PDS-408G Web Management User Guide

Ver. 1.0.1, 03-2019

Microsemi Headquarters

One Enterprise, Aliso Viejo, CA 92656 USA

Within the USA: +1 (800) 713-4113

Outside the USA: +1 (949) 380-6100

Sales: +1 (949) 380-6136

Fax: +1 (949) 215-4996

Email: sales.support@microsemi.com
www.microsemi.com

Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer's responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided "as is, where is" and with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.

Microsemi, a wholly owned subsidiary of Microchip Technology Inc. (Nasdaq: MCHP), offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, California, and has approximately 4,800 employees globally. Learn more at www microsemi.com

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

The following sections describe the manual objectives, concepts used, conventions used, and associated documentation.

1.1 Objectives

This User Guide introduces Microsemi's PDS-408G 802.3BT PoE 90W IPv4, IPv6 Ethernet Switch Web Management configuration and maintenance interface.

1.2 Abbreviations

IPv4	32-bit long IP address
IPv6	128-bit long IP address
DHCPv4	Dynamic IPv4 Host Configuration Protocol
DHCPv6	Dynamic IPv6 Host Configuration Protocol
PoE	Power over Ethernet
NTP	Network Time Protocol
DES	Data Encryption Standard
AES	Advanced Encryption Standard
MD5	Message Digest algorithm 5
SHA	Secure Hash Algorithm
MDI	Media Dependent Interface
MIB	Management Information Base
PD	Powered Device
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TFTP	Trivial File Transfer Protocol
SysLog	System Log
SSH	Secure Shell
RADIUS	Remote Authentication Dial In User Service
TACACS+	Terminal Access Controller Access-Control System Plus
IGMP	Internet Group Management Protocol

Table 1-1: List of Abbreviations

1.3 Front panel – Quick Overview

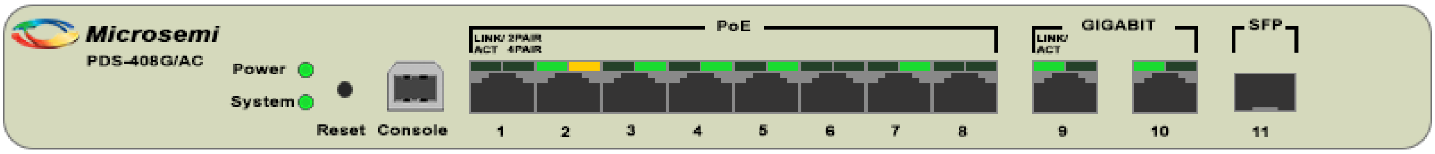


Figure 1-1: Unit front panel

1.4 Reset Button

- Press button for less than 2 seconds and release: Does nothing.
- Press button for 2-10 seconds and release: Reset switch by software (no configuration change).
- Press button for more than 10 seconds and release: Restore unit to **factory default**.

NOTE:

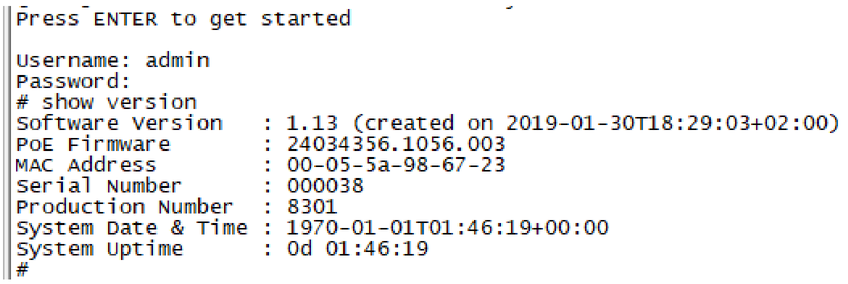
To restore unit to factory default – press and hold the Reset button switch for more than 10 Sec (12 Sec or more) and then release it. Unit will reset itself using factory default configuration

1.5 Power and System LEDs

- Power: Green wheACn -Power is applied to the unit.
- System: Slow 1Hz blinking in green - indicates that the Switch software is OK.

1.6 USB Interface (virtual COMM)

The USB interface should be used for management of serial communication over CLI



```
Press ENTER to get started

Username: admin
Password:
# show version
Software Version       : 1.13 (created on 2019-01-30T18:29:03+02:00)
PoE Firmware           : 24034356.1056.003
MAC Address            : 00-05-5a-98-67-23
Serial Number          : 000038
Production Number      : 8301
System Date & Time     : 1970-01-01T01:46:19+00:00
System Uptime          : 0d 01:46:19
#
```

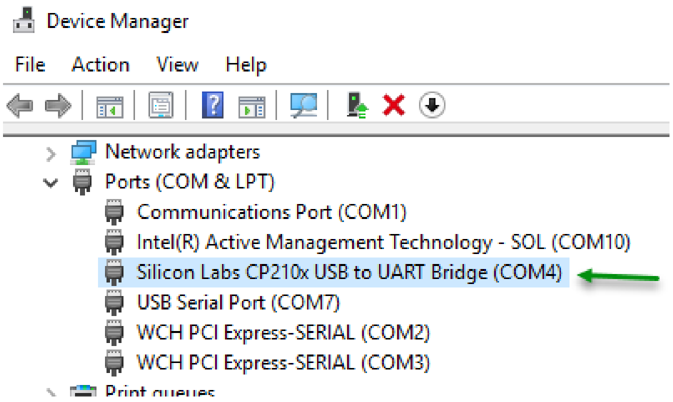
Figure 1-2: CLI interface example

NOTE:

Make sure the USB port is disconnected prior to installing the USB driver.

The unit uses Silicon Labs CP210x USB to UART IC internally. If this is the 1st time you are connecting to the USB interface, then an appropriate USB driver should be installed in advanced before using the USB serial interface. Please use the link bellow to download the most updated drivers: https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers

Next, connect your laptop/desktop USB to the unit's USB interface, and verify that the virtual COMM was successfully added (COM4 in the example below).



- Network adapters
- Ports (COM & LPT)
  - Communications Port (COM1)
  - Intel(R) Active Management Technology - SOL (COM10)
  - Silicon Labs CP210x USB to UART Bridge (COM4)
  - USB Serial Port (COM7)
  - WCH PCI Express-SERIAL (COM2)
  - WCH PCI Express-SERIAL (COM3)
- Print queues

Figure 1-3: Windows 10 ports report

After successful USB to UART driver installation use the following steps to obtain the CLI interface:

- Run the serial communication application as PuTTY https://www.putty.org/
- Select the serial COM index allocated for SiliconLabs CP210x USB to UART driver
- Set Baud rate to 115200
- One Stop bit
- No flow control

1.7 RJ45 Ports 1-8

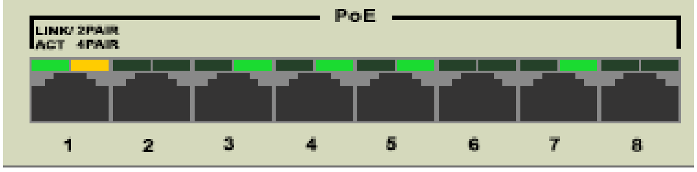


Figure 1-4 : Unit ports 1-8 (out of 11)

- **RJ45** - Gigabit Ethernet, PoE-BT 90Watt capable.
- **Top left green LED** – Ethernet Link + Activity LED.
- **Top right Orange/Green LED** – PoE Power indication.
- Orange = power is delivered over two pair.
- Green = power is delivered over four pair.

1.8 RJ45 Ports 9-10

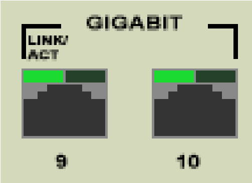


Figure 1-5: Unit ports 9-10 (out of 11)

- **RJ45** - Gigabit Ethernet only (none PoE)
- **Top left green LED** – Ethernet Link + Activity LED.

1.9 SFP Ports 11

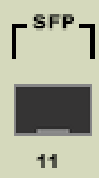


Figure 1-6: Unit port 11 (out of 11)

- **SFP interface** – SFP interface supports the following type of SFP modules
  - 100M/1000M fiber SFP transvers
  - 100M/1000M Copper SFP transvers
  - Single/Multi mode SFP fiber transvers

NOTE:
There is no support for SFP+ transvers

2 MANAGING THE UNIT OVER THE WEB – A GENERAL WALK-THROUGH

This section describes how to manage the new unit or after the unit has been restored to factory default, how to change the unit configuration, save the new unit configuration, etc.

2.1 Default unit IP, username and password.

The unit is shipped with the following default configuration parameters.

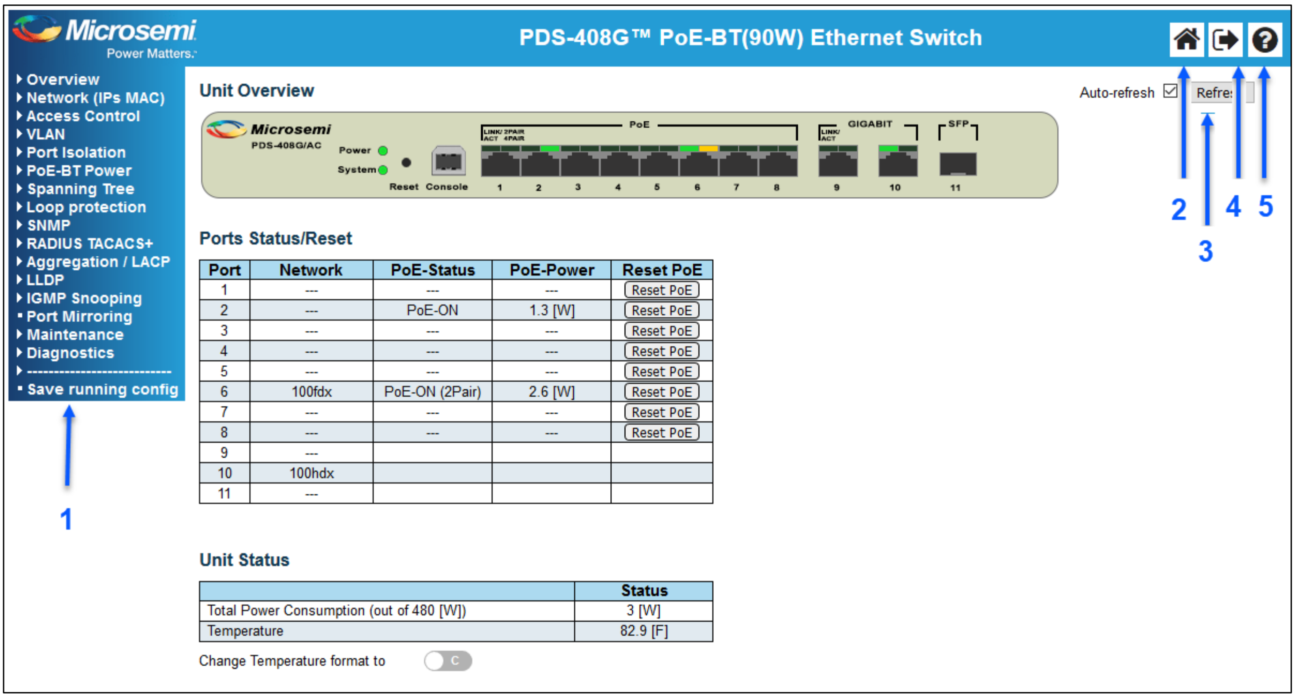
Ports 1-11 VLAN	VLAN1 (access mode).
Default VLAN1 IP Address:	*192.168.0.50*
Default login username is:	*admin*
Default login password:	*blank (no password)*

SNMP - disabled by default due to security concerns. It is recommended to enable SNMP only after changing the SNMP default passwords.

Web – the interface is configured as HTTP. Please change to HTTPS whenever there are security concerns.

2.2 Web interface overview

Page items 1-5 (see below) are always displayed on all web pages regardless of whether the page is accessible to the user. Please note that the refresh button will be presented only on selected web pages.



Ports Status/Reset

Port	Network	PoE-Status	PoE-Power	Reset PoE
1	---	---	---	Reset PoE
2	---	PoE-ON	1.3 [W]	Reset PoE
3	---	---	---	Reset PoE
4	---	---	---	Reset PoE
5	---	---	---	Reset PoE
6	100fdx	PoE-ON (2Pair)	2.6 [W]	Reset PoE
7	---	---	---	Reset PoE
8	---	---	---	Reset PoE
9	---			
10	100hdx			
11	---			

Unit Status

	Status
Total Power Consumption (out of 480 [W])	3 [W]
Temperature	82.9 [F]

Change Temperature format to C

Figure 2-1: Unit overview main Web page

1. The left panel provides an all-switch configuration/view. Each topic includes all sub-pages relevant for this topic. Pressing on the topic title (for example VLAN) will reveal the sub-pages. Pressing on the topic again will hide the sub-pages.
2. The Home icon at the top-right redirects to the main web page as shown in figure 2-1.
3. Pressing on the *Refresh* button will refresh the current page. Please note that the *Refresh* button will only be available on selected web pages.

4. Pressing on the *Logout* button will log the user out of the web session.

NOTE:
Only one help page can be opened at any given time. You must close the opened help web page in order to be able to open a new one.

