor, System and Information.
2. Check the contact information for the system administrator as well as the name and location of the switch. Also indicate the local time zone by configuring the appropriate offset.
3. Click the “Refresh”

System Information

Auto-refresh Refresh

System	
Contact Name	
Location	
Hardware	
MAC Address	00-05-65-73-c5-90
Chip ID	VSC7425
Time	
System Date	2000-01-06T03:04:35+00:00
System Uptime	5d 03:04:37
Software	
Software Version	v00.00.01B07
Software Date	2015-10-13T17:33:32+08:00
Acknowledgments	Details

Parameter description:

1. **Contact :**
Enable DDMI mode operation.
2. **Name :**
Disable DDMI mode operation.
3. **Location :**
Enable DDMI mode operation.
4. **MAC Address :**
Disable DDMI mode operation.

5. Chip ID :

Enable DDMI mode operation.

6. System Date :

Disable DDMI mode operation.

7. System Uptime :

Enable DDMI mode operation.

8. Software Version :

Disable DDMI mode operation.

9. Software Date :

Disable DDMI mode operation.

Button :

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

Refresh – Click to refresh the page.

5.1.2.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.

Web Interface

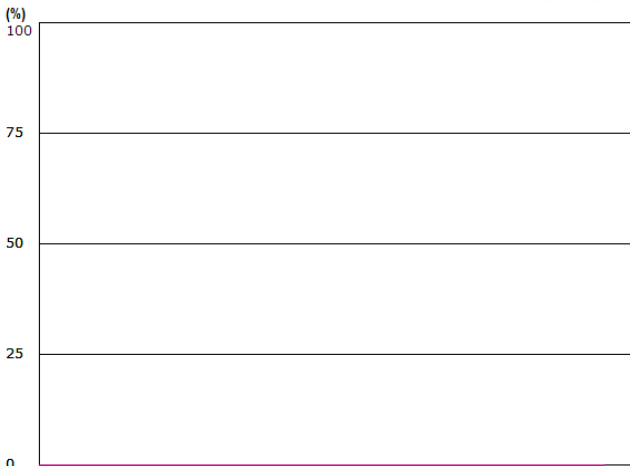
To configure CPU Load in the web interface:

1. Click Monitor, System and CPU load.

CPU Load

Auto-refresh

100ms 0% 1sec 0% 10sec 0% (all numbers running average)



Parameter description:

Button :

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

5.1.3.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.

Web Interface

To configure IP Status in the web interface:

1. Click Monitor, System and IP Status.

IP Interfaces

Auto-refresh Refresh

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	00-05-65-73-c5-90	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.0.2.1/24	
VLAN1	IPv6	fe80:2::205:65ff:fe73:c590/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
192.0.2.0/24	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
192.0.2.88	VLAN1:48-5b-39-4f-4b-9f
fe80:2::205:65ff:fe73:c590	VLAN1:00-05-65-73-c5-90

Parameter description:

IP Interfaces

1. Interface :

The name of the interface.

2. Type :

The address type of the entry. This may be **LINK** or **IPv4**.

3. Address :

The current address of the interface (of the given type).

4. Status :

The status flags of the interface (and/or address).

IP Routers

1. Network :

The destination IP network or host address of this route.

2. Gateway :

The gateway address of this route.

3. Status :

The status flags of the route.

Neighbor cache

1. IP Address :

The IP address of the entry.

2. Link Address :

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

1. Button :

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

Refresh – Click to refresh the page.

5.1.4.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.

Web Interface

To configure log configuration in the web interface:

1. Click Configuration, System and log.

System Log Information

Level	All
Clear Level	All

Auto-refresh Refresh Clear |<< << >> >>|

The total number of entries is 7 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
1	Info	1999-12-31T23:59:59+00:00	Switch just made a cold boot.
2	Info	2000-01-01T00:00:02+00:00	Link up on port 2
3	Info	2000-01-01T00:00:09+00:00	Power alarm occurs
4	Info	2000-01-01T04:38:02+00:00	Link down on port 2
5	Info	2000-01-04T19:37:48+00:00	Link up on port 2
6	Info	2000-01-04T19:38:09+00:00	Link down on port 2
7	Info	2000-01-04T19:38:13+00:00	Link up on port 2

Parameter description:

1. ID :

The identification of the system log entry.

2. 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.

3. Time :

The occurred time of the system log entry.

4. Message :

The detail message of the system log entry.

Button :

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

Refresh – Click to refresh the page.

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.

5.1.5.Detailed Log

The identification of the system log entry.

Web Interface

To configure detailed log configuration in the web interface:

1. Click Configuration, System and detailed log.

Detailed System Log Information



ID

Message

Level	Info
Time	1999-12-31T23:59:59+00:00
Message	Switch just made a cold boot.

Parameter description:

1. ID :

The ID (>= 1) of the system log entry.

2. Message :

The detailed message of the system log entry.

Button :

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

Refresh – Click to refresh the page.

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.

5.1.6.Alarm

Current Alarm is provided on this page

Web Interface

To configure detailed log configuration in the web interface:

1. Click Monitor, System and Alarm.

Alarm Current

Auto-refresh Refresh

Alarm Current		Alarm History
Description	Time	
No entry exists		

Parameter description:

1. **Description :**

Alarm Type Description..

2. **Time :**

Alarm occurrence date time.

Button :

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

Refresh – Click to refresh the page.

5.2 Green Ethernet

5.2.1.Port Power Savings

A set of enhancements to the twisted-pair and backplane Ethernet family of computer networking standards that allow for less power consumption during periods of low data activity. The intention is to reduce power consumption by 50% or more, while retaining full compatibility with existing equipment.^[1] The Institute of Electrical and Electronics Engineers (IEEE), through the IEEE 802.3az task force developed the standard. The first study group had its call for interest in November 2006, and the official standards task force was authorized in May 2007.^[2] The IEEE ratified the final standard in September 2010.^[3] Some companies introduced technology to reduce the power required for Ethernet before the standard was ratified, using the name Green Ethernet.

This page provides the current status for [EEE](#)

Web interface

To configure Green Ethernet in the web interface:

1. Click Monitor, Green Ethernet and Port Power Saving.

Parameter description:**1. Port:**

This is the logical port number for this row.

2. Link:

Shows if the link is up for the port (green = link up, red = link down).

3. EEE:

Shows if **EEE** is enabled for the port (reflects the settings at the Port Power Savings configuration page).

4. LP EEE cap:

Shows if the link partner is **EEE** capable.

5. EEE Savings:

Shows if the system is currently saving power due to **EEE**. When **EEE** is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec.

6. ActiPhy Saving:

Shows if the system is currently saving power due to ActiPhy.

7. PerfectReach Savings:

Shows if the system is currently saving power due to PerfectReach.

Button :

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

Refresh – Click to refresh the page.

5.3 Ports

5.3.1. Ports State

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

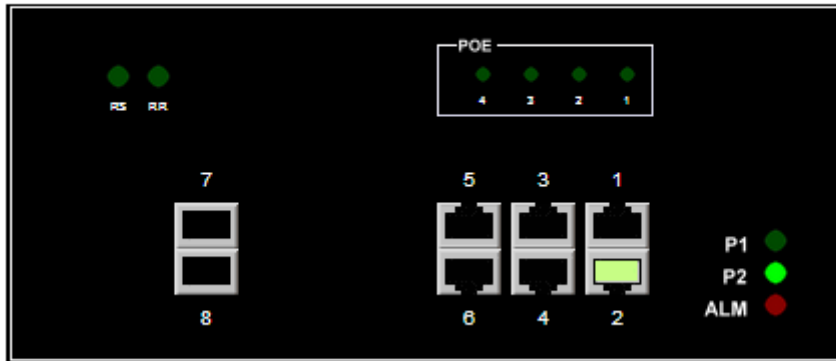
Web interface

To configure Ports in the web interface:

1. Click Monitor, Ports and Port State.

Port State Overview

Auto-refresh Refresh



The port states are illustrated as follows:



Parameter description:

Button :

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

Refresh – Click to refresh the page.

5.3.2. Traffic Overview

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

Web interface

To configure Traffic Overview in the web interface:

1. Click Monitor, Ports and Traffic Overview.

Port Statistics Overview

Auto-refresh Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	17765	54933	2583706	6903409	0	0	0	0	10060
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0

Parameter description:

1. **Port:**

The logical port for the settings contained in the same row.

2. **Packet:**

The number of received and transmitted packets per port.

3. Bytes:

The number of received and transmitted bytes per port.

4. Errors:

The number of frames received in error and the number of incomplete transmissions per port.

5. Drops:

The number of frames discarded due to ingress or egress congestion.

6. Filtered:

The number of received frames filtered by the forwarding process.

Button :

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

Refresh – Click to refresh the page.

Clear – Clears the counters for all ports.

5.3.3.QoS Statistics

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

Web interface

To configure QoS Statistics in the web interface:

1. Click Monitor, Ports and QoS Statistics.

Queuing Counters

Auto-refresh Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	17824	0	0	0	0	0	0	0	0	0	0	0	0	0	0	55015
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Parameter description:

1. Port:

The logical port for the settings contained in the same row.

2. Qn:

There are 8 QoS queues per port. Q0 is the lowest priority queue.

3. Rx/Tx:

The number of received and transmitted packets per queue.

Button :

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

Refresh – Click to refresh the page.

Clear – Clears the counters for all ports.

5.3.4.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.

Web interface

To configure QCL status in the web interface:

1. Click Monitor, Ports and QCL status.

QoS Control List Status

Combined Auto-refresh

User	QCE	Port	Frame Type	Action			Conflict
				CoS	DPL	DSCP	
No entries							

Parameter description:

1. User:

The logical port for the settings contained in the same row.

2. QCE:

There are 8 QoS queues per port. Q0 is the lowest priority queue.

3. Port:

Indicates the list of ports configured with the QCE.

4. 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

5. Action:

The number of received and transmitted packets per queue.

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.

6. 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.

Button :

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.

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

Web interface

To configure Detailed Statistics in the web interface:

1. Click Monitor, Ports and Detailed Statistics.

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		

Parameter description:

Receive Total and Transmit Total

1. Rx and Tx Packets:

The logical port for the settings contained in the same row.

2. Rx and Tx Octets:

There are 8 QoS queues per port. Q0 is the lowest priority queue.

3. Rx and Tx Unicast:

The number of received and transmitted (good and bad) unicast packets.

4. Rx and Tx Multicast:

The number of received and transmitted (good and bad) multicast packets.

5. Rx and Tx Broadcast:

The number of received and transmitted (good and bad) broadcast packets.

6. 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

1. Rx Drops:

The number of frames dropped due to lack of receive buffers or egress congestion.

2. Rx CRC/Alignment:

The number of frames received with CRC or alignment errors.

3. Rx Undersize:

The number of short 1 frames received with valid CRC.

4. Rx Oversize:

The number of long 2 frames received with valid CRC.

5. Rx Fragments:

The number of short 1 frames received with invalid CRC.

6. Rx Jabber:

The number of long 2 frames received with invalid CRC.

7. Rx Filtered:

The number of received frames filtered by the forwarding process.
Short frames are frames that are smaller than 64 bytes.

Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

1. Tx Drops:

The number of frames dropped due to output buffer congestion.

2. Tx Late/Exc. Coll:

The number of frames dropped due to excessive or late collisions.

Button :

Refresh – Click to refresh the page immediately..

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

Clear – Click to refresh the page immediately.

5.4 DHCP

The section describes to configure the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

5.4.1. Sever

5.4.1.1. Statistics

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

Web interface

To configure Detailed Statistics in the web interface:

1. Click Monitor, DHCP, Sever and Statistics.

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

Parameter 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.

2. REQUEST:

Number of DHCP REQUEST messages received.

3. DECLINE:

Number of DHCP DECLINE messages received.

4. RELEASE:

Number of DHCP RELEASE messages received.

5. INFORM:

Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP Message Sent Counters

1. OFFER:

Number of DHCP DISCOVER messages received.

2. ACK:

Number of DHCP REQUEST messages received.

3. NAK:

Number of DHCP DECLINE messages received.

Button :

Refresh – Click to refresh the page immediately..

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

Clear – Click to Clears DHCP Message Received Counters and DHCP Message Sent Counters.

5.4.1.2. Binding

This page displays bindings generated for DHCP clients.

Web interface

To configure Detailed Statistics in the web interface:

1. Click Monitor, DHCP, Sever and Binding.

DHCP Server Binding IP Auto-refresh Refresh Clear Selected Clear Automatic Clear Manual Clear Expired

Binding IP Address

Delete	IP	Type	State	Pool Name	Server ID
--------	----	------	-------	-----------	-----------

Parameter description:

Database Counters

1. IP:

IP address allocated to DHCP client.

2. Type:

Type of binding. Possible types are Automatic, Manual, Expired.

3. State:

State of binding. Possible states are Committed, Allocated, Expired.

4. Pool Name:

The pool that generates the binding.

5. SeverID:

Server IP address to service the binding.

Button :

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 Clears DHCP Message Received Counter

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.

5.4.1.3. Declined IP

This page displays declined IP addresses.

Web interface

To configure Detailed Statistics in the web interface:

1. Click Monitor, DHCP, Sever and Declined IP.

DHCP Server Declined IP

Auto-refresh Refresh

Declined IP Address

Declined IP

Parameter description:

1. Declined IP:

List of IP addresses declined.

Button :

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

Refresh – Click to refresh the page immediately..

5.4.2.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.

Web interface

To configure Detailed Statistics in the web interface:

1. Click Monitor, DHCP, DHCP Snooping Table.

Dynamic DHCP Snooping Table

Start from MAC address , VLAN with entries per page.

Auto-refresh Refresh |<< >>

Parameter description:

1. MAC Address:

User MAC address of the entry.

2. VLAN ID:

VLAN-ID in which the DHCP traffic is permitted.

3. Source Port:

Switch Port Number for which the entries are displayed.

4. IP Address:

User IP address of the entry.

5. IP Subnet Mask:

User IP subnet mask of the entry.

6. DHCP Server Address:

DHCP Server address of the entry.

Button :

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

Refresh – Click to refresh the page immediately..

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.

5.4.3.Relay Statistics

This page provides statistics for DHCP relay.

Web interface

To configure Detailed Statistics in the web interface:

1. Click Monitor, DHCP, DHCP Relay Statistics.

DHCP Relay Statistics

Auto-refresh Refresh Clear

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

Parameter description:

Server Statistics

1. Transmit to Server:

User MAC address of the entry.

2. Transmit Error:

VLAN-ID in which the DHCP traffic is permitted.

3. Receive from Server:

Switch Port Number for which the entries are displayed

4. Receive Missing Agent Option:

The number of packets received without agent information options.

5. Receive Missing Circuit ID:

The number of packets received with the Circuit ID option missing.

6. Receive Missing Remote ID:

The number of packets received with the Remote ID option missing.

7. Receive Bad Circuit ID:

The number of packets whose Circuit ID option did not match known circuit ID.

8. Receive Bad Remote ID:

The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

1. Transmit to Client:

The number of relayed packets from server to client.

2. Transmit Error:

The number of packets that resulted in error while being sent to servers.

3. Receive from Client:

The number of received packets from server.

4. Receive Agent Option:

The number of received packets with relay agent information option.

5. Replace Agent Option:

The number of packets which were replaced with relay agent information option.

6. Keep Agent Option:

The number of packets whose relay agent information was retained.

7. Drop Anget Option:

The number of packets that were dropped which were received with relay agent information.

Button :

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

Refresh – Click to refresh the page immediately..

Clear – Flushes all dynamic entries.

5.4.4.Detailed Statistics

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

Web interface

To configure Detailed Statistics in the web interface:

1. Click Monitor, DHCP, DHCP Detailed Statistics.

Parameter description:**1. Rx and Tx Discover:**

The number of discover (option 53 with value 1) packets received and transmitted.

2. Rx and Tx Offer:

The number of offer (option 53 with value 2) packets received and transmitted.

3. Rx and Tx Request:

The number of request (option 53 with value 3) packets received and transmitted.

4. Rx and Tx Delcine:

The number of decline (option 53 with value 4) packets received and transmitted.

5. Rx and Tx ACK:

The number of ACK (option 53 with value 5) packets received and transmitted.

6. Rx and Tx NAK:

The number of NAK (option 53 with value 6) packets received and transmitted.

7. Rx and Tx Release:

The number of release (option 53 with value 7) packets received and transmitted.

8. Rx and Tx Inform:

The number of inform (option 53 with value 8) packets received and transmitted.

9. Rx and Tx Lease Query:

The number of lease query (option 53 with value 10) packets received and transmitted.

10. Rx and Tx Lease Unassigned:

The number of lease unassigned (option 53 with value 11) packets received and transmitted.

11. Rx and Tx Unknown:

The number of lease unknown (option 53 with value 12) packets received and transmitted.

12. Rx and Tx Active:

The number of lease active (option 53 with value 13) packets received and transmitted.

13. Rx Discarded checksum error:

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

14. Rx Discarded from Untrusted:

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

Button :

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

Refresh – Click to refresh the page immediately..

Clear – Flushes all dynamic entries.

5.5 Security

5.5.1. Access Management Statistics

This page provides statistics for access management.

Web interface

To configure Security in the web interface:

1. Click Monitor, Security, Access Management Statistics.

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

Parameter description:
1. Interface:

The interface type through which the remote host can access the switch.

2. Received Packets:

Number of received packets from the interface when access management mode is enabled.

3. Allowed Packets:

Number of allowed packets from the interface when access management mode is enabled

4. Discarded Packets:

Number of discarded packets from the interface when access management mode is enabled.

Button :

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

Refresh – Click to refresh the page immediately..

Clear – Flushes all dynamic entries.