5. Pressing on the *Help* button will open a new individual help web page.

2.3 Saving configuration changes

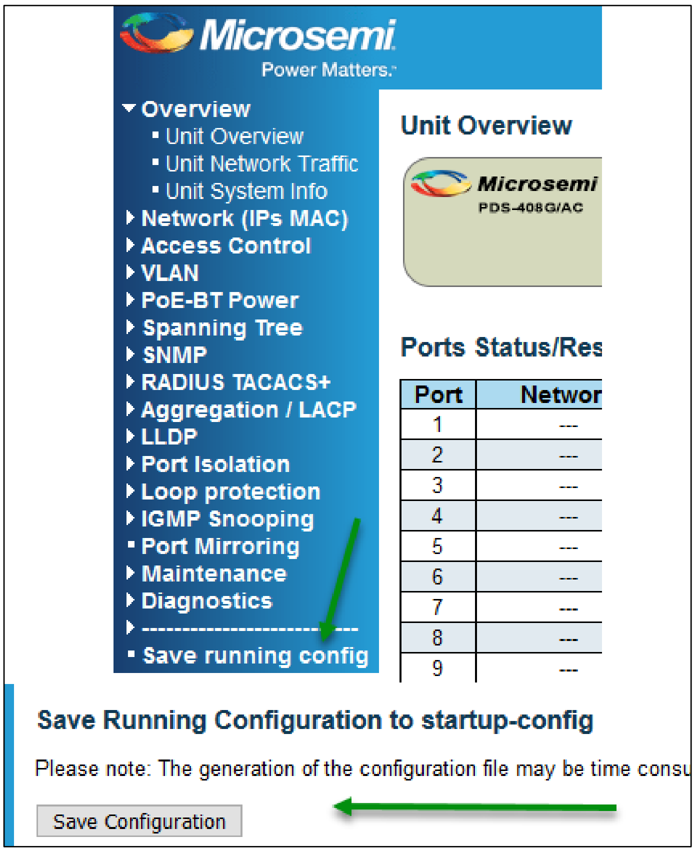
2.3.1 Configuration profiles

The unit has three different configuration profiles. It is important to understand the differences between the three profiles and how to work with each of them. Failing to do so may lead to configuration errors.

- **Running configuration profile** – immediate unit configuration. Any configuration change will take effect immediately, and will be part of the *Running Configuration* profile. Turning the unit off and on or resetting the unit by software will cause the unit to load it's *Startup Configuration*, completely ignoring the unit's *Running Configuration* unless the user copies the *Running-Configuration* to the *Startup-Configuration* before power-off and power-on or the software reset was applied.
- **Startup Configuration profile** – Unit configuration to be used whenever power is applied to the unit, or after each unit software reset.
- **Default Configuration profile** – Unit configuration as it was released from the factory before the user made any changes.

2.3.2 Saving unit configuration over Web and CLI

- **From the Web -** press on *Save running config* followed by pressing on *Save Configuration*.



Unit Overview

Ports Status/Res

Port	Networ
1	---
2	---
3	---
4	---
5	---
6	---
7	---
8	---
9	---

Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consu

Figure 2-2: Save unit configuration

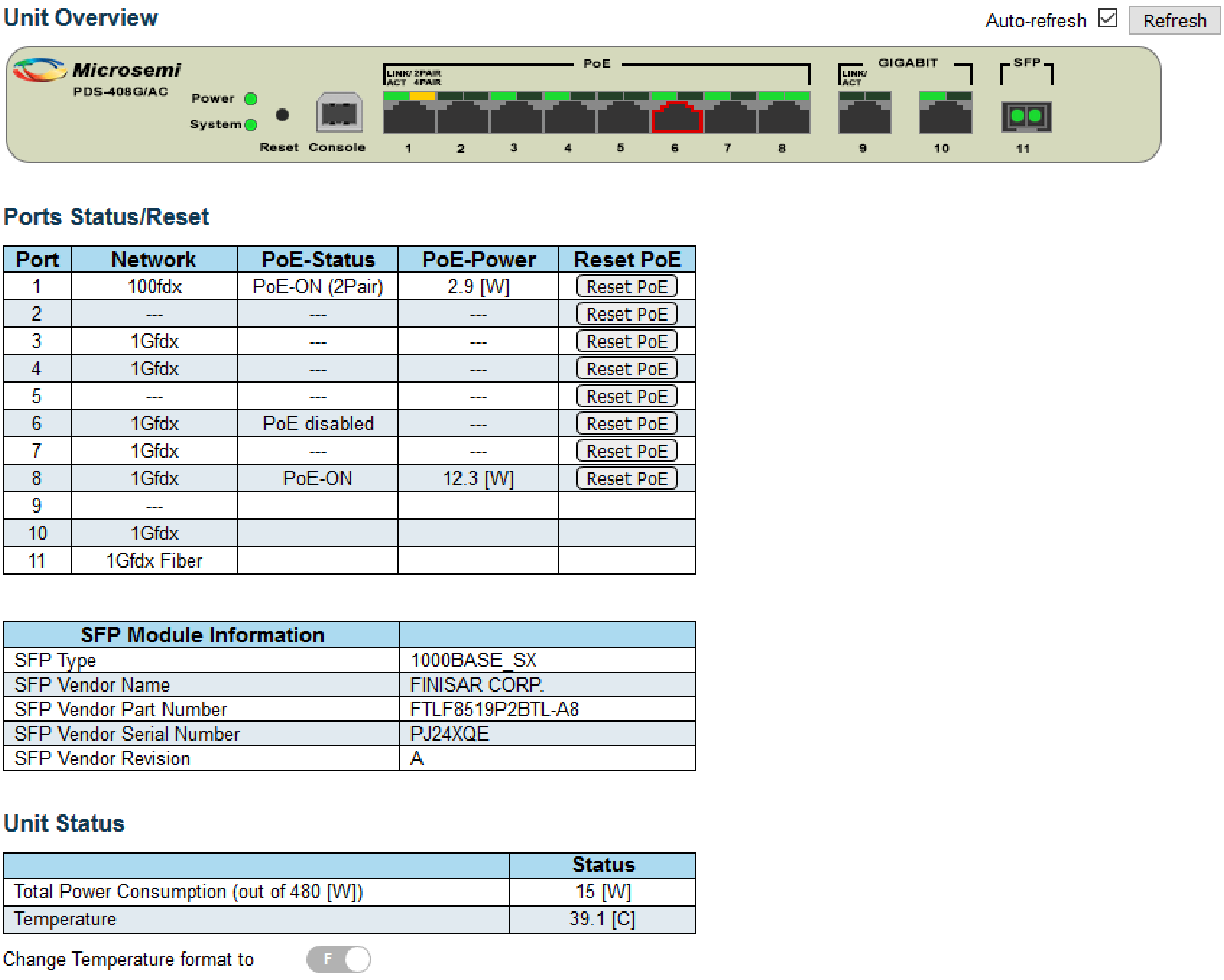
- **From CLI -** type over the USB serial interface/Telnet/SSH: *"copy running-config startup-config"*.

3 OVERVIEW

The web unit overview contains the following subpages:

- **Unit Overview** – Main view page with a graphic display of the network status, PoE status and power consumption per port. Unit total power consumption and unit internal temperature.
- **Unit Network Traffic** – Provides a high-level overview of overall Network traffic per port by reporting the total number of received, transmitted, dropped, error and filtered packets. Pressing on any of the port numbers will open a detailed table page, with much more in-depth traffic statistics for the specific selected port.
- **Unit System Info** – displays system information such as unit software version, PoE firmware version, unit MAC address, serial number, system time and system up time.

3.1 Unit Overview



Unit Overview

Auto-refresh ☑ Refresh

Ports Status/Reset

Port	Network	PoE-Status	PoE-Power	Reset PoE
1	100fdx	PoE-ON (2Pair)	2.9 [W]	Reset PoE
2	---	---	---	Reset PoE
3	1Gfdx	---	---	Reset PoE
4	1Gfdx	---	---	Reset PoE
5	---	---	---	Reset PoE
6	1Gfdx	PoE disabled	---	Reset PoE
7	1Gfdx	---	---	Reset PoE
8	1Gfdx	PoE-ON	12.3 [W]	Reset PoE
9	---			
10	1Gfdx			
11	1Gfdx Fiber			

SFP Module Information	
SFP Type	1000BASE_SX
SFP Vendor Name	FINISAR CORP.
SFP Vendor Part Number	FTLF8519P2BTL-A8
SFP Vendor Serial Number	PJ24XQE
SFP Vendor Revision	A

Unit Status

	Status
Total Power Consumption (out of 480 [W])	15 [W]
Temperature	39.1 [C]

Change Temperature format to F

Figure 3-1: Unit Overview

The Unit Overview page provides a general overview of the unit status regarding network connectivity, PoE power usage, overall PoE power consumption and unit temperature. Hovering with the mouse above the RJ45 connector will display the port network status. Left mouse click on the RJ45 connector will open a detailed port network traffic report page.

3.1.1 RJ45 LEDs and connecter jack

The top left RJ45 green LED **indicate**s that **the network l**ink is up regardless **of l**ink speed. The LED will blink whenever **network** traffic is **passing** through this port.

The top left RJ45 green LED **indicates** PoE status. It can be green, blinking green, orange, **or** off.

- **Green -** POE power is delivered on all four Ethernet cable pairs.
- **Orange -** Power is delivered on only two of the four Ethernet cable pairs.
- **Blinking Green -** there is a PoE problem
- **Off -** PoE power is not delivered to the end **network** device.

NOTE:
The left network LED and the right PoE LED are working independently. Each of them can be turned On and Off regardless of the status of the other LED.

The tables bellow summarize al the LED combinations used to indicate network status, PoE status, network configuration and PoE configuration

Link LED (left)	🟩	⬛		
State	Link-up (1000/100/10)	Link down or disabled		
PoE LED (right)	🟩	🟧	⬛	(blink) 🟩
State	Powering on all 4-pair	Powering on only 2-pair	Disabled or no PD	PoE Error (short, overload, etc.)

Table 3-1: RJ45 LEDs indicating Ethernet link and PoE power status

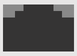
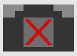
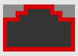
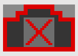
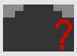
RJ45 image					
State	Link enabled PoE enabled	Link disabled PoE enabled	Link enabled PoE disabled	Link disabled PoE disabled	Link enabled PoE unknown

Table 3-2: RJ45 jack images of Ethernet link and PoE power status

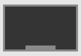
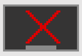
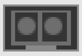
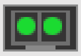
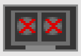
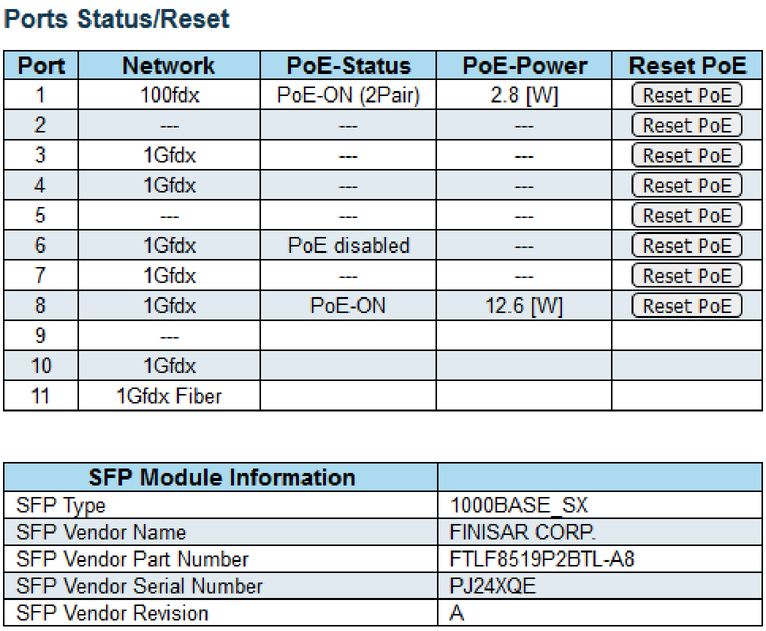
SFP image					
State	No SFP Link enabled	No SFP 8 Link disabled	SFP inserted Link down	SFP inserted Link up	SFP inserted Link disabled

Table 3-3: SFP jack images of both Ethernet link and link status.

NOTE:
Some SFP modules may fail to report as being inserted whenever their Link is Down (applicable to state: SFP-Inserted, Link-Down/Disabled).

3.1.2 Ports Status/Reset

This dynamically updated table display the following for every port: network connection status and speed, PoE power status (only for ports 1-8), PoE power consumption. It also provides an option to reset the PoE device by turning the PoE power off for a few seconds followed by turning it back on.



Ports Status/Reset

Port	Network	PoE-Status	PoE-Power	Reset PoE
1	100fdx	PoE-ON (2Pair)	2.8 [W]	Reset PoE
2	---	---	---	Reset PoE
3	1Gfdx	---	---	Reset PoE
4	1Gfdx	---	---	Reset PoE
5	---	---	---	Reset PoE
6	1Gfdx	PoE disabled	---	Reset PoE
7	1Gfdx	---	---	Reset PoE
8	1Gfdx	PoE-ON	12.6 [W]	Reset PoE
9	---			
10	1Gfdx			
11	1Gfdx Fiber			

SFP Module Information	
SFP Type	1000BASE_SX
SFP Vendor Name	FINISAR CORP.
SFP Vendor Part Number	FTLF8519P2BTL-A8
SFP Vendor Serial Number	PJ24XQE
SFP Vendor Revision	A

Figure 3-2: Unit Overview

NOTE:
The SFP Module information table section will appear only whenever the SFP module is reported as inserted.

Network – The following network status displays are available:

network Status	Description
Disabled	Ethernet port is disabled (regardless if PoE is enabled/disabled)
---	Ethernet port is enabled and link is down
10Mbs HDX	Ethernet port is enabled, link is up, half duplex, 10Mbit/seconds
10Mbs FDX	Ethernet port is enabled, link is up, full duplex, 10Mbit/seconds
100Mbs HDX	Ethernet port is enabled, link is up, half duplex, 100Mbit/seconds
100Mbs FDX	Ethernet port is enabled, link is up, full duplex, 100Mbit/seconds
1Gbps FDX	Ethernet port is enabled, link is up, full duplex, 1000Mbit/seconds

Table 3-4: network S

PoE Status – The following PoE status indications are available:

PoE Status	Description
---	PoE is enabled, and no PD was detected.
PoE Disabled	PoE port was disabled (regardless if Ethernet port is enabled/disabled)
PoE-ON	PoE power is being delivered on all four pairs of the Ethernet cable.
PoE-ON (2Pair)	PoE power is delivered only on two out of four pairs of the Ethenet cable.
PoE-OFF-fault	PoE-Power is not delivered to the connected PoE-PD device due to one of the following reasons: • PD-Overload: The PoE-PD had requested or consumed more power than what the port could deliver, so it was turned off. • Power-Overload: Overall total power including new PD power request exceeds the maximum unit overall power capabilities. • PD-Underload: PD device power consumption is to low (less then 10mA), so power was turned off (endless On On/Off cycle).

Table 3-5: PoE Status

PoE Power – This column displays the PoE PD device ongoing power consumption in Watt. The PoE PD device may consume up to 90[W].

NOTE:

NOTE1 - The maximum power that a PoE PD may consume is determined by its PD class signature:

- **Class-8 = 90[W]**
- **Class-7 = 75[W]**
- **Class-6 = 60[W]**
- **Class-5 = 45[W]**
- **Class-4 = 30[W]**
- **Class-3 = 15[W]**
- **Class-2 = 7[W]**
- **Class-1 = 4[W],**
- **Class-0 = same as Class-3 = 15[W]**

NOTE2 - PoE PD signature can be found on *View PoE-BT Power page.*

NOTE3 – PoE configuration has the option to deliver slightly higher power values for each class then those noted above.

Reset PoE – This column allows you to reset any PoE PD device by temporary shutting down its power (PoE disabled) for around 5-8 seconds, followed by restoring POE power (PoE Enabled).

NOTE:

Pressing on Reset PoE will open a dialog box reporting that PoE power will be turned Off and back to On, allowing the user to cancel this action.

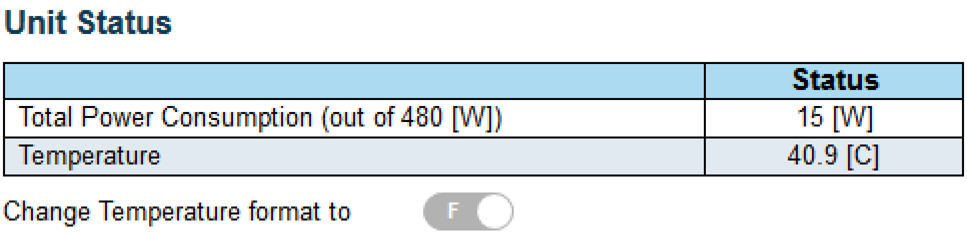
SFP Module Information – SFP related table will appear only when SFP is detected, and will disappear whenever SFP is not detected. The following SFP information will be reported:

SFP Module Information	Example	Comments
SFP Type	1000BASE_SX	100/1000M, single/multi-mode SFP type
SFP Vendor Name	FINISAR CORP.	
SFP Vendor Part Number	FTLF8519P2BTL-A8	
SFP Vendor Part Number	PJ24XQE	
SFP Vendor Revision	PJ24XQE	

Table 3-6: SFP Module Information

3.1.3 Unit Status

The unit status dynamically updated table displays the overall power consumed by all PoE PD devices, and unit internal temperature. The temperature has the option to be displayed in Celsius or Fahrenheit.



Unit Status

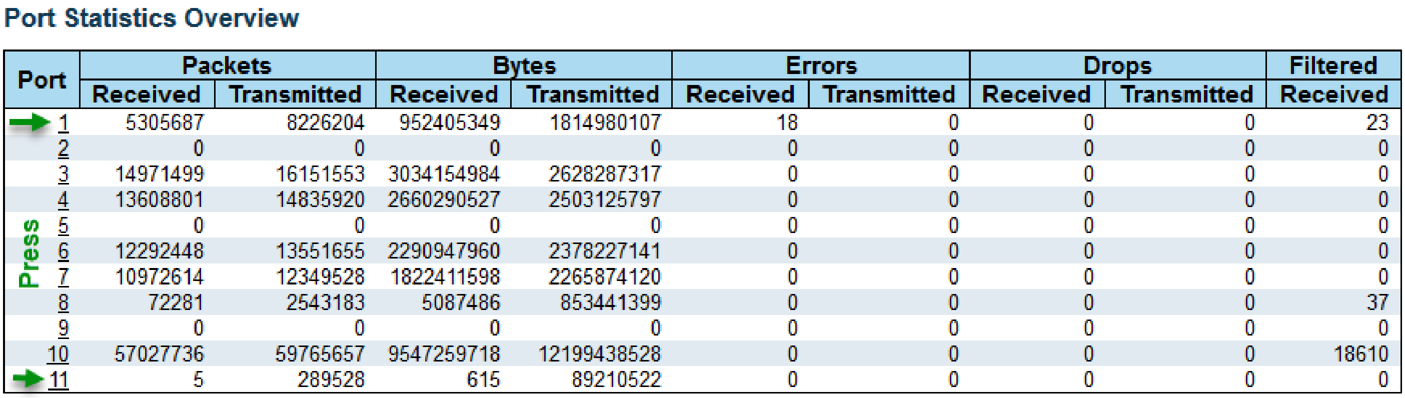
	Status
Total Power Consumption (out of 480 [W])	15 [W]
Temperature	40.9 [C]

Change Temperature format to F

Figure 3-3: Unit Status

3.2 Unit network Traffic Overview

Unit network Traffic page provides an overview for the entire traffic pass through the Switch various Ethernet ports. In addition, pressing on any of the port numbers 1-11 will reveal an in-depth report for the selected port.



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	5305687	8226204	952405349	1814980107	18	0	0	0	23
2	0	0	0	0	0	0	0	0	0
3	14971499	16151553	3034154984	2628287317	0	0	0	0	0
4	13608801	14835920	2660290527	2503125797	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	12292448	13551655	2290947960	2378227141	0	0	0	0	0
7	10972614	12349528	1822411598	2265874120	0	0	0	0	0
8	72281	2543183	5087486	853441399	0	0	0	0	37
9	0	0	0	0	0	0	0	0	0
10	57027736	59765657	9547259718	12199438528	0	0	0	0	18610
11	5	289528	615	89210522	0	0	0	0	0

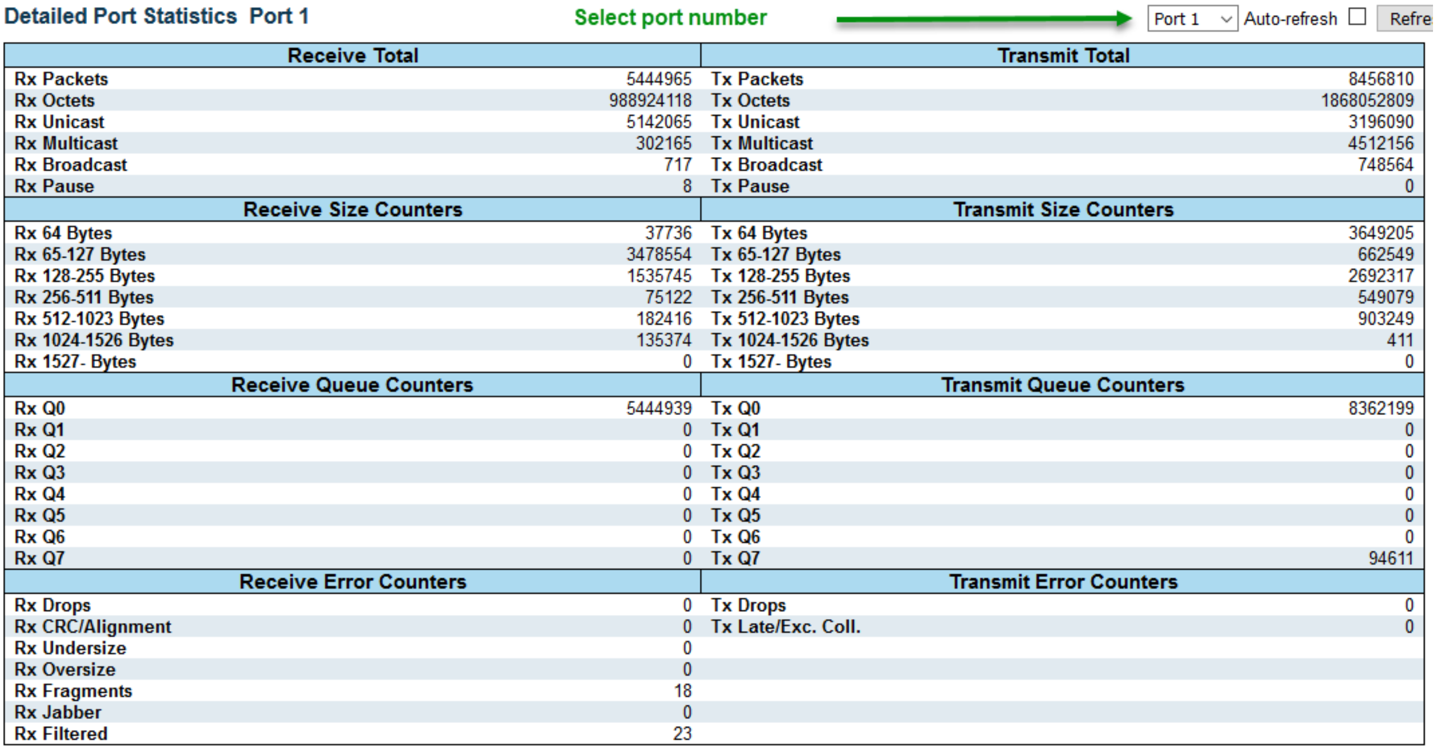
Figure 3-4: Port Statistics Overview

3.2.1 Port Statistics Overview

Port Statistics Overview - displays incremental counters for the number of received, transmitted, errors, drops and filtered packets for each one of the eleven ports.

3.2.2 Detailed Port Statistics

Detailed Port Statistics displays in-depth information on how packets were received or transmitted from the selected port. Please note that you can switch to another in-depth port report by using the drop-down port list on the top right.



Detailed Port Statistics Port 1

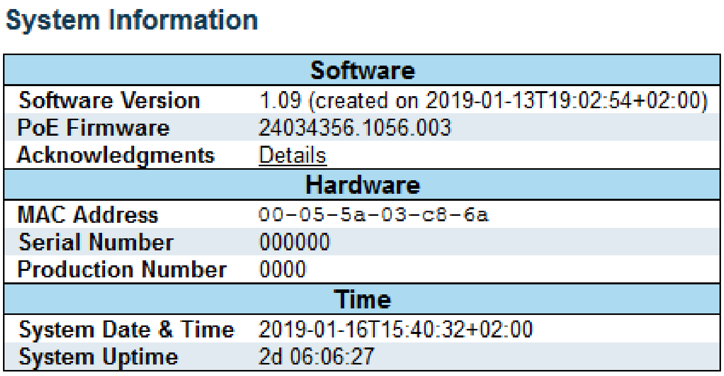
Port 1 Auto-refresh □ Refre

Receive Total		Transmit Total	
Rx Packets	5444965	Tx Packets	8456810
Rx Octets	988924118	Tx Octets	1868052809
Rx Unicast	5142065	Tx Unicast	3196090
Rx Multicast	302165	Tx Multicast	4512156
Rx Broadcast	717	Tx Broadcast	748564
Rx Pause	8	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	37736	Tx 64 Bytes	3649205
Rx 65-127 Bytes	3478554	Tx 65-127 Bytes	662549
Rx 128-255 Bytes	1535745	Tx 128-255 Bytes	2692317
Rx 256-511 Bytes	75122	Tx 256-511 Bytes	549079
Rx 512-1023 Bytes	182416	Tx 512-1023 Bytes	903249
Rx 1024-1526 Bytes	135374	Tx 1024-1526 Bytes	411
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	5444939	Tx Q0	8362199
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	94611
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	18		
Rx Jabber	0		
Rx Filtered	23		

Figure 3-5: Port Statistics Overview

3.3 Overview – Unit System Information

The unit system information page displays the unit software version, PoE-Firmware version, unit MAC, unit serial number and part number for internal use. It also displays the total time the unit has been operational from last power up or software reset, unit system time and details on various Linux packages that are part of the software making it all work.