5.5.2.Network

5.5.2.1.Port Security

5.5.2.1.1. Switch

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

Web interface

To configure Security in the web interface:

1. Click Monitor, Security, Network, Port Security and Switch.

Port Security Switch Status

 Auto-refresh Refresh

User Module Legend

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

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	-	-
2	----	Disabled	-	-
3	----	Disabled	-	-
4	----	Disabled	-	-
5	----	Disabled	-	-
6	----	Disabled	-	-
7	----	Disabled	-	-
8	----	Disabled	-	-

Parameter description:
User Module Legend
1. User Module Name:

The interface type through which the remote host can access the switch.

2. Abbr:

Number of received packets from the interface when access management mode is enabled.

Port Status
1. Port:

The port number for which the status applies. Click the port number to see the status for this particular port.

2. User:

Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security..

3. Status:

Shows the current state of the port. It can take one of four values:

Disabled: No user modules are currently using the Port Security service.

Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page

4. MAC Count(Current, Limit):

The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that

can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Button :

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

Refresh – Click to refresh the page immediately.

5.5.2.1.2. Port

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for softwarebased learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

Web interface

To configure Security in the web interface:

1. Click Monitor, Security, Network, Port Security and Port.

Parameter description:

1. MAC Address & VLAN ID:

The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

2. State:

Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

3. Time of Addition:

Shows the date and time when this MAC address was first seen on the port.

4. Age/Hold:

If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table.

Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Button :

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

Refresh – Click to refresh the page immediately.

5.5.2.2. NAS

5.5.2.2.1. Switch

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

Web interface

To configure Security in the web interface:

1. Click Monitor, Security, Network, NAS and Switch.

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			-	

Parameter description:

1. Port:

The switch port number. Click to navigate to detailed NAS statistics for this port.

2. Admin State:

The port's current administrative state. Refer to NAS Admin State for a description of possible values.

3. Port State:

The current state of the port. Refer to NAS Port State for a description of the individual states.

4. 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.

5. 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.

6. QoS Class:

QoS Class assigned to the port by the RADIUS server if enabled.

7. 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 her.

Button :

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

Refresh – Click to refresh the page immediately.

5.5.2.2.2. 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.

Web interface

To configure Security in the web interface:

1. Click Monitor, Security, Network, NAS and Port.

NAS Statistics Port 1

Port 1 Auto-refresh

Port State

Admin State	Force Authorized
Port State	Globally Disabled

Parameter description:

Port State

1. Admin State:

The port's current administrative state. Refer to NAS Admin State for a description of possible values.

2. Port State:

The current state of the port. Refer to NAS Port State for a description of the individual states.

3. QoS Class:

The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

4. 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

1. 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

2. Backend Server:

These backend (RADIUS) frame counters are available for the following.

3. Counters:

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 her.

4. 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

1. 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

1. 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.

2. 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.

3. VLAN ID:

This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

4. 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.

5. Last Authentication:

Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Button :

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

Refresh – Click to refresh the page immediately.

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

5.5.2.3. 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.

Web interface

To configure Security in the web interface:

1. Click Monitor, Security, Network and ACL Status.

ACL Status Combined Auto-refresh Refresh

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
LLDP	All	EType- 0x88cc	Deny	Disabled	Disabled	Disabled	Yes	No	0	No
RING	All	EType	Deny	Disabled	Disabled	Disabled	Yes	No	0	No

Parameter description:

1. User:

Indicates the ACL user.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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".

8. CPU:

Forward packet that matched the specific ACE to CPU.

9. CPU Once:

Forward first packet that matched the specific ACE to CPU.

10. Counter:

The counter indicates the number of times the ACE was hit by a frame.

11. Conflict:

Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Button :

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

Refresh – Click to refresh the page immediately.

5.5.2.4. ARP Inspection

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

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next Dynamic ARP Inspection 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

Web interface

To configure Security in the web interface:

1. Click Monitor, Security, Network and ARP Inspection.

Dynamic ARP Inspection Table Auto-refresh Refresh |<< >>

Start from Port 1, VLAN 1, MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			

Parameter description:

1. **Port:**
Switch Port Number for which the entries are displayed.
2. **VLAN ID:**
VLAN-ID in which the ARP traffic is permitted.
3. **MAC Address:**
User MAC address of the entry.
4. **Action:**
User IP address of the entry.

Button :

- 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 ARP Inspection Table.
- >>** – **Updates the table, starting with the entry after the last entry currently displayed.**

5.5.2.5. IP Source Guard

Each page shows up to 99 entries from the Dynamic IP Source Guard 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 IP Source Guard Table.

The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the “**Refresh**” button will update the displayed table starting from that or the closest next Dynamic IP Source Guard 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.

Web interface

To configure Security in the web interface:

1. Click Monitor, Security, Network and ARP Inspection.

Dynamic IP Source Guard Table Auto-refresh Refresh |<< >>

Start from , VLAN and IP address with entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

Parameter description:

1. **Port:**
Switch Port Number for which the entries are displayed.
2. **VLAN ID:**
VLAN-ID in which the ARP traffic is permitted.
3. **IP Address:**
User IP address of the entry.
4. **MAC Address:**
Source MAC address.

Button :

- 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** –Flush all dynamic entries.
- |<<** –Update the table starting from the first entry in the Dynamic IP Source Guard Table.
- >>** – Updates the table, starting with the entry after the last entry currently displayed.

5.5.3.AAA

5.5.3.1.RADIUS Overview

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

Web interface

To configure Security in the web interface:

1. Click Monitor, Security, AAA and RADIUS Overview.

RADIUS Authentication Server Status Overview

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

Auto-refresh Refresh

RADIUS Accounting Server Status Overview

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

Parameter description:

RADIUS Authentication Servers

1. **#:**
The RADIUS server number. Click to navigate to detailed statistics for this server..

2. IP Address:

The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

3. 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**1. #:**

The RADIUS server number. Click to navigate to detailed statistics for this server.

2. IP Address:

The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server..

3. 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..

Button :

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.

5.5.3.2.RADIUS Details

This page provides detailed statistics for a particular RADIUS server.

Web interface

To configure Security in the web interface:

1. Click Monitor, Security, AAA and RADIUS Details.

RADIUS Authentication Statistics for Server #1

Server #1 Auto-refresh

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address		0.0.0.0	
State		Disabled	
Round-Trip Time		0 ms	

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address		0.0.0.0	
State		Disabled	
Round-Trip Time		0 ms	

Parameter description:

RADIUS Authentication Statistics

1. Packet Counters:

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

2. Other Info:

This section contains information about the state of the server and the latest roundtrip time.

RADIUS Accounting Statistics

1. Packet Counter:

RADIUS accounting server packet counter. There are five receive and four transmit counters.

2. Other Info:

This section contains information about the state of the server and the latest roundtrip time.

Button :

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 – Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

5.5.4.Switch

5.5.4.1.RMON

5.5.4.1.1. 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.

Web interface

To configure Security in the web interface:

1. Click Monitor, Security, Switch ,RMON and Statistics.

RMON Statistics Status Overview Auto-refresh Refresh |<< >>

Start from Control Index with entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

Parameter description:

1. **ID:**
Indicates the index of Statistics entry.
2. **Data Source(ifIndex):**
The port ID which wants to be monitored.
3. **Drop:**
The total number of events in which packets were dropped by the probe due to lack of resources.
4. **Octets:**
The total number of octets of data (including those in bad packets) received on the network.
5. **Pkts:**
The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
6. **Broad-cast:**
The total number of good packets received that were directed to the broadcast address.
7. **Multi-cast:**
The total number of good packets received that were directed to a multicast address.
8. **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).
9. **Under-Size:**
The total number of packets received that were less than 64 octets.

10. Over-size:

The total number of packets received that were longer than 1518 octets.

11. Frag.:

The number of frames which size is less than 64 octets received with invalid CRC.

12. Jabb.:

The number of frames which size is larger than 64 octets received with invalid CRC.

13. Coll.:

The best estimate of the total number of collisions on this Ethernet segment.

14. 64:

The total number of packets (including bad packets) received that were 64 octets in length.

15. 65~127:

The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

16. 128~255:

The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

17. 256~511:

The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

18. 512~1023:

The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

19. 1024~1588:

The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Button :

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.

5.5.4.1.2. 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.

Web interface

To configure Security in the web interface:

1. Click Monitor, Security, Switch ,RMON and History.

RMON History Overview Auto-refresh Refresh |<< >>

Start from Control Index and Sample Index with entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

Parameter description:

1. History Index:

Indicates the index of History control entry.

2. Sample Index:

Indicates the index of the data entry associated with the control entry.

3. Sample Start:

The value of sysUpTime at the start of the interval over which this sample was measured.

4. Drop:

The total number of events in which packets were dropped by the probe due to lack of resources.

5. Octets:

The total number of octets of data (including those in bad packets) received on the network.

6. Pkts:

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

7. Broadcast:

The total number of good packets received that were directed to the broadcast address.

8. Multicast:

The total number of good packets received that were directed to a multicast address.

9. 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).

10. Undersize:

The total number of packets received that were less than 64 octets.

11. Oversize:

The total number of packets received that were longer than 1518 octets.

12. Frag.:

The number of frames which size is less than 64 octets received with invalid CRC.

13. Jab.:

The number of frames which size is larger than 64 octets received with invalid CRC.

14. Coll.:

The best estimate of the total number of collisions on this Ethernet segment.

15. Utilization:

The total number of packets (including bad packets) received that were 64 octets in length.

Button :

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.

5.5.4.1.3. 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.

Web interface

To configure Security in the web interface:

1. Click Monitor, Security, Switch ,RMON and History.

RMON Alarm Overview Auto-refresh Refresh |<< >>

Start from Control Index with entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

Parameter description:

1. ID:

Indicates the index of Alarm control entry.

2. Interval:

Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

3. Variable:

Indicates the particular variable to be sampled.

- 4. **Sample Type:**
The method of sampling the selected variable and calculating the value to be compared against the thresholds.
- 5. **Value:**
The value of the statistic during the last sampling period.
- 6. **Startup Alarm:**
The alarm that may be sent when this entry is first set to valid.
- 7. **Rising Threshold:**
Rising threshold value.
- 8. **Rising Index:**
Rising event index.
- 9. **Falling Threshold:**
Falling threshold value..
- 10. **Falling Index:**
Falling event index.

Button :

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.

5.5.4.1.4. 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.

Web interface

To configure Security in the web interface:

- 1. Click Monitor, Security, Switch ,RMON and Event.

RMON Event Overview Auto-refresh Refresh |<< >>

Start from Control Index and Sample Index with entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

Parameter description:

- 1. **Event Index:**
I Indicates the index of the event entry.

2. **Log Index:**
Indicates the index of the log entry.
3. **Log Time:**
Indicates Event log time.
4. **LogDescription:**
Indicates the Event description.

Button :

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.

5.6 LACP

5.6.1. System Status

This section describes that when you complete to set LACP function on the switch then it provides a status overview for all LACP instances.

Web interface

To configure LACP in the web interface:

1. Click Monitor, LACP, System.
2. Checked “Auto-refresh”.
3. Click “ Refresh” to refresh the port detailed statistics.

LACP System Status

Auto-refresh Refresh

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

Parameter description:

1. **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'.
2. **Partner System ID:**
Indicates the index of the log entry.
3. **Partner Key:**
The Key that the partner has assigned to this aggregation ID.
4. **Last Changed:**
The time since this aggregation changed.

5. Local Ports:

Shows which ports are a part of this aggregation for this switch.

Button :

Refresh – Click to refresh the page immediately.

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

5.6.2.Port Status

This section describes that when you complete to set LACP function on the switch then it provides a Port Status overview for all LACP instances

Web interface

To configure LACP in the web interface:

1. Click Monitor, LACP, Port Status.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh“ to refresh the LACP Port Status.

LACP Status

Auto-refresh Refresh

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

Parameter description:

1. Port:

The switch port number.

2. 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.

3. Key:

The key assigned to this port. Only ports with the same key can aggregate together.

4. Aggr ID:

The Aggregation ID assigned to this aggregation group.

5. Partner System ID:

The partner's System ID (MAC address).

6. Partner Port:

The partner's port number connected to this port.

7. Partner Prio:

The partner's port priority.

Button :

Refresh – Click to refresh the page immediately.

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

5.6.3.Port Statistics

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

Web interface

To configure LACP in the web interface:

1. Click Monitor, LACP, Port Statistics.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh“ to refresh the LACP Port Statistics.

LACP Statistics

Port	LACP	LACP	Discarded	
	Received	Transmitted	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

Auto-refresh Refresh Clear

Parameter description:

1. Port:

The switch port number.

2. 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.

3. Key:

The key assigned to this port. Only ports with the same key can aggregate together.

4. Aggr ID:

The Aggregation ID assigned to this aggregation group.

Button :

Refresh – Click to refresh the page immediately.

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

Clear –Clears the counters for all ports.

5.7 Loop Protection

The loop Protection is used to detect the presence of traffic. When switch receives packet's (looping detection frame) MAC address the same as oneself from port, show Loop Protection happens. The port will be locked when it received the looping Protection frames. If you want to resume the locked port, please find out the looping path and take off the looping path, then select the resume the locked port and click on "Resume" to turn on the locked ports.

Web interface

To configure Loop Protection in the web interface:

1. Click Monitor, Loop Protection.

Loop Protection Status

Auto-refresh Refresh

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

Parameter description:

1. **Port:**
The switch port number of the logical port.
2. **Action:**
The currently configured port action.
3. **Transmit:**
The currently configured port transmit mode.
4. **Loops:**
The number of loops detected on this port.
5. **Status:**
The current loop protection status of the port.
6. **Loop:**
Whether a loop is currently detected on the port.
7. **Time of Last Loop:**
The time of the last loop event detected.

Button :

Refresh – Click to refresh the page immediately.

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

5.8 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

5.8.1. Bridge Status

After you complete the MSTI Port configuration the you could to ask the switch display the Bridge Status. The Section provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the following information.

Web interface

To configure Spanning Tree in the web interface:

1. Click Monitor, Spanning Tree, Bridge Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the Spanning Tree Bridge Status.

STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-05-65-73-C5-90	32768.00-05-65-73-C5-90	-	0	Steady	-

Auto-refresh Refresh

Parameter description:

1. **MSTI:**
The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
2. **Bridge ID:**
The Bridge ID of this Bridge instance.
3. **Root ID:**
The Bridge ID of the currently elected root bridge.
4. **Root Port:**
The switch port currently assigned the root port role.
5. **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.
6. **Topology Flag:**
The current state of the Topology Change Flag of this Bridge instance.
7. **Topology Change Last:**
The time since last Topology Change occurred.

Button :

Refresh – Click to refresh the page immediately.

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

5.8.2. Port Status

After you complete the STP configuration the you could to ask the switch display the STP Port Status. The Section provides you to ask switch to display the STP CIST port status for physical ports of the currently selected switch.

Web interface

To configure Spanning Tree in the web interface:

1. Click Monitor, Spanning Tree, Bridge Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the Spanning Tree Port Status.

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	DesignatedPort	Forwarding	1d 05:30:54
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-

Auto-refresh Refresh

Parameter description:

1. Port:

The switch port number of the logical STP port.

2. 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**.

3. CIST State:

The current STP port state of the CIST port. The port state can be one of the following values: **Discarding Learning Forwarding**.

4. Uptime:

The time since the bridge port was last initialized.

Button :

Refresh – Click to refresh the page immediately.

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

5.8.3.Port Statistics

After you complete the STP configuration then you could to let the switch display the STP Statistics. The Section provides you to ask switch to display the STP Statistics detail counters of bridge ports in the currently selected switch.

Web interface

To configure Spanning Tree in the web interface:

1. Click Monitor, Spanning Tree, Port Statistics.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the Spanning Tree Port Statistics.

STP Statistics

 Auto-refresh Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
2	100965	0	0	0	0	0	0	0	0	0

Parameter description:

1. Port:

The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

2. MSTP:

The Bridge ID of this Bridge instance.

3. RSTP:

The Bridge ID of the currently elected root bridge.

4. STP:

The switch port currently assigned the root port role.

5. TCN:

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.

6. Discarded Unknown:

The current state of the Topology Change Flag of this Bridge instance.

7. Discarded Illegal:

The time since last Topology Change occurred.

Button :

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.

5.9 MVR

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

5.9.1. Statistics

Web interface

To configure MVR in the web interface:

1. Click Monitor, MVR, Port Statistics.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the MVR Port Statistics.

MVR Statistics

 Auto-refresh Refresh Clear

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
No more entries						

Parameter description:
1. VLAN ID:

The Multicast VLAN ID.

2. IGMP/MLD Queries Received:

The number of Received Queries for IGMP and MLD, respectively.

3. IGMP/MLD Queries Transmitted:

The number of Transmitted Queries for IGMP and MLD, respectively.

4. IGMPv1 Joins Received:

The number of Received IGMPv1 Join's.

5. IGMPv2/MLDv1 Report's Received:

The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

6. IGMPv3/MLDv2 Report's Received:

The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.

7. IGMPv2/MLDv1 Leave's Received:

The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Button :

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 reset the counters.

5.9.2.MVR Channel Groups

Each page shows up to 99 entries from the MVR 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 MVR Channels (Groups) Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. Clicking the **“Refresh”** button will update the displayed table starting from that or the closest next MVR Channels (Groups) 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.

Web interface

To configure MVR in the web interface:

1. Click Monitor, MVR, Channel Groups.

2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the MVR Channel Groups.

MVR Channels (Groups) Information Auto-refresh Refresh |<< >>

Start from VLAN and Group Address :: with entries per page.

VLAN ID	Groups	Port Members							
		1	2	3	4	5	6	7	8
No more entries									

Parameter description:

1. **VLAN ID:**
VLAN ID of the group.
2. **Groups:**
Group ID of the group displayed.
3. **Port Members:**
Ports under this group.

Button :

- 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 MVR Channels (Groups) Information Table.
- >>** –Updates the table, starting with the entry after the last entry currently displayed.

5.9.3.MVR SFM Information

Each page shows up to 99 entries from the MVR 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 MVR SFM Information Table. The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next MVR 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.