System Information

Software	
Software Version	1.09 (created on 2019-01-13T19:02:54+02:00)
PoE Firmware	24034356.1056.003
Acknowledgments	Details
Hardware	
MAC Address	00-05-5a-03-c8-6a
Serial Number	000000
Production Number	0000
Time	
System Date & Time	2019-01-16T15:40:32+02:00
System Uptime	2d 06:06:27

Figure 3-6: System Information

4 NETWORK (IPS MAC)

The network (IPs MAC) topic combines multiple configuration pages, each related to its own specific feature, plus a collection of view pages providing dynamic information on the configured features.

The following network configuration subpages are available:

Configuration topic	Description
Ethernet ports	configure Link speed, max packet size, flow control, and view link status (up/down/speed).
IPv4/6	configure static/dynamic IPv4,IPv6 address and mask, default gateway, DNS.
NTP	configure NTP Server IP address, Enable/Disable NTP Server
Time Zone	configure time zone and daylight-saving time
SysLog Report	configure syslog server and from what SysLog level to send SysLog messages.
MAC Table learning	configure MAC address learning and aging algorithms.

Table 4-1: network - Configuration sub pages

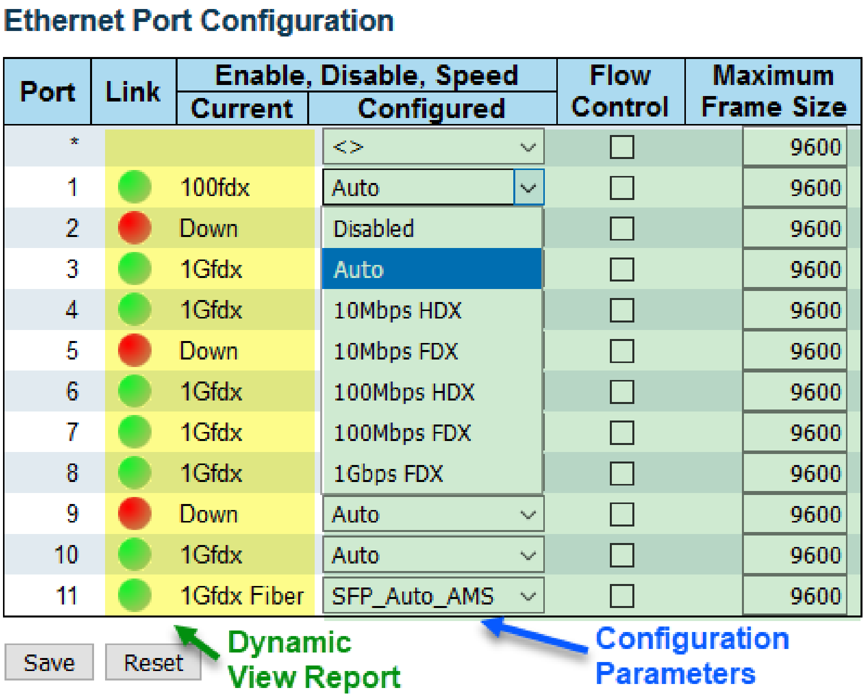
The following network view subpages are available:

Configuration topic	Description
MAC Table in use	Report static and dynamic MAC address learned by the Switch, and from which Ethernet port
IP Status	Summary of all the IPv4, IPv6 address in use
Routing Info	Summary of all route entries in use

Table 4-2: network - View sub pages

4.1 Network - Configuration - Ethernet Ports

This page allows the user to configure how each of the Ethernet Switch ports should operate on the Ethernet physical level. In addition, it displays the actual port Link status and speed.



Ethernet Port Configuration

Port	Link	Enable, Disable, Speed		Flow Control	Maximum Frame Size
		Current	Configured		
*			<>	□	9600
1	🟢	100fdx	Auto	□	9600
2	🔴	Down	Disabled	□	9600
3	🟢	1Gfdx	Auto	□	9600
4	🟢	1Gfdx	10Mbps HDX	□	9600
5	🔴	Down	10Mbps FDX	□	9600
6	🟢	1Gfdx	100Mbps HDX	□	9600
7	🟢	1Gfdx	100Mbps FDX	□	9600
8	🟢	1Gfdx	1Gbps FDX	□	9600
9	🔴	Down	Auto	□	9600
10	🟢	1Gfdx	Auto	□	9600
11	🟢	1Gfdx Fiber	SFP_Auto_AMS	□	9600

Dynamic View Report

Configuration Parameters

Figure 4-1: Ethernet Port Configuration

Item	View/ Configure	Description
Link	View	Green = Ethernet Link On, Red = Ethernet Link Off
Current	View	The actual Ethernet Link speed (10/100/1000M) and is it half/full duplex.
Configured	Configure	Enable/Disable Ethernet port. • Copper ports 1-10 - When enabled, set port speed to Auto or limit its speed to specific speed rate. Also set port to Half/Full duplex mode (applicable only for 10/100M). • SFP port #11 – Enable/Disable SFP port. When enabled, set its SFP mode to Auto/1000M/100M.
Flow Control	Configure	Applicable only for Auto mode. Enable/Disable from the port to send 802.3x pause frames to signal to the other network device to slow down its traffic rate momentarily in order to avoid reception packet loss.
Maximum Frame Size	Configure	Set the maximum supported Ethernet frame size (including FCS). Possible values range from 1518-9600.

Table 4-3: Ethernet port Configuration/View options

4.2 Network - Configuration – Ipv4/6

This page allows you to configure the IP address of DNS Servers, or how the Switch should obtain such DNS IP address over DHCPv4/6 and from which VLAN.

4.2.1 DNS Servers

Multiple DNS Servers can be configured with the following options:

DNS configuration option	Description
No DNS Server	No DNS server – Only numeric IP address services should be used (as SysLog, etc).
Configured IPv4 or IPv6	IPv4 or IPv6 Server address, except Link-Local. For example, 192.168.0.1 or 1234::1
From any DHCPv4 VLANS-ID	The first DNS server offered from a DHCPv4-enabled interface.
From this DHCPv4 VLANS-ID	DNS server offered from a DHCPv4-enabled interface over specific VLAN-ID.
From any DHCPv6 VLANS-ID	The first DNS server offered from a DHCPv6-enabled interface.
From this DHCPv6 VLANS-ID	DNS server offered from a DHCPv6-enabled interface over specific VLAN-ID.

Table 4-4: DNS Server Configuration options

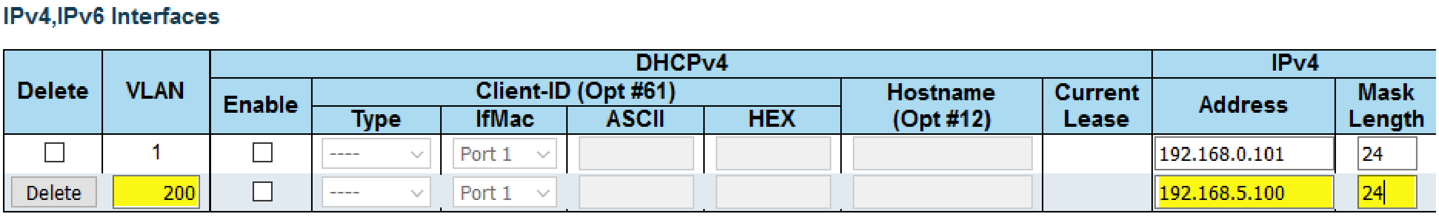
4.2.2 IPv4 / IPv6 Interfaces

IP address configuration can be done for every VLAN-ID in use. The configured IP address for each VLAN-ID can be from type IPv4, IPv6 or both. IPv4 address and IPv6 address can be configured as static or dynamic from type DHCPv4, DHCPv6.

4.2.2.1 Static IPv4 Address Configuration

Whenever configuring static IPv4 address (DHCPv4 checkbox is unchecked), all irrelevant DHCPv4 fields will become gray and unwritable. You only need to configure VLAN-ID, IPv4 address, and IPv4 mask length (for example 24 is equivalent to 255.255.255.0)

NOTE:
To delete an IP address raw, select the *Delete* checkbox and press *Save*



IPv4,IPv6 Interfaces

Delete	VLAN	DHCPv4							IPv4	
		Enable	Client-ID (Opt #61)				Hostname (Opt #12)	Current Lease	Address	Mask Length
			Type	IfMac	ASCII	HEX				
□	1	□	----	Port 1					192.168.0.101	24
Delete	200	□	----	Port 1					192.168.5.100	24

Figure 4-2: Static IPv4 Address Configuration.

4.2.2.2 Dynamic DHCPv4 IPv4 Address Configuration

For IPv4 dynamic DHCP IP address configuration, you need to configure the following:

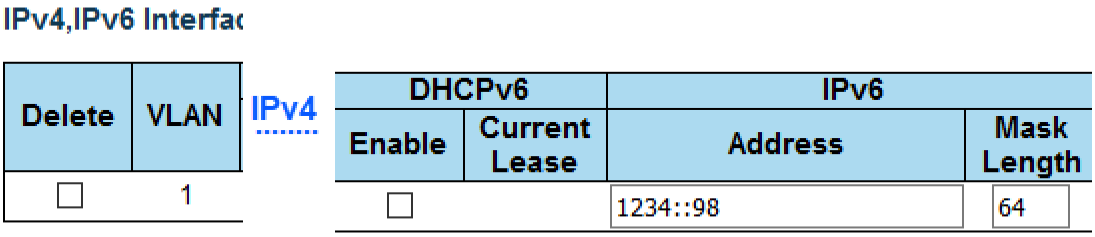
DHCPv4 Parameter	Description
Enable	Enable/Disable DHCPv4. **NOTE:** **Enabling DHCPv4 removes static IPv4 address configuration, which means that whenever DHCPv4 is disabled, the user must reconfigure IPv4 static address.**
Client-ID (opt#61)	DHCPv4 – Client-ID (opt#61) has three configuration options: IF-MAC: DHCPv4 client will use unit MAC address + port index as option #61 ASCII: Text string HEX: Hexadecimal number
Hostname (opt#12)	Text string

Table 4-5: DNS Server Configuration options

NOTE:
DHCPv4 dynamically obtained IPv4 address will be displayed on the Current Lease column.

4.2.2.3 Static/Dynamic DHCPv6 Address Configuration

- **Static IPv6 address** – Configure IPv6 address and IPv6 mask (prefix)
- **DHCPv6 address** – Enable DHCPv6 checkbox.



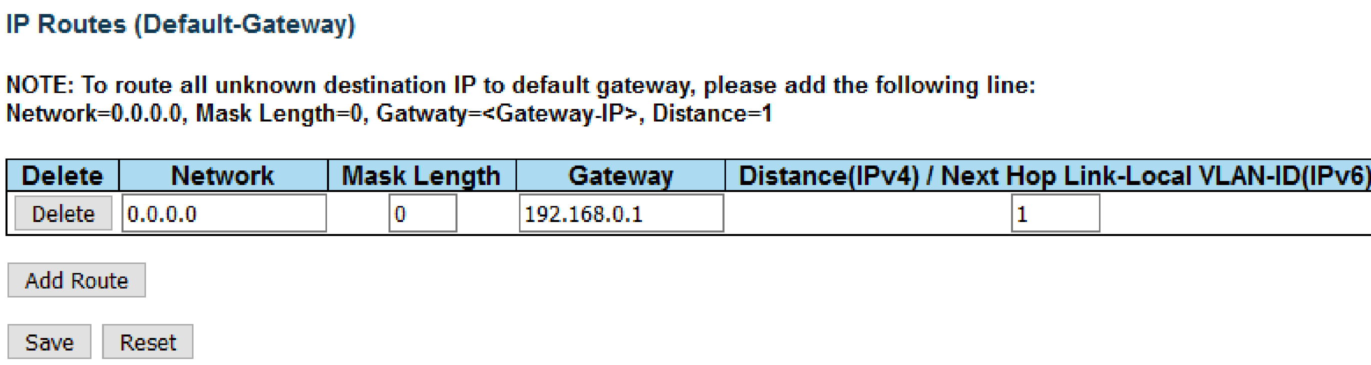
IPv4,IPv6 Interfac

Delete	VLAN	IPv4	DHCPv6		IPv6	
			Enable	Current Lease	Address	Mask Length
□	1		□		1234::98	64

Figure 4-3: Dynamic/Static IPv6 Address Configuration.

4.2.3 IP Routes (Default-Gateway) configuration

The IP routes section controls which default gateway to use when an IP address should be sent by the unit management interface to another network outside of the unit local LAN.