Web interface

To configure MVR in the web interface:

1. Click Monitor, MVR, SFM Information.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".

3. Click “Refresh” to refresh the MVR SFM Information.

MVR SFM Information

Auto-refresh Refresh |<< >> 🌐

Start from VLAN and Group Address with entries per page.

Parameter description:

1. VLAN ID:

VLAN ID of the group.

2. Group:

Group address of the group displayed.

3. Port:

Switch port number.

4. Mode:

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

5. Source Address:

IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.

6. Type:

Indicates the Type. It can be either Allow or Deny.

7. Hardware Filter/Switch:

Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

Button :

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 MVR SFM Information Table.

>> –Updates the table, starting with the entry after the last entry currently displayed.

5.10 IPMC

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

5.10.1. IGMP Snooping

The function, is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP

Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before. The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

5.10.1.1. Status

After you complete the IGMP Snooping configuration, then you could to let the switch display the IGMP Snooping Status. The Section provides you to let switch to display the IGMP Snooping detail status.

Web interface

To configure IPMC in the web interface:

1. Click Monitor, IPMC, IGMP Snooping and Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the 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	-

Parameter description:

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

5. Querier Transmitted:

The number of Transmitted Queries.

6. Queries Received:

The number of Received Queries.

7. V1 Report Received:

The number of Received V1 Reports.

8. V2 Report Received:

The number of Received V2 Reports.

9. V3 Report Received:

The number of Received V3 Reports.

10. V2 Leaves Received:

The number of Received V2 Leaves.

11. 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.

12. Port:

Switch port number.

13. Status:

Indicate whether specific port is a router port or not.

Button :

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 reset the counters.

5.10.1.2. Groups Information

After you complete to set the IGMP Snooping function then you could let the switch to display the IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group. 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.

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.

Web interface

To configure IPMC in the web interface:

1. Click Monitor, IPMC, IGMP Snooping and Group Information.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the IGMP Snooping Group Information.

IGMP Snooping Group Information Auto-refresh Refresh |<< >>

Start from VLAN and group address with entries per page.

		Port Members							
VLAN ID	Groups	1	2	3	4	5	6	7	8
No more entries									

Parameter description:

1. VLAN ID:

The VLAN ID of the entry.

2. Querier Version:

Working Querier Version currently.

3. Host Version:

Working Host Version currently.

Button :

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 Group Table.

>> –Updates the table, starting with the entry after the last entry currently displayed.

5.10.1.3. 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.

Web interface

To configure IPMC in the web interface:

1. Click Monitor, IPMC, IGMP Snooping and IPv4 SFM Information.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the IGMP Snooping IPv4 SFM Information.

IGMP SFM Information Auto-refresh Refresh |<< >>

Start from VLAN and Group with entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Parameter description:

1. **VLAN ID:**
VLAN ID of the group.
2. **Group:**
Group address of the group displayed.
3. **Port:**
Switch port number.
4. **Mode:**
Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
5. **Source Address:**
IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
6. **Type:**
Indicates the Type. It can be either Allow or Deny.
7. **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.

Button :

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.

5.10.2. MLD Snooping

5.10.2.1. Status

Web interface

To configure IPMC in the web interface:

1. Click Monitor, IPMC, MLD Snooping and Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the MLD Snooping Status.

MLD 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	V1 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

Parameter description:

1. VLAN ID:

The VLAN ID of the entry.

2. Querier Version:

Working Querier Version currently.

3. Host Version:

Working Host Version currently.

4. Querier Status:

Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

5. Querier Transmitted:

The number of Transmitted Queries.

6. Queries Received:

The number of Received Queries.

7. V1 Report Received:

The number of Received V1 Reports.

8. V2 Report Received:

The number of Received V2 Reports.

9. V1 Leaves Received:

The number of Received V1 Leaves.

10. 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 MLD 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.

11. Port:

Switch port number.

12. Status:

Indicate whether specific port is a router port or not.

Button :

- 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 reset the counters.

5.10.2.2. Groups Information

Each page shows up to 99 entries from the MLD 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 MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the **“Refresh”** button will update the displayed table starting from that or the closest next MLD 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.

Web interface

To configure IPMC in the web interface:

1. Click Monitor, IPMC, MLD Snooping and Group Information.
2. If you want to auto-refresh the information then you need to evoke the **“Auto-refresh”**.
3. Click **“Refresh”** to refresh the MLD Snooping Group Information.

MLD Snooping Group Information Auto-refresh Refresh |<< >>

Start from VLAN and group address with entries per page.

		Port Members							
VLAN ID	Groups	1	2	3	4	5	6	7	8
No more entries									

Parameter description:

1. VLAN ID:

VLAN ID of the group.

2. Groups:

Group address of the group displayed.

3. Port Members:

Ports under this group.

Button :

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 MLD Group Table.

>> –Updates the table, starting with the entry after the last entry currently displayed.

5.10.2.3. IPv6 SFM Information

Each page shows up to 99 entries from the MLD 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 MLD SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD SFM Information Table. Clicking the “**Refresh**” button will update the displayed table starting from that or the closest next MLD 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.

Web interface

To configure IPMC in the web interface:

1. Click Monitor, IPMC, MLD Snooping and IPv6 SFM Information.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the MLD Snooping IPv6 SFM Information.

MLD SFM Information Auto-refresh Refresh |<< >>

Start from VLAN and Group with entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Parameter description:

1. VLAN ID:

VLAN ID of the group.

2. Group:

Group address of the group displayed.

3. Port:

Switch port number.

4. **Mode:**
Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
5. **Source Address:**
IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
6. **Type:**
Indicates the Type. It can be either Allow or Deny.
7. **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.

Button :

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 MLD SFM Information Table.

>> –Updates the table, starting with the entry after the last entry currently displayed.

5.11 LLDP

The switch supports the LLDP. For current information on your switch model, The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document IEEE 802.1AB.

5.11.1. 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. The columns hold the following information.

Web interface

To configure LLDP in the web interface:

1. Click Monitor, LLDP, Neighbors.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the LLDP Neighbors.

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							

Parameter description:

1. Local Port:

The port on which the LLDP frame was received.

2. Chassis ID:

The Chassis ID is the identification of the neighbor's LLDP frames.

3. Port ID:

The Port ID is the identification of the neighbor port.

4. Port Description:

Port Description is the port description advertised by the neighbor unit.

5. System Name:

System Name is the name advertised by the neighbor unit.

6. 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 (-).

7. 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.

Button :

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

Refresh – Click to refresh the page.

5.11.2. LLDP-MED Neighbors

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED.

Web interface

To configure LLDP in the web interface:

1. Click Monitor, LLDP, LLDP-MED neighbors.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the LLDP-MED neighbors.

LLDP Neighbors EEE Information

Auto-refresh Refresh

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
No LLDP EEE information found								

Parameter description:

1. Port:

The port on which the LLDP frame was received.

2. Device Type:

LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device Definition

LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (included for historical reasons)
4. IEEE 802.11 Wireless Access Point
5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA1057 and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

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

LLDP-MED Media Endpoint (Class II)

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

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

LLDP-MED Communication Endpoint (Class III)

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

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

3. LLDP-MED Capabilities:

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

1. LLDP-MED capabilities

2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
5. Extended Power via MDI - PD
6. Inventory
7. Reserved

4. Application Type:

Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.
3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.
5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.
6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.

5. Policy:

Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown

Unknown: The network policy for the specified application type is currently unknown.

Defined: The network policy is defined.

6. TAG:

TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

Tagged: The device is using the IEEE 802.1Q tagged frame format.

7. VLAN ID:

VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

8. Priority:

Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).

9. DSCP:

DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

10. Auto-negotiation:

Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.

11. Auto-negotiation status:

Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

12. Auto-negotiation Capabilities:

Capabilities

Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

Button :

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

Refresh – Click to refresh the page.

5.11.3. EEE

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx "wakeup time", as a way to agree upon the minimum wakeup time they need.

This page provides an overview of EEE information exchanged by LLDP.

Web interface

To configure LLDP in the web interface:

1. Click Monitor, LLDP, EEE.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".

3. Click "Refresh" to refresh the LLDP EEE.

LLDP Neighbors EEE Information

Auto-refresh Refresh

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
No LLDP EEE information found								

Parameter description:

1. Local Port:

The port on which LLDP frames are received or transmitted.

2. Tx Tw:

The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.

3. Rx Tw:

The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.

4. Fallback Receive Tw:

The link partner's fallback receive Tw.

A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

5. Echo Tx Tw:

The link partner's Echo Tx Tw value.

The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

6. Echo Rx Tw:

The link partner's Echo Rx Tw value.

7. Resolved Tx Tw:

The resolved Tx Tw for this link. Note : NOT the link partner.

The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

13. Resolved Rx Tw:

The resolved Rx Tw for this link. Note : NOT the link partner

The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

14. EEE in Sync:

Shows whether the switch and the link partner have agreed on wake times.

Red - Switch and link partner have not agreed on wakeup times.

Green - Switch and link partner have agreed on wakeup times.

Button :

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

Refresh – Click to refresh the page.

5.11.4. Port Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the currently selected switch.

Web interface

To configure LLDP in the web interface:

1. Click Monitor, LLDP, Port Statistics.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh“ to refresh the LLDP Port Statistics.

LLDP Global Counters

Auto-refresh Refresh Clear

Global Counters	
Neighbor entries were last changed	1999-12-31T23:59:58+00:00 (2413354 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	13742	0	0	0	0	0	0	0
2	28839	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

Parameter description:

Global Counters

1. Neighbor entries were last change:

Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

2. Total Neighbors Entries Added:

Shows the number of new entries added since switch reboot.

3. Total Neighbors Entries Deleted:

Shows the number of new entries deleted since switch reboot.

4. Total Neighbors Entries Dropped:

Shows the number of LLDP frames dropped due to the entry table being full.

5. Echo Tx Tw:

Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

1. Local Port:

The link partner's Echo Rx Tw value.

2. Tx Frames:

The resolved Tx Tw for this link. Note : NOT the link partner.

The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

3. Rx Frames:

The number of LLDP frames received on the port.

4. Rx Errors:

The number of received LLDP frames containing some kind of error.

5. Frames Discarded:

If a LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

6. TLVs Discarded:

Shows the number of new entries added since switch reboot.

7. TLVs Unrecognized:

Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

8. Org. Discarded:

If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.

9. Age-Outs:

Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

Button :

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

Refresh – Click to refresh the page.

Clear – Clears the local counters. All counters (including global counters) are cleared upon reboot.

5.12 PoE

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

Web interface

To configure PoE in the web interface:

1. Click Monitor, PoE.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the PoE.

Power Over Ethernet Status

Auto-refresh Refresh

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

Parameter description:

Port Status

1. Local Port:

This is the logical port number for this row.

2. PD Class:

Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class.

Five Classes are defined:

Class 0: Max. power 15.4 W

Class 1: Max. power 4.0 W

Class 2: Max. power 7.0 W

Class 3: Max. power 15.4 W

Class 4: Max. power 30.0 W.

3. Power Requested:

The Power Requested shows the requested amount of power the PD wants to be reserved.

4. Power Allocated:

The Power Allocated shows the amount of power the switch has allocated for the PD.

5. Power Used:

The Power Used shows how much power the PD currently is using.

6. Current Used:

The Power Used shows how much current the PD currently is using.

7. Priority:

The Priority shows the port's priority configured by the user.

8. Port Status:

The Port Status shows the port's status. The status can be one of the following values:

PoE not available - No PoE chip found - PoE not supported for the port.

PoE turned OFF - PoE disabled - PoE is disabled by user.

PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.

No PD detected - No PD detected for the port.

PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down.

PoE turned OFF - PD is off. Invalid PD - PD detected, but is not working correctly.

Button :

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

Refresh – Click to refresh the page.

5.13 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

Web interface

To configure MAC Table in the web interface:

1. Click Monitor, MAC Table.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the MAC Table.

MAC Address Table

 Auto-refresh Refresh Clear |<< >>

 Start from VLAN and MAC address with entries per page.

Type	VLAN	MAC Address	Port Members														
			CPU	1	2	3	4	5	6	7	8						
Static	1	00-05-65-73-C5-90	✓														
Dynamic	1	30-65-EC-2B-2D-D8		✓													
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-73-C5-90	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Parameter description:
1. Switch(stack only):

The stack unit where the entry is learned.

2. Type:

Indicates whether the entry is a static or a dynamic entry.

3. MAC Address:

The MAC address of the entry.

4. VLAN:

The VLAN ID of the entry.

5. Port Members:

The ports that are members of the entry.

Button :

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

Refresh – Click 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

5.14 VLANs

To assign a specific VLAN for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN using the Management VLAN window. Only one management VLAN can be active at a time. When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route

5.14.1. 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.

Web interface

To configure VLANs in the web interface:

1. Click Monitor, VLANs and VLANs Membership.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the VLANs Membership.

Parameter description:




1. 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.

2. VLAN ID:

VLAN ID for which the Port members are displayed.

3. Port Members:

A row of check boxes for each port is displayed for each VLAN ID. If a port is included in a VLAN, the following image will be displayed: . If a port is in the forbidden port list, the following image will be displayed: . If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed: . The port will not be a member of the VLAN in this case.

Button :

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 Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

5.14.2. Port

Web interface

To configure VLANs in the web interface:

1. Click Monitor, VLANs and VLANs Port.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the VLANs Port.

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	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
2	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
3	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
4	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
5	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
6	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
7	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
8	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No

Parameter description:

1. 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.

2. Port:

The logical port for the settings contained in the same row.

3. 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.

4. Ingress Filtering:

Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user..

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

Button :

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.

5.15 VCL

5.15.1. MAC-based VLAN

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently we support following VLAN User types:

CLI/Web/SNMP : These are referred to as static.

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

Web interface

To configure VCL in the web interface:

1. Click Monitor, VCL and MAC-Based VLAN.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the VCL MAC-Based VLAN.

MAC-based VLAN Membership Status for User Static

Static Auto-refresh Refresh

		Port Members							
MAC Address	VLAN ID	1	2	3	4	5	6	7	8
No data exists for the user									

Parameter description:

1. MAC Address:

Indicates the MAC address.

2. VLAN ID:

Indicates the VLAN ID.

3. Port Members:

Port members of the MAC-based VLAN entry.

Button :

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

Refresh – Refreshes the displayed table.

5.16 sFlow

This page shows receiver and per-port sFlow statistics.

Web interface

To configure sFlow in the web interface:

1. Click Monitor, sFlow.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh“ to refresh the sFlow.

sFlow Statistics

Auto-refresh Refresh Clear Receiver Clear Ports

Receiver Statistics

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

Port Statistics

Port	Rx Flow Samples	Tx Flow Samples	Counter Samples
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0

Parameter description:

Receiver Statistics

1. Owner:

This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver..

2. IP Address/Hostname:

The IP address or hostname of the sFlow receiver.

3. **Timeout:**
The number of seconds remaining before sampling stops and the current sFlow owner is released.
4. **Tx Successes:**
The number of UDP datagrams successfully sent to the sFlow receiver.
5. **Tx Errors:**
The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6).
6. **Flow Samples:**
The total number of flow samples sent to the sFlow receiver.
7. **Counter Samples:**
The total number of counter samples sent to the sFlow receiver.

Port Statistics

1. **Port:**
The port number for which the following statistics applies.
2. **Rx and Tx Flow Samples:**
The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.
3. **Counter Samples:**
The total number of counter samples sent to the sFlow receiver originating from this port.

Button :

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

Refresh – Click to refresh the page.

Clear Receiver – Clears the sFlow receiver counters.

Clear Ports –Clears the per-port counters

5.17 RingV2

This page provides a status overview for all of Ring status.

Web interface

To configure RingV2 in the web interface:

1. Click Monitor, RingV2.

2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the RingV2.

RingV2 Group Status

Group index	Mode	State	Role	Ring Port(s)
1	Disable	--	Ring(Slave)	--
2	Disable	--	Ring(Slave)	--
3	Disable	--	Chain(Member)	--

Auto-refresh Refresh

Parameter description:

1. Group Index:

The group index. This parameter is used for easy identifying which ring group.

2. Mode:

It indicates whether the group is enabled.

3. Role:

It indicates group is configured as which role.

4. State:

When ring is complete, it will show "Normal".

When ring is incomplete (at least one link is down), it will show "Fail".

5. Ring Port(s):

Describes current status of ring port(s).

Button :

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

Refresh – Click to refresh the page.

5.18 DDMI

5.18.1. Overview

Display DDMI overview information on this page.

Web interface

To configure DDMI in the web interface:

1. Click Monitor, DDMI and overview.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the DDMI overview.

DDMI Overview

Port	Vendor	Part Number	Serial Number	Revision	Date Code	Transceiver
7	-	-	-	-	-	-
8	-	-	-	-	-	-

Auto-refresh Refresh

Parameter description:

1. **Port:**
DDMI port.
2. **Vendor:**
Indicates Vendor name SFP vendor name.
3. **Part Number:**
Indicates Vendor PN Part number provided by SFP vendor.
4. **Serial Number:**
Indicates Vendor SN Serial number provided by vendor.
5. **Revision:**
Indicates Vendor rev Revision level for part number provided by vendor.
6. **Date Code:**
Indicates Date code Vendor's manufacturing date code.
7. **Transceiver:**
Indicates Transceiver compatibility.

5.18.2. Detailed

Display DDMI detailed information on this page.

Web interface

To configure DDMI in the web interface:

1. Click Monitor, DDMI and detailed.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the DDMI detailed.

Transceiver Information

Port 7 ▾ Auto-refresh Refresh

Vendor	-
Part Number	-
Serial Number	-
Revision	-
Date Code	-
Transceiver	-

DDMI Information

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	-	-	-	-	-
Voltage(V)	-	-	-	-	-
Tx Bias(mA)	-	-	-	-	-
Tx Power(dBm)	-	-	-	-	-
Rx Power(dBm)	-	-	-	-	-

Parameter description:

Transceiver Information

1. **Vendor:**
Indicates Vendor name SFP vendor name.