IP Routes (Default-Gateway)

NOTE: To route all unknown destination IP to default gateway, please add the following line:
Network=0.0.0.0, Mask Length=0, Gatwaty=<Gateway-IP>, Distance=1

Delete	Network	Mask Length	Gateway	Distance(IPv4) / Next Hop Link-Local VLAN-ID(IPv6)
Delete	0.0.0.0	0	192.168.0.1	1

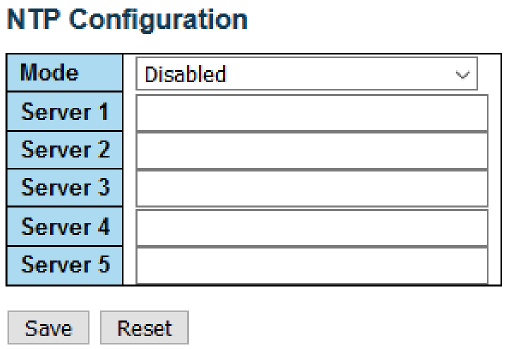
Figure 4-4: IP Routes (Default-Gateway) configuration

NOTE:
To route all unknown destination IP to a default gateway, please add the following line: network=0.0.0.0, Mask Length=0, Gateway=<Gateway-IP> , Distance=1

Different IP networks may have different IPv4/v6 gateways. Please use the configuration as in the note above to route all unknown destination IP traffic to the same default gateway. In case there are multiple path options, please use the appropriate Distance/Next-Hop cost field to prioritize one path over the other.

4.3 Network - Configuration – NTP (Network Time Protocol)

This page is used to configure the unit NTP Servers IP. The NTP Server updates the unit with the correct GMT (Greenwich Mean Time).



NTP Configuration

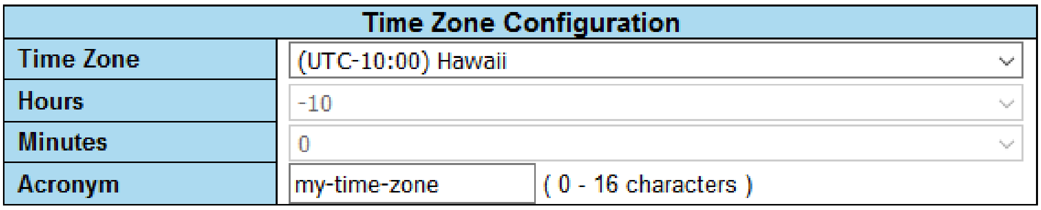
Mode	Disabled
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

Figure 4-5: NTP Server configuration

4.4 Network - Configuration – Time Zone

This page is used to configure the unit’s local time zone and daylight saving.

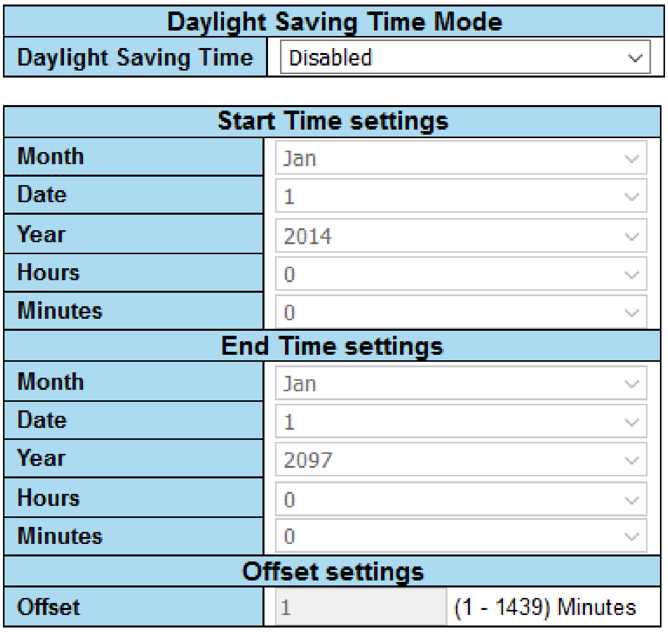
4.4.1 Time Zone Configuration



Time Zone Configuration	
Time Zone	(UTC-10:00) Hawaii
Hours	-10
Minutes	0
Acronym	my-time-zone (0 - 16 characters)

Figure 4-6: Time Zone Configuration

4.4.2 Daylight Saving Time Configuration.



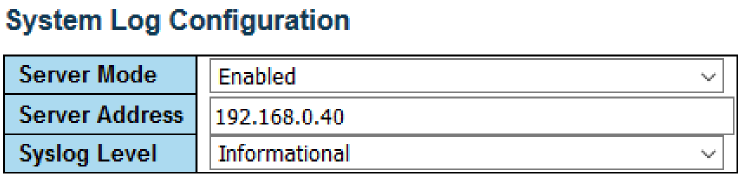
Daylight Saving Time Mode	
Daylight Saving Time	Disabled

Start Time settings	
Month	Jan
Date	1
Year	2014
Hours	0
Minutes	0
End Time settings	
Month	Jan
Date	1
Year	2097
Hours	0
Minutes	0
Offset settings	
Offset	1 (1 - 1439) Minutes

Figure 4-7: Daylight Saving Time Configuration

4.5 Network - Configuration – SysLog Report

This page is used to configure the SysLog Server IP address. The unit sends SysLog messages during Power-up and normal operation. The SysLog events are sent by the unit over the network to the SysLog Server. The user has the option to filter some of the SysLog messages being sent by the unit, by configuring the severity/importance of the SysLog messages that will trigger the sending.



System Log Configuration

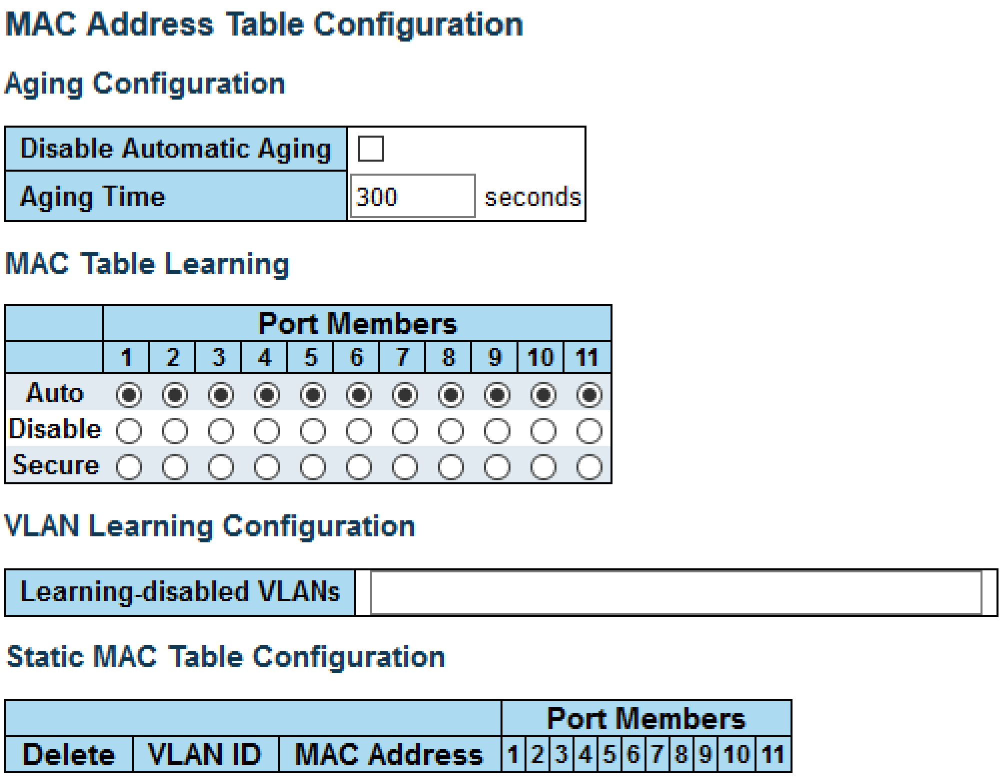
Server Mode	Enabled
Server Address	192.168.0.40
Syslog Level	Informational

Figure 4-8: SysLog configuration

4.6 Network - Configuration – MAC Table learning

This page provides various options regarding the way MAC address learning should be processed by the Ethernet Switch, and how to process a packet with an unknown source MAC address, unknown destination MAC address, etc.

When a packet is received, it is classified by its Source-MAC, Destination-MAC, VLAN-ID and Port number. As part of the Ethernet Switch forwarding algorithm, the switch will look for Destination-MAC and VLAN inside the MAC learning table. If it is found, then the packet will be forwarded to the specified port; otherwise the packet is flooded to all ports on the same VLAN.



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members										
	1	2	3	4	5	6	7	8	9	10	11
Auto	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○

VLAN Learning Configuration

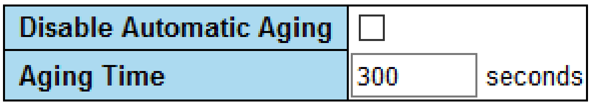
Learning-disabled VLANs	

Static MAC Table Configuration

			Port Members										
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11

Figure 4-9: MAC Table learning configuration page.

4.6.1 Aging Configuration



Disable Automatic Aging	□
Aging Time	300 seconds

Figure 4-10: MAC Table Ageing Configuration

NOTE:
Every new incoming packet with the same source MAC address will set the aging counter for the specific MAC address to start counting from zero again.

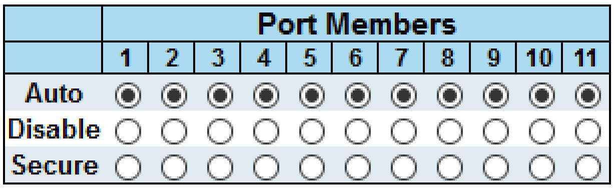
Disable Automatic Aging

Enable/Disable from MAC table to automatically erase MAC address if no packet with the same source MAC address was received for a time longer then the Aging Time.

Aging Time

Set the maximum time in seconds in which a source MAC address may remain in the Switch MAC table without receiving another packet with the same source MAC address from the same port.

4.6.2 MAC Table Learning



	Port Members										
	1	2	3	4	5	6	7	8	9	10	11
Auto	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○

Figure 4-11: MAC Table Learning

The following MAC learning options are available:

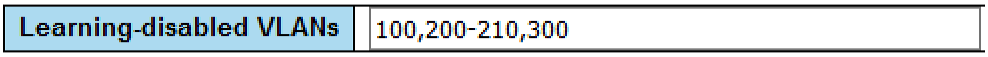
Auto – Normal automatic source MAC address learning and filtering for every incoming packet.

Disable - No MAC learning is done from the selected port. However, the same Switch MAC filtering algorithm applies, meaning that the received incoming packet will be sent to a specific port in case the destination MAC is in the MAC leaning table, or be flooded to all other ports **on the same VLAN in case the destination MAC is unknown.**

Secure – Source MAC address learning is disabled for the selected port. Any incoming packet with unknown source MAC will be discarded. This mode should be used whenever network communication should be restricted to a limited number of network devices with known MAC address.
However, whenever a packet is received on another port configured as Auto (for example) with destination MAC unknown, or multicast/broadcast, then this packet will be flooded to all other ports on same VLAN including those configured as Secure.

NOTE:
To avoid unit management loss, please make sure that the link used for managing the unit was added to the Static Mac Table before changing to secure learning mode.

4.6.3 VLAN Learning-Disabled configuration



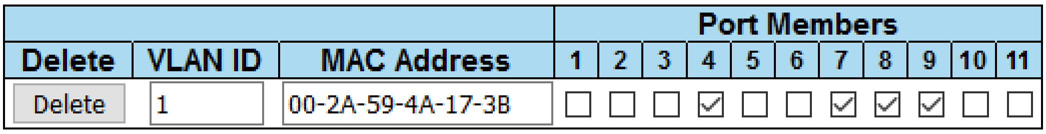
Learning-disabled VLANs	100,200-210,300

Figure 4-12: VLAN Learning Configuration

It is possible to configure the Switch not to the learn source MAC address from specific VLAN, or a group of VLANs. Incoming packets from learning-disabled VLANs will be forwarded to other ports as before (no packet drop. Forward to specific port if destination MAC is known, or flood to all other ports on same VLAN if destination MAC is unknown).

NOTE:
The following example: 1,10-13,200,300 will disable source MAC learning from VLANs 1, 10, 11, 12, 13, 200, and 300.

4.6.4 Static MAC Table Configuration



			Port Members										
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11
Delete	1	00-2A-59-4A-17-3B	□	□	□	☑	□	□	☑	☑	☑	□	□

Figure 4-13: Static MAC Table Configuration

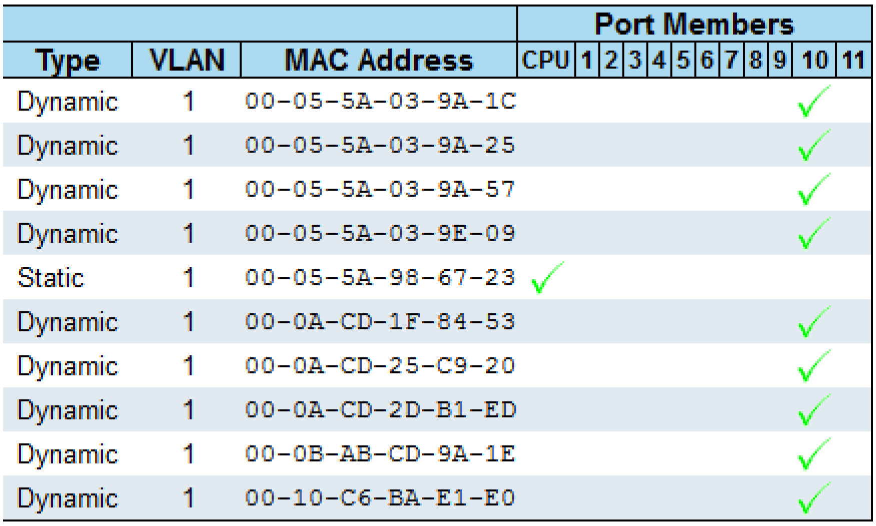
Static MAC address configuration affects mostly the way packets with destination MAC matching to one of the static MAC addresses are being handled by the Switch.

Forwarding a packet with static destination MAC – A packet with a destination MAC matching to one of the static MAC table entries will be forward only to the checked ports. For example, if packet with destination MAC 00-2A-59-4A-17-3B, as in the image above, will be received on port #2 (unchecked), then it will be forwarded to ports 4,7,8,9 (checked)

Forwarding a packet with a static source MAC – A packet with source MAC which is the same as one of the MAC address in the static MAC table entries, for example 00-2A-59-4A-17-3B as in the image above, which received from one of the unchecked source ports, will be forwarding as a usual packet based on the destination MAC. The Switch MAC table will not update the source port from which the packet was received.

4.7 Network - View – MAC Table in use

The Switch MAC table may contain up to 8192 entries. This page can show up to 999 MAC entries for every page, with a default of 20 MAC addresses per page.

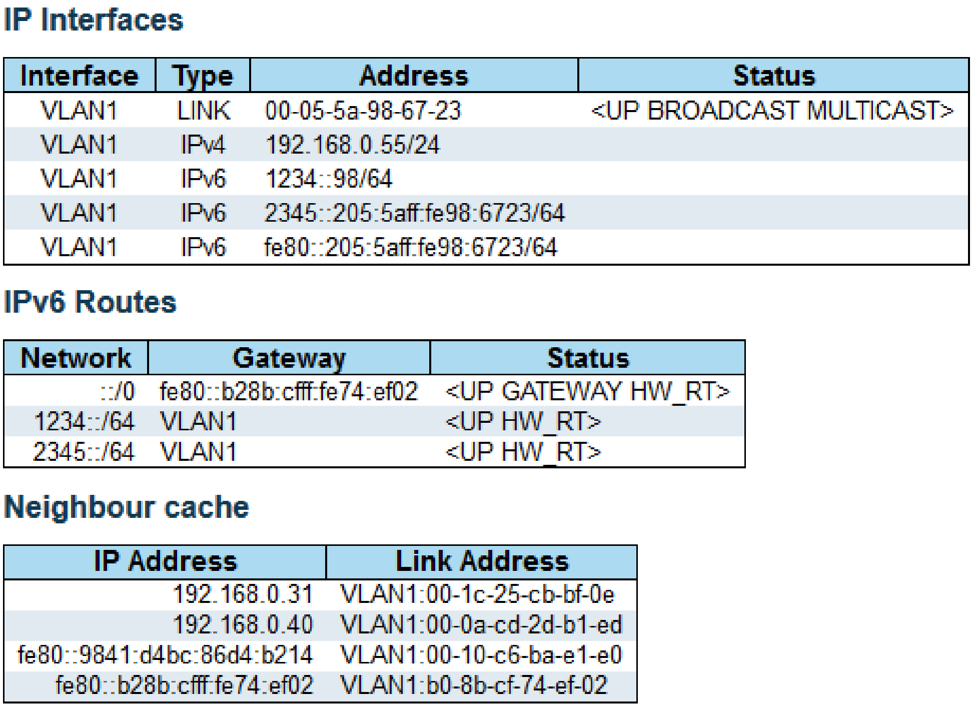


			Port Members											
Type	**VLAN**	**MAC Address**	**CPU**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Dynamic	1	00-05-5A-03-9A-1C											✓	
Dynamic	1	00-05-5A-03-9A-25											✓	
Dynamic	1	00-05-5A-03-9A-57											✓	
Dynamic	1	00-05-5A-03-9E-09											✓	
Static	1	00-05-5A-98-67-23	✓											
Dynamic	1	00-0A-CD-1F-84-53											✓	
Dynamic	1	00-0A-CD-25-C9-20											✓	
Dynamic	1	00-0A-CD-2D-B1-ED											✓	
Dynamic	1	00-0B-AB-CD-9A-1E											✓	
Dynamic	1	00-10-C6-BA-E1-E0											✓	

Figure 4-14: View unit MAC Address Table

4.8 Network - View – IP Status

This page displays the various dynamic addresses that can be used to manage the unit, the IPv6 routes and the neighbor cache (ARP cache) status.



IP Interfaces

Interface	Type	Address	Status
VLAN1	LINK	00-05-5a-98-67-23	<UP BROADCAST MULTICAST>
VLAN1	IPv4	192.168.0.55/24	
VLAN1	IPv6	1234::98/64	
VLAN1	IPv6	2345::205:5aff:fe98:6723/64	
VLAN1	IPv6	fe80::205:5aff:fe98:6723/64	

IPv6 Routes

Network	Gateway	Status
::/0	fe80::b28b:cfff:fe74:ef02	<UP GATEWAY HW_RT>
1234::/64	VLAN1	<UP HW_RT>
2345::/64	VLAN1	<UP HW_RT>

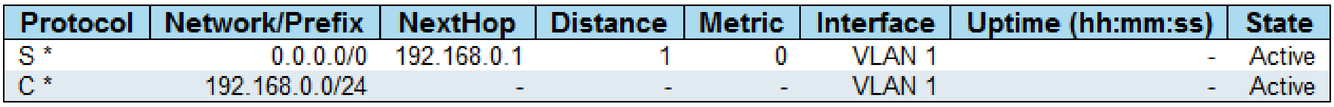
Neighbour cache

IP Address	Link Address
192.168.0.31	VLAN1:00-1c-25-cb-bf-0e
192.168.0.40	VLAN1:00-0a-cd-2d-b1-ed
fe80::9841:d4bc:86d4:b214	VLAN1:00-10-c6-ba-e1-e0
fe80::b28b:cfff:fe74:ef02	VLAN1:b0-8b-cf-74-ef-02

Figure 4-15: View unit in use IP address

4.9 Network - View – Routing Info

This page displays the routing option used by the unit for communicating with other IP-based network devices located on other networks. The routing information may be based on user static configuration, or by DHCP.



Protocol	Network/Prefix	NextHop	Distance	Metric	Interface	Uptime (hh:mm:ss)	State
S *	0.0.0.0/0	192.168.0.1	1	0	VLAN 1	-	Active
C *	192.168.0.0/24	-	-	-	VLAN 1	-	Active

Figure 4-16: View unit Routing Information

5 ACCESS CONTROL

The pages under Access Control control who can access the unit, from what type of network interface, who will verify the remote user username and password (by the unit locally, or by RADIUS/TACACS+ Authentication Server), etc.

5.1 Access Control – Local Users Configuration

This page allows to change the admin user password, add or remove additional users, and change users' password.

NOTE:
NOTE1 – The unit is shipped with a default username admin and with no password. It is strongly recommended to assign a strong password instead.
NOTE2 – The username *admin* can't be removed or changed, only its password

5.1.1 Changing the admin password

Click on the user *admin* located under *Local Users*. Select *Change Password*. Enter a new password and press *Save*.

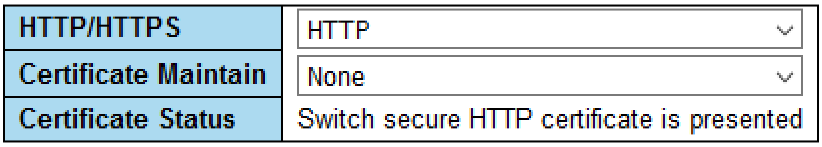
5.1.2 Changing a username or a password

To change a username (other than admin), you need to delete the old user first, and then add the new user instead.

To change an existing user password, click on the user name. Select *Change Password* and enter the new password.

5.2 Access Control – Web Server HTTPS Configuration

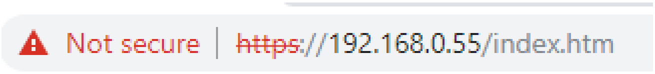
HTTP/HTTPS - Controls whether the unit embedded web server should operate in HTTP or HTTPS mode. HTTPS uses TLS v1.2 encryption to encrypt all Web network traffic between the user web browser and the unit Web Server.



HTTP/HTTPS	HTTP
Certificate Maintain	None
Certificate Status	Switch secure HTTP certificate is presented

Figure 5-1: Web Server HTTP/HTTPS Configuration

Certificate Maintain – This option offers the administrator to manage the unit web-server's self-signed or CA signed certificate, used by web clients to verify if the unit web site is legit. Adding such a certificate into the unit should eliminate the browser warning message, which recommends to the user to avoid browsing to the unit.



⚠ Not secure | ~~https~~://192.168.0.55/index.htm

Figure 5-2: Unsecure HTTPS browsing warning

The following certificate management options are available:

- **None**: No action (default).
- **Delete**: Delete the certificate being used by the Web Server. Since HTTPS cannot operate without a certificate, this option can be executed only when the Web Server is configured as HTTP Web Server.

- **Generate**: Generate a new self-signed certificate required for HTTPS Web Server operation. Please note that a self-signed certificate will cause a web browser warning requesting user permission to add an exception to the web browser security protection policy, before browsing to the unit.
- **Upload:** Upload a PEM certificate file. The possible methods are: use a web browser for uploading a certificate from your local drive, or a URL for uploading a certificate over HTTP, HTTPS, TFTP, FTP.

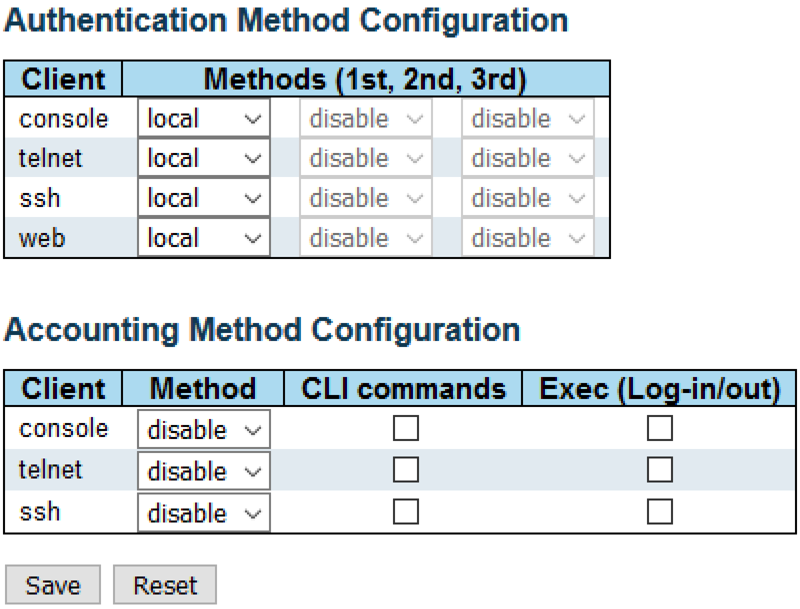
NOTE:

NOTE – Please refer to document 06-0013-021 for information on how to generate and maintain Self-Signed, CA-Signed certificates

5.3 Access Control – Telnet/SSH/Web

Authentication Method Configuration - Configures which network interface such as telnet, SSH, Web or a local console should be enabled or disable, and how the remote user username + password will be authenticated. Should it be done locally by the unit or by remote RADIUS/TACACS+ authentication server.

Accounting Method Configuration - Configures if the unit should send Accounting messages to remote TACACS+ Accounting server whenever a remote user logs in / logs out, and report any CLI command typed by the user over Console, Telnet or SSH.



Authentication Method Configuration

Client	Methods (1st, 2nd, 3rd)		
console	local	disable	disable
telnet	local	disable	disable
ssh	local	disable	disable
web	local	disable	disable

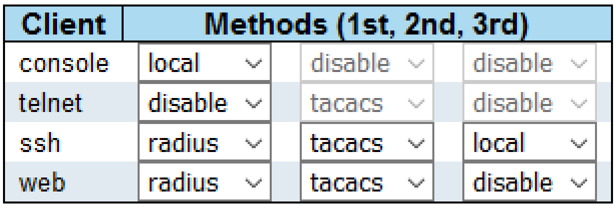
Accounting Method Configuration

Client	Method	CLI commands	Exec (Log-in/out)
console	disable	□	□
telnet	disable	□	□
ssh	disable	□	□

Figure 5-3: Access Control – Telnet/SSH/Web

5.3.1 Authentication Method Configuration

Every one of the management interfaces (console, Telnet, SSH, web) has 3 optional authentication services going from left to right. If the 1st remote authentication service cannot be reached then the 2nd authentication service will be used instead, and the same for 3rd in case both the 1st and the 2nd authentication services are unreachable.



Client	Methods (1st, 2nd, 3rd)		
console	local	disable	disable
telnet	disable	tacacs	disable
ssh	radius	tacacs	local
web	radius	tacacs	disable

Figure 5-4: Authentication Example

In the example above the user username + password authentication is processed as follows:

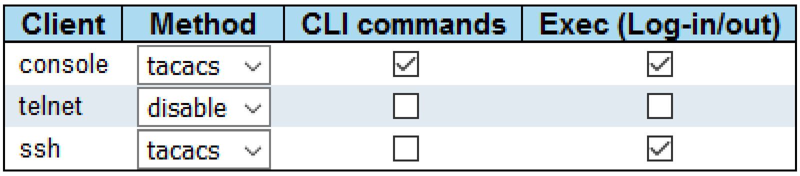
- **Console:** The username and password are processed localy based on the unit configuration.
- **Telnet**: Telnet is disabled (no Telnet)
- **SSH**: The remote SSH username + password authentication will be done by a remote Radius Server. In case the Radius Server is down (no reply), then TACACS+ authentication server will be used instead. In case TACACS+ Server is also down (no reply) then it will be tested against the unit local configuration.
- **Web**: The remote web username + password authentication will be done by a remote Radius Server. In case the Radius Server is down (no reply), then TACACS+ authentication server will be used instead. In case TACACS+ server is also down, then the user will be rejected.