2. **Part Number:**
Indicates Vendor PN Part number provided by SFP vendor.
3. **Serial Number:**
Indicates Vendor SN Serial number provided by vendor.
4. **Revision:**
Indicates Vendor rev Revision level for part number provided by vendor.
5. **Date Code:**
Indicates Date code Vendor's manufacturing date code..
6. **Transceiver:**
Indicates Transceiver compatibility..

Transceiver Information

1. **Current:**
The current value of temperature, voltage, TX bias, TX power, and RX power.
2. **High Alarm Threshold:**
The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.
3. **High Warn Threshold:**
The high warn threshold value of temperature, voltage, TX bias, TX power, and RX power.
4. **Low Warn Threshold:**
The low warn threshold value of temperature, voltage, TX bias, TX power, and RX power.
5. **Low Alarm Threshold:**
The low alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

Button :

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

Refresh – Click to refresh the page.

6

Web Management: Diagnostics of IGR-842POE

6.1 Ping

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

Web interface

To configure Ping in the web interface:

1. Click Diagnostics, Ping.

ICMP Ping

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

Start

ICMP Ping Output

```

PING server 0.0.0.0, 56 bytes of data.
rcvfrom: Operation timed out
rcvfrom: Operation timed out
rcvfrom: Operation timed out
rcvfrom: Operation timed out
rcvfrom: Operation timed out
Sent 5 packets, received 0 OK, 0 bad
  
```

New Ping

Parameter description:

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

5. 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..

Button :

Start – Click to start transmitting ICMP packets.

New Ping –Click to re-start diagnostics with PING.

6.2 Ping6

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

Web interface

To configure Ping6 in the web interface:

1. Click Diagnostics, Ping6.

ICMPv6 Ping

IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1
Egress Interface	

Start

ICMPv6 Ping Output

```

PING6 server ::, 56 bytes of data.
sendto
sendto
sendto
sendto
sendto
Sent 0 packets, received 0 OK, 0 bad
    
```

New Ping

Parameter description:

1. IP Address:

The destination IP Address.

2. Ping Length:

The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

3. Ping Count:

The count of the ICMP packet. Values range from 1 time to 60 times.

4. Ping Interval:

The interval of the ICMP packet. Values range from 0 second to 30 seconds.

5. 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.

Button :

Start – Click to start transmitting ICMP packets.

New Ping –Click to re-start diagnostics with PING.

6.3 VeriPHY

Press “Start” to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters. 10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Web interface

To configure VeriPHY in the web interface:

1. Click Diagnostics, VeriPHY.

VeriPHY Cable Diagnostics

Port ▾

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--

After pressing “Start” ,following table show up.

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	OK	189	OK	189	Open	0	Open	0
2	OK	3	OK	3	OK	3	OK	3
3	OK	189	OK	189	Open	0	Open	0
4	OK	189	OK	189	OK	189	Open	0
5	OK	189	OK	189	Cross A	48	Open	0
6	OK	189	OK	189	OK	189	Open	0

Parameter description:

1. Port:

The port where you are requesting VeriPHY Cable Diagnostics.

2. Cable Status:

Port: Port number.

Pair: The status of the cable pair.

OK - Correctly terminated pair

Open - Open pair

Short - Shorted pair

Short A - Cross-pair short to pair A

Short B - Cross-pair short to pair B

Short C - Cross-pair short to pair C

Short D - Cross-pair short to pair D

Cross A - Abnormal cross-pair coupling with pair A

Cross B - Abnormal cross-pair coupling with pair B

Cross C - Abnormal cross-pair coupling with pair C

Cross D - Abnormal cross-pair coupling with pair D

Length: The length (in meters) of the cable pair. The resolution is 3 meters.

Button :

Start – Click to run the diagnostics.

7

Web Management: Maintenance of IGR-842POE

7.1 Restart Device

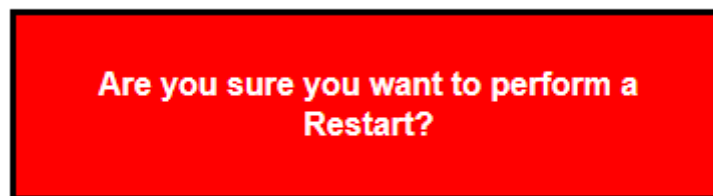
You can restart the switch on this page. After restart, the switch will boot normally.

Web interface

To configure Restart Device in the web interface:

1. Click Maintenance, Restart Device.

Restart Device



Parameter description:

Button :

Yes – Click to restart device.

No – Click to return to the Port State page without restarting.

7.2 Factory Default

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

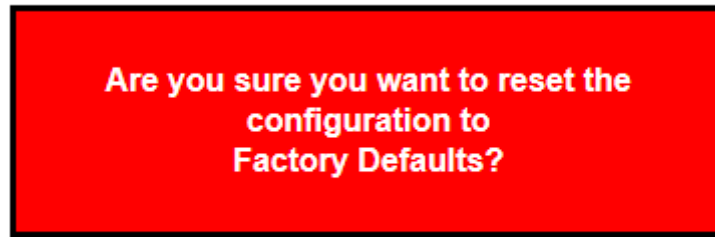
The new configuration is available immediately, which means that no restart is necessary.

Web interface

To configure Factory Default in the web interface:

1. Click Maintenance, Factory Default.

Factory Defaults



Parameter description:

Button :

Yes – Click to restart device.

No – Click to return to the Port State page without restarting.

7.3 Software

7.3.1.Upload

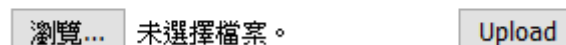
This page facilitates an update of the firmware controlling the switch.

Web interface

To configure Software in the web interface:

1. Click Maintenance, Software and Upload.

Software Upload



Parameter description:

Button :

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.

7.3.2. Image Select

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

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

Note:

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

Web interface

To configure Software in the web interface:

1. Click Maintenance, Software and Image Select.

Software Image Selection

Active Image	
Image	managed
Version	v00.00.01B07
Date	2015-10-13T17:33:32+08:00

Alternate Image	
Image	managed.bk
Version	v00.00.01B07
Date	2015-10-13T17:33:32+08:00

Activate Alternate Image

Cancel

Parameter description:

1. Image :

The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named image.bk.

2. Version :

The version of the firmware image.

3. Data :

The date where the firmware was produced.

Button :

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.

7.4 Configuration

7.4.1. Save startup-config

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

Web interface

To configure Configuration in the web interface:

1. Click Maintenance, Configuration and Save startup-config.

Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Save Configuration

7.4.2. 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.

Web interface

To configure Configuration in the web interface:

1. Click Maintenance, Configuration and Download.

Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
<input type="radio"/> running-config
<input type="radio"/> default-config
<input type="radio"/> startup-config

Download Configuration

7.4.3. 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.

Web interface

To configure Configuration in the web interface:

1. Click Maintenance, Configuration and Upload.

Upload Configuration

File To Upload

未選擇檔案。

Destination File

File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> startup-config	
<input type="radio"/> Create new file	

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

Web interface

To configure Configuration in the web interface:

1. Click Maintenance, Configuration and Activate.

Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will not be saved to startup-config automatically.

File Name
<input type="radio"/> default-config
<input type="radio"/> startup-config

Activate Configuration

7.4.5.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.

Web interface

To configure Configuration in the web interface:

1. Click Maintenance, Configuration and Delete..

Delete Configuration File

Select configuration file to delete.

File Name
<input type="radio"/> startup-config

Delete Configuration File

8

Trouble Shooting

This section is intended to help you solve the most common problems on the IGR-842POE.

8.1 Incorrect Connections

The switch port can auto detect straight or crossover cable when you link switch with other Ethernet device. For the RJ-45 connector should use correct UTP or STP cable, 10/100Mbps port use 2 pairs twisted cable and Gigabit 1000T port use 4 pairs twisted cable. If the RJ-45 connector is not correct pin on right position then the link will fail. For fiber connection, please notice that fiber cable mode and fiber module should be match.

■ Faulty or loose cables

Look for loose or obviously faulty connections. If they appear to be OK, make sure the connections are snug. IF that does not correct the problem, try a different cable.

■ Non-standard cables

Non-standard and miss-wired cables may cause numerous network collisions and other network problem, and can seriously impair network performance. A category 5e-cable tester is a recommended tool for every 1000Base-T network installation.

■ Improper Network Topologies

It is important to make sure that you have a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, you should make sure that your network topology contains no data path loops. Between any two ends nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

8.2 Cabling

RJ-45 ports: use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections or 100Ω Category 5 cable for 100Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet). Gigabit port should use Cat-5 or cat-5e cable for 1000Mbps connections. The length does not exceed 100 meters.

9

Specifications

This section provides the specifications of IGR-842POE, and the following table lists these specifications.