NOTE:

NOTE – RADIUS, TACACS+ configuration is done from in other pages.

5.3.2 Accounting Method Configuration

Any activity on any of the text-based interface (Console, Telnet, SSH) has the option to be reported and logged to an Accounting TACACS+ Server



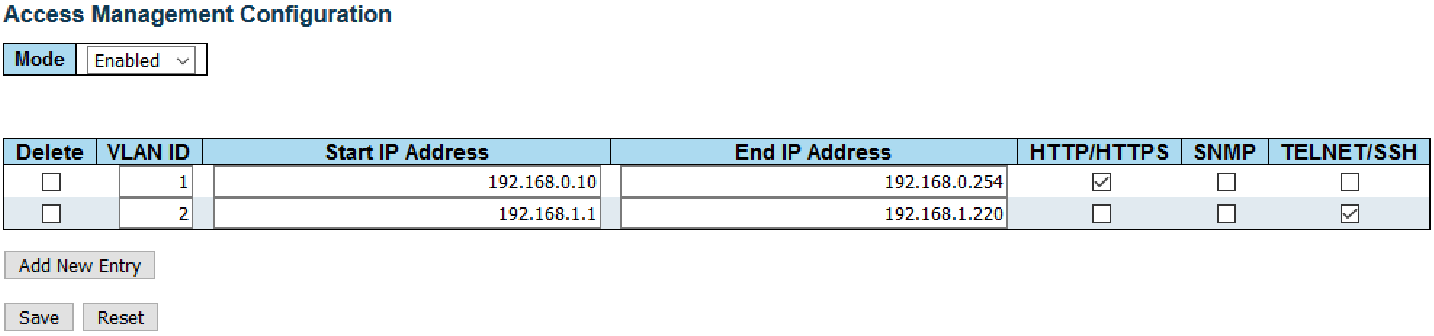
Client	Method	CLI commands	Exec (Log-in/out)
console	tacacs	☑	☑
telnet	disable	□	□
ssh	tacacs	□	☑

Figure 5-5: Accounting Method Configuration example

The user can configure that any login/logout or any command being typed will be reported to TACACS+ Accounting Server (the same used for remote user authentication). Same for any CLI command typed by the user.

5.4 Access Control – Access Control List

The access control list allows the user to configure from what IP range the remote user will be able to access the Switch management interface over the web, SNMP, and Telnet/SSH. Up to 16 entries can be added to the Access Control List table.



Access Management Configuration

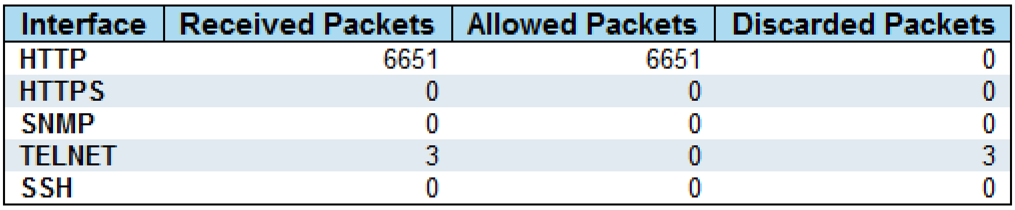
Mode	Enabled

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
□	1	192.168.0.10	192.168.0.254	☑	□	□
□	2	192.168.1.1	192.168.1.220	□	□	☑

Figure 5-6: Access Control List

5.5 Access Control – View ACL Statistics

This page tracks the number of packets used to access the Switch management interface whenever the Access Control List is enabled. This report may help, for example, to identify an external user trying to hack the unit by reporting the number of discarded packets, etc.



Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	6651	6651	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	3	0	3
SSH	0	0	0

Figure 5-7: View ACL Statistics

6 VLAN

6.1 General

- **VLAN Access -** VLAN is a mean to split Switch ports into support groups while each group is totally isolated from the other as if we are using two or more independent Switches. Such splitting is done by assigning different VLAN-IDs to various groups of ports, each group is assigned a different VLAN-ID and the ports for each group are configured as Access ports, meaning that VLAN tagging and port splitting is done internally by the switch. The packets transmitted over the Access ports are the normal Ethernet ports with no VLAN tagging.
- **VLAN Trunk** – VLAN Trunk port configuration allows multiple VLAN-IDs to transfer over the same Ethernet cable or local LAN network with absolute separation between the VLANs transferring over the same infrastructure. A good analogy will be a highway with several lanes having physical separation between each lane, preventing from a car to switch lanes although all the cars are traveling from one side of the highway to the other.

6.1.1 Supported VLAN types

The switch supports single 802.1Q VLAN tagging and double 802.1Q VLAN tagging also known as QinQ or 802.1ad. Switch ports with no external VLAN tagging are referred to as Access-Ports. Switch Ports with external single VLAN tagging are referred to as Trunk C-Ports (C=customer VLAN). Ports with double VLAN tagging are referred to as Trunk S-Ports (S=Service VLAN), as an internet service provider may encapsulate customer VLAN on top of its own VLAN, resulting in double VLAN tagging.

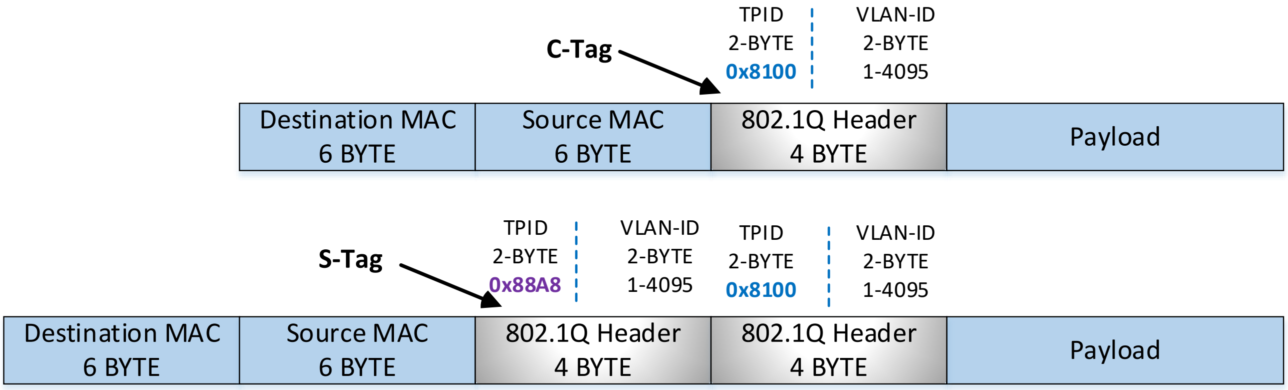


Figure 6-1: single and double VLAN tagging packet format

6.1.2 VLAN typing syntax

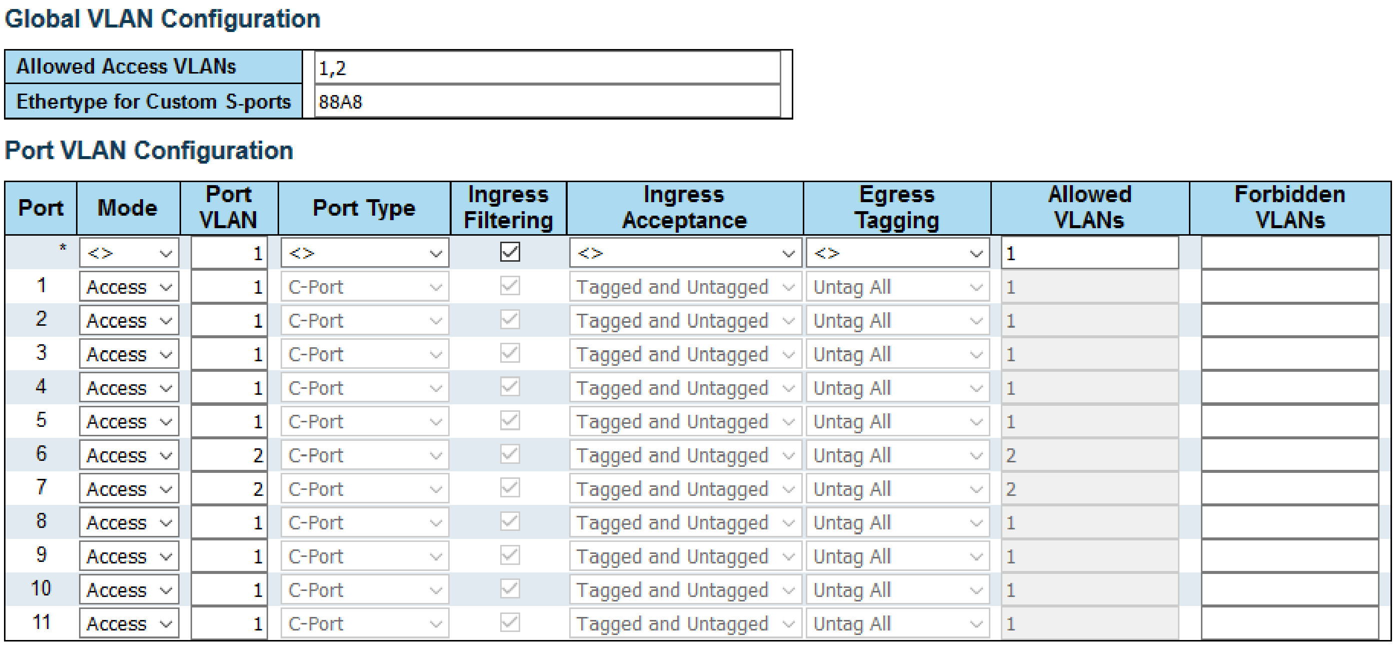
Individual VLAN elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example **1,10-13,200,300** will create VLANs 1, 10, 11, 12, 13, 200, and 300.

6.2 VLAN – Configuration

The VLAN configuration page consists of a global section and per port VLAN configuration.

NOTE:

NOTE – The next section contains several VLAN configuration examples which should make VLAN configuration understanding easier.



Global VLAN Configuration

Allowed Access VLANs	1,2
Ethertype for Custom S-ports	88A8

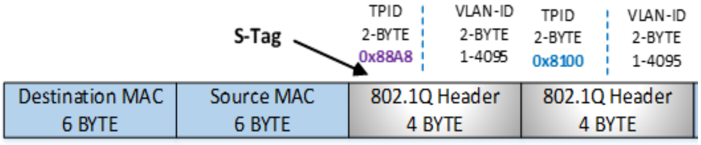
Port VLAN Configuration

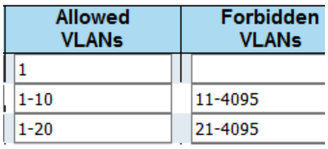
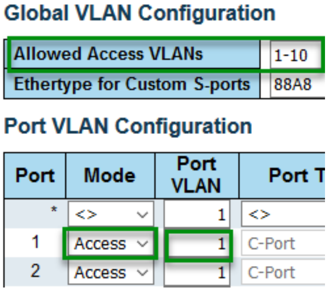
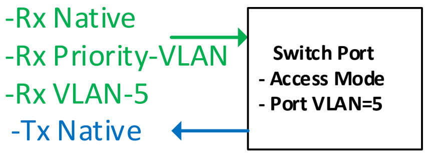
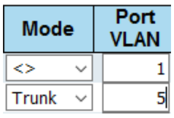
Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	2	C-Port	☑	Tagged and Untagged	Untag All	2	
7	Access	2	C-Port	☑	Tagged and Untagged	Untag All	2	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
11	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

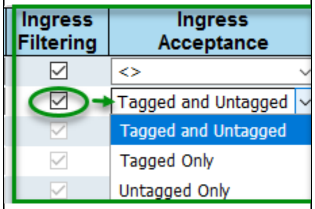
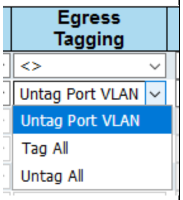
Figure 6-2: VLAN configuration (global plus per-port)

6.2.1 Switch VLAN Terminology - explained

The table below attempts to simplify some of the VLAN terminology used in this chapter. To simplify term description, some configuration parameters will be used with real values rather than using their general term.