Standard	<ul style="list-style-type: none"> ● IEEE802.3 10BASE-T ● IEEE802.3u 100BASE-TX/100BASE-FX ● IEEE802.3z Gigabit SX/LX ● IEEE802.3ab Gigabit 1000T ● IEEE802.3x Flow Control and Back pressure ● IEEE802.1d Spanning tree protocol ● IEEE802.1w Rapid Spanning tree protocol ● IEEE802.1s Multicast Spanning Tree Protocol ● IEEE802.1p Class of service ● IEEE802.1Q VLAN Tagging ● IEEE802.1ad Double Tagging(Q in Q) ● IEEE802.3 at/af PoE
Interface	<ul style="list-style-type: none"> ● 6 x 10/100/1000Mbp RJ45 ports, ● 2x SFP 100/1000Mbps ports
Switch architecture	<ul style="list-style-type: none"> ● Store and forward switch architecture. ● Back-plane up to 16Gbps
MAC address	<ul style="list-style-type: none"> ● 8K

LED	<ul style="list-style-type: none"> ● Power 1 ● Power 2 ● Alarm ● Link/Act ● POE ● RR/RS
Management	<ul style="list-style-type: none"> ● Web/ SNMP v1,v2c management, ● RFC Standard <ul style="list-style-type: none"> ✓ SNMP agent : MIB-2 (RFC 1213) ✓ Bridge MIB (RFC 1493) ✓ RMON MIB (RFC 1757)-statistics ✓ Ethernet-like MIB (RFC 1643) ✓ Enterprise MIB ● SNMP Trap ● Port Trunk <ul style="list-style-type: none"> ✓ Support IEEE802.3ad with LACP function. ✓ Static aggregation. ● Supports IEEE802.1d STP & IEEE802.1w RSTP & 802.1s MSTP ● VLAN <ul style="list-style-type: none"> ✓ Port-base VLAN ✓ IEEE 802.1Q Tag-base VLAN ✓ Private VLAN Edge (PVE) ✓ Q-in-Q (double tag) VLAN ✓ Voice VLAN ● QoS policy: <ul style="list-style-type: none"> ✓ Support 8 hardware queues ✓ Support WRR , 802.1p/CoS

	<ul style="list-style-type: none"> ✓ Support Port based; 802.1p VLAN Priority based, IPv4/IPv6 precedence/ToS/(DiffServ), Classification and re-marking ACLs, trusted QoS ✓ IPv6 Applications QoS ● Supports IGMP v1/v2 snooping ● Supports IGMP Querier ● Support Port Mirroring ● Supports 802.1x, Radius/TACACS+ ● Support Access Control List
Temperature	<ul style="list-style-type: none"> ● Operating: -40 to 75°C ● Storage: -40 to 85°C
Humidity	<ul style="list-style-type: none"> ● 5% ~ 95%
Power	<ul style="list-style-type: none"> ● 12~58 VDC
PoE Power Budget	<ul style="list-style-type: none"> ● 120W
Dimensions	<ul style="list-style-type: none"> ● 154(W)x 128(H)x 77(D) mm
	<ul style="list-style-type: none"> ●

10

Network Glossary

The network glossary contains explanation or information about common terms used in wireless networking products. Some of information in this glossary might be outdated, please use with caution.

100Base-FX

The IEEE standard defines how to transmit Fast Ethernet 100Mbps data using multi-mode or single fiber optic cable

100Base-TX

Also known as 802.3u. The IEEE standard defines how to transmit Fast Ethernet 100Mbps using Cat.5 UTP/STP cable. The 100Base-TX standard is backward compatible with the 10Mbps 10-BaseT standard.

1000Base-SX

Also known as 802.3z. The IEEE standard defines how to transmit gigabit Ethernet data using multi-mode fiber optic cables. This standard allows transmission distance of 550 meter, which is more than 5 times longer than the 100-meter limitation of 1000Base-T. The 1000Base-SX cannot run in 100Mbps mode.

1000Base-LX

The IEEE standard defines how to transmit gigabit Ethernet data using single mode fiber optic cables. This standard allows transmission distance of 5km or more using single mode fiber. The 1000Base-LX cannot run in 100Mbps mode.

1000Base-T

Also known 802.3ab standard. The IEEE standard defines how to transmit Gigabit data through the use of Cat.5 UTP/STP cable. The 1000Base-T can run in 10/100/1000Mbps speed, and is backward compatible with 10/100Base-TX standard.

802.1d STP

Spanning Tree Protocol. It is an algorithm to prevent network from loop topology. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loop must be avoided because of flooding issue in the network.

802.1Q Tag VLAN

In 802.1Q VLAN, the VLAN information is written into the Ethernet packet itself. Each packet carries a VLAN ID(called Tag) as it traveled across the network. Therefore, the VLAN configuration can be configured across multiple switches. In 802.1Q spec, possible 4096 VLAN ID can be created. Although for some devices, they can only view in frames of 256 ID at a time.

802.1x

802.1x is a security standard for wired and wireless LANs. In the 802.1x parlance, there are usually supplicants (client), authenticator (switch or AP), and authentication server (radius server) in the network. When a supplicants request a service, the authenticator will pass the request and wait for the authentication server to grant access and register accounting. The 802.1x is the most widely used method of authentication by WISP.

802.1w

Rapid Spanning Tree Protocol. It is a refinement of STP, which provides faster spanning tree convergence after a topology change. While STP can take 30 or 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a second.

DHCP

Dynamic Hosting Configuration Protocol. A protocol that enables a server to dynamically assign IP addresses. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned by DHCP server. A DHCP server can either be a designed PC on the network or another network device, such as a router.

Firmware

The program that runs inside embedded device such as AP or Switch. Many network devices are firmware upgradeable through web interface or utility program.

FTP

File Transfer Protocol. A standard protocol for sending files between computer over a TCP/IP network and the internet.

IGMP Snooping

Internet Group Management Protocol. It is a Layer 3 protocol to report IP multicast memberships to neighboring multicast switches and routers. IGMP Snooping is a feature that allows an Ethernet Switch to “listen in” on the IGMP conversation between hosts and routers. When IGMP snooping is enabled in a switch, it prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (IGMP client).

IP Address

IP (Internet Protocol) is a Layer 3 network protocol that is the basis of all Internet communication. An IP address is 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. The new IPv6 specification supports 128-bit IP address format.

LACP (802.3ad) Trunking

Link Aggregation Control Protocol. It is protocol defines how to combine the several Ethernet ports into one high-bandwidth port to increase the transmission speed. It is also known as port trunking. Both devices must set the trunking feature to work.

MAC

Media Access Control. MAC address provides Layer-2 identification for network devices. Each Ethernet device has its own unique address. The first 6 digits are unique for each device manufacturers. When a network device has MAC access control feature, only the devices with the approved MAC address can connect with the network.

Mbps

Megabits Per Second. One million bits per second; a unit of measurement for data transmission.

MiniGBIC

A type of Gigabit Ethernet module interface that uses SFP (Small Form-factor Pluggable) transceiver. The MiniGBIC equipped with Switches typically comes with the MiniGBIC slot for optional SFP optical transceiver.

Packet

A unit of data sent over a network.

Rate Control

It is an Ethernet switch's function to control the upstream and downstream speed of an individual port. Rate control management use "Flow Control" to limit the speed of a port. Therefore, the Ethernet adapter must also have the flow control enabled. One way to force the adapter's flow control on is to set a port to half-duplex mode.

SNMP

Simple Network Management Protocol. A set of protocols for managing complex networks. The SNMP network contains three key elements: managed devices, agents, and network-management system (NMS). Managed devices are network devices that contain SNMP agents. SNMP agents are programs that reside on a device's firmware to provide SNMP configuration service. The NMS typically is PC-based software that can monitor and control managed devices remotely.

Subnet Mask

An address code mask that determines the size of the network. An IP subnet is determined by performing a BIT-wise AND operation between the IP address and the subnet mask. By changing the subnet mask, you can change the scope and size of a network.

TFTP

Trivial File transfer Protocol. A file transfer protocol, with the functionality of a very basic form of FTP. It is used to transfer small amounts of data between hosts on a network, such as Switch firmware.

The switch port can auto detect straight or crossover cable when you link switch with other Ethernet device. For the RJ-45 connector should use correct UTP or STP cable, 10/100Mbps port use 2 pairs twisted cable and Gigabit 1000T port use 4 pairs twisted cable. If the RJ-45 connector is not correct pin on right position then the link will fail. For fiber connection, please notice that fiber cable mode and fiber module should be match.

■ Faulty or loose cables

Look for loose or obviously faulty connections. If they appear to be OK, make sure the connections are snug. If that does not correct the problem, try a different cable.

■ Non-standard cables

Non-standard and miss-wired cables may cause numerous network collisions and other network problem, and can seriously impair network performance. A category 5e-cable tester is a recommended tool for every 100Base-T network installation.

■ Improper Network Topologies

It is important to make sure that you have a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, you should make sure that your network topology contains no data path loops. Between any two ends nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

10.1 Cabling

RJ-45 ports: use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100 Ω Category 3, 4 or 5 cable for 10Mbps connections or 100 Ω Category 5 cable for 100Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet). Gigabit port should use Cat-5 or cat-5e cable for 1000Mbps connections. The length does not exceed 100 meters.