Term	Description
Ingress	Received packet
Egress	Transmitted packet
TPID = Tag Protocol Identifier	The first two out of four-byte of VLAN tagging. Typically, it should be 0x8100 followed by additional two-byte VLAN-ID. In case of Q-in-Q 802.1ad double VLAN tagging it should be 0x88A8
Valid VLAN-ID range	Valid VLAN-ID numbers range from 1-4095. VLAN-ID number 0, also known as VLAN Priority Tag is an exception. It is used typically by VoIP systems to prioritize VoIP traffic over regular data traffic. VLAN tag is made of four bytes. 1st two bytes=0x8100 followed by customer VLAN-ID tag)
VLAN Priority Tag	VLAN-ID #0 used typically by VoIP system to mark VoIP priority packets
Native VLAN	Packet with no VLAN tagging
C-Tag	Customer VLAN-ID tag.
S-Tag	Service provider encapsulation of original customer C-Tag VLAN-ID with another VLAN-ID named S-Tag. Double  S-Tag TPID 2-BYTE 0x88A8 VLAN-ID 2-BYTE 1-4095 TPID 2-BYTE 0x8100 VLAN-ID 2-BYTE 1-4095 Destination MAC 6 BYTE Source MAC 6 BYTE 802.1Q Header 4 BYTE 802.1Q Header 4 BYTE

Term	Description	
	VLAN encapsulation tagging is also referred as Q-in-Q or 802.1ad	
Allowed VLANs/ Forbidden VLANs - Mode = Trunk - Mode = Hybrid	Switch port in Trunk or Hybrid mode can be configured to discard packets from specific VLAN-IDs, and must be configured to accept the VLAN-IDs in use.	 Allowed VLANs | Forbidden VLANs 1 | 1-10 | 11-4095 1-20 | 21-4095
Switch port config Access-Mode - Port VLAN=5	The figure to the right highlights in green the VLAN configuration parameters to be set when configuring Switch ports to Access mode. Please verify that Port VLAN-ID is included in the *Allowed Access Vlans* configuration field VLANs list. ➢ Used usually to connect end devices ➢ Receive native VLAN packets (no VLAN) ➢ Receive Priority VLAN (VLAN-0) packets ➢ Receive VLAN packets with VLAN-ID same as Access VLAN-ID (VLAN-5 as in this example) ➢ Transmit only native VLAN packets (removes the VLAN-ID tag - no VLAN)	 Global VLAN Configuration Allowed Access VLANs | 1-10 Ethertype for Custom S-ports | 88A8 Port VLAN Configuration Port | Mode | Port VLAN | Port T * | <> | 1 | <> 1 | Access | 1 | C-Port 2 | Access | 1 | C-Port  -Rx Native -Rx Priority-VLAN -Rx VLAN-5 -Tx Native Switch Port - Access Mode - Port VLAN=5
Switch port config Trunk-Mode - Port VLAN=5	➢ Used to connect between Switches. May use multiple VLANs between Switches ➢ Egress Tag configuration parameter = untag Port VLAN o Rx native VLAN (no VLAN) as VLAN-5 o Rx VLAN priority tag (VLAN-0) as VLAN-5 o Tx tag all packets except VLAN-5. For example, a packet received from another port configured as Access Port VLAN-5, will be transmitted untagged. ➢ Egress Tag configuration parameter = Tag All o Rx native VLAN (untagged packets) is discarded. o Rx VLAN priority tag (VLAN-0) is discarded. o Tx all packets as VLAN tagged	 Mode | Port VLAN <> | 1 Trunk | 5

Term	Description
Hybrid-Mode (general)	Hybrid-Mode is an extension of Trunk-Mode. The difference between Hybrid-Mode and Trunk-Mode is more configuration changes of additional parameters as Port-Type, Ingress-Filtering, etc. (described in more detail below).
Hybrid Ingress (Rx) Filtering	In Hybrid mode it is possible to enable/disable Rx packets filtering based on VLAN header presence. The following options are available: ➢ Tagged and Untagged: accept both tagged and untagged frames. ➢ Tagged Only: accept only tagged frames. Discard Untagged frames. ➢ Untagged Only: accept only untagged frames. **NOTE:** **Ingress filter is inactive (accept all) when the port is configured as *Hybrid → Unaware*.** Discard Tagged frames.  Ingress Filtering Ingress Acceptance ☑ <> ☑ Tagged and Untagged Tagged and Untagged Tagged Only Untagged Only
Hybrid/Trunk Egress (Tx) Tagging - Port VLAN=5	Ports in Trunk and Hybrid mode may control the tagging of frames on egress. ➢ Untag Port VLAN: Remove VLAN tagging only for port VLAN (VLAN-5 in this example). Leave all other VLAN tags unchanged. This apply to both VLAN TPID 0x88A8 and 0x8100. . ➢ Tagged All: all frames, whether classified to the Port VLAN (VLAN-5) or not, are transmitted with a tag. ➢ Untagged All (only Hybrid mode): All frames, whether classified to the Port VLAN (VLAN-5) or not, are transmitted without a tag **NOTE:** **VLAN double tagging will become single tagged.**  Egress Tagging <> Untag Port VLAN Untag Port VLAN Tag All Untag All
Switch port config Hybrid-Mode - Port Type= Unaware - Port VLAN=5	On ingress (Rx), all frames (whether carrying a VLAN tag or not) are classified to the Port VLAN (VLAN-5 in this example). Possible tags are not removed on egress (Tx). ➢ Rx tags all incoming packets as VLAN-5 even if Rx packet is already tagged. In case packet is tagged with TPID=0x8100, it will be 0x8100 double tagged. For example Rx packet with VLAN-10 will become 0x8100,0x0005,0x8100,0x000A ➢ TX does not untag any transmitted packet
Switch port config Hybrid-Mode - Port Type= C-Port - Port VLAN=5	On ingress (Rx), frames with a VLAN tag with TPID = 0x8100 are classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified. Rx path: o Rx VLAN-2 (an example), Tx to another Trunk port as VLAN-2, also any Access Port VLAN-2.

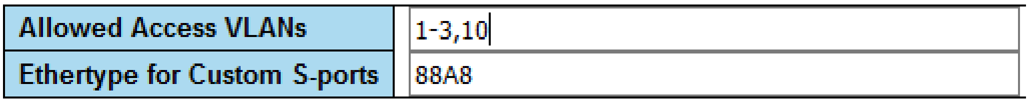
Term	Description
	o Rx native (no VLAN tag), Tx to another Trunk port as VLAN-5 (port VLAN), also any Access port configured as VLAN-5. o Rx priority tagged (VLAN-0), Tx to another Trunk port as VLAN-5 (port VLAN), also any Access port configured as VLAN-5. o Rx from another Access port TX path: o TX does not untag any transmitted packets. However, it may untag Tx packet if its VLAN-ID is the same as Port-VLAN (VLAN-5 in this example) and Egress-Tagging was set to Untag Port VLAN (packet will be sent as native VLAN – untagged).
Switch port config Hybrid-Mode - Port Type= S-Port - Port VLAN=5	On ingress (Rx), frames with a VLAN tag with TPID = 0x8100 or 0x88A8 are classified to the VLAN-ID embedded in the tag (first VLAN-ID in case of Q-in-Q double tagging). If a frame is untagged (no VLAN) or priority tagged (VLAN-0), the frame gets classified to Port VLAN (VLAN-5 in this example). If frames must be tagged on egress (Tx), they will be tagged with an S-tag 0x88A8.
Switch port config Hybrid-Mode - Port Type= S-Custom-Port	Same as for Hybrid S-Port except that the user may configure custom TPID different than 0x88A8 by customizing global VLAN configuration parameter Ethertype for Custom S-ports.

Table 6-1: VLAN terminology explained

6.2.2 Global VLAN Configuration

Allowed Access VLANs - This field shows the allowed Access VLANs. **This field affects only 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 example bellow will create VLANs 1,2,3,10. Spaces are allowed in between the delimiters.



Allowed Access VLANs	1-3,10
Ethertype for Custom S-ports	88A8

Figure 6-3: VLAN Global configuration

Ethertype for Custom S-ports – TPID value (specified in hexadecimal) used for Q-in-Q 802.1ad double VLAN tagging as described in the image bellow. The default value is 0x88A8, and it applies to all ports whose Port Type is set to S-Custom-Port.

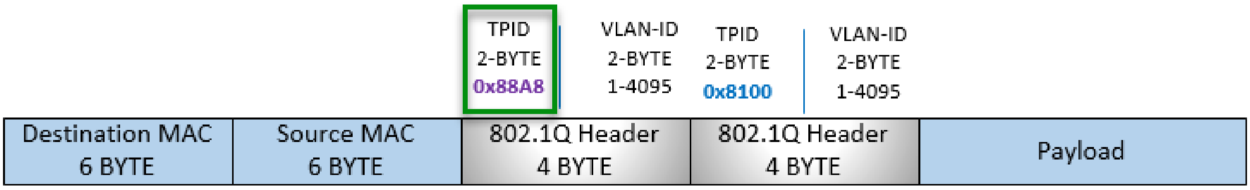
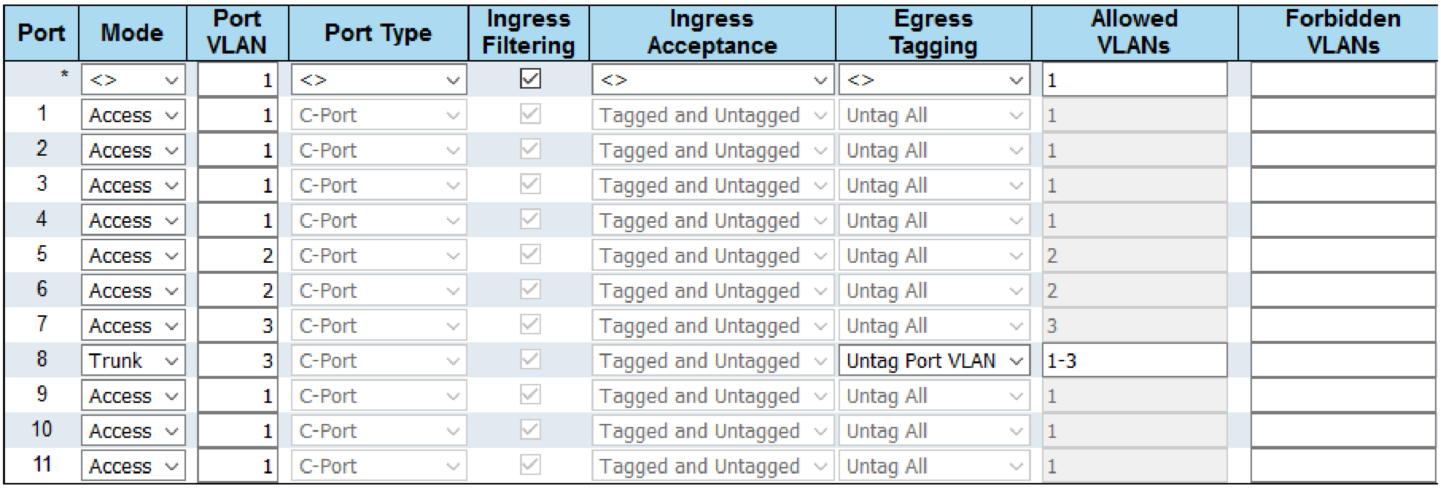


Figure 6-4: VLAN 802.1ad Q-in-Q double VLAN tagging

6.2.3 Port VLAN Configuration



Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	2	C-Port	☑	Tagged and Untagged	Untag All	2	
6	Access	2	C-Port	☑	Tagged and Untagged	Untag All	2	
7	Access	3	C-Port	☑	Tagged and Untagged	Untag All	3	
8	Trunk	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
11	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Figure 6-5: Port VLAN configuration

Port: Switch Ethernet port number

Mode: The Mode field controls the basic VLAN functionality of the port mode (default is Access). A port can be configured to one out of three modes as described below. Whenever a particular mode is selected, the remaining Page fields for that port will be either grayed out or changeable depending on the mode being configured. Grayed out fields show the value that the port will get when the appropriate mode will be applied.

- **Access**: Access ports are normally used to connect end devices which are VLAN unaware. Access ports have the following characteristics:
  - Member of exactly one VLAN as configured in the Port VLAN field. Default Access VLAN is 1
  - Accepts untagged and C-tagged frames.
  - Discards all frames that are not classified to the Access VLAN.
  - On egress all frames are transmitted untaggedγ
- **Trunk**: Trunk ports can carry traffic of multiple VLANs simultaneously. Trunk mode is usually in use whenever there is a need to connect one Switch using multiple VLANs to another Switch. Trunk ports have the following characteristics:
  - By default, a trunk port is member of all VLANs (1-4095) unless defined otherwise by an Allowed VLANs field. In this case none members VLANs are discarded.
  - By default, all frames except frames classified to the Port VLAN (also called as 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 are very similar to Trunk ports with the following extra features:
  - Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware.
  - Ingress filtering can be controlled.
  - Ingress acceptance of frames and configuration of egress tagging can be configured independently.

Port VLAN: configure port VLAN ID (also named as PVID). Valid VLAN values range from 1-4095, with the default value being 1.

On ingress, frames get classified to the Port VLAN. If the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

Port Type: Ports in hybrid mode allow for changing the port type, i.e., whether a frames VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

- **Unaware**: On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.
- **C-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.
- **S-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.
- **S-Custom-Port:** On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.

Ingress Filtering: Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

NOTE:
The Ingress filter is inactive (accept all) when the port is configured as *Hybrid → Unaware*.

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

- **Tagged and Untagged:** Both tagged and untagged frames are accepted.
- **Tagged Only:** Only tagged frames are accepted on ingress. Untagged frames are discarded.
- **Untagged Only:** Only untagged frames are accepted on ingress. Tagged frames are discarded.

Egress Tagging: Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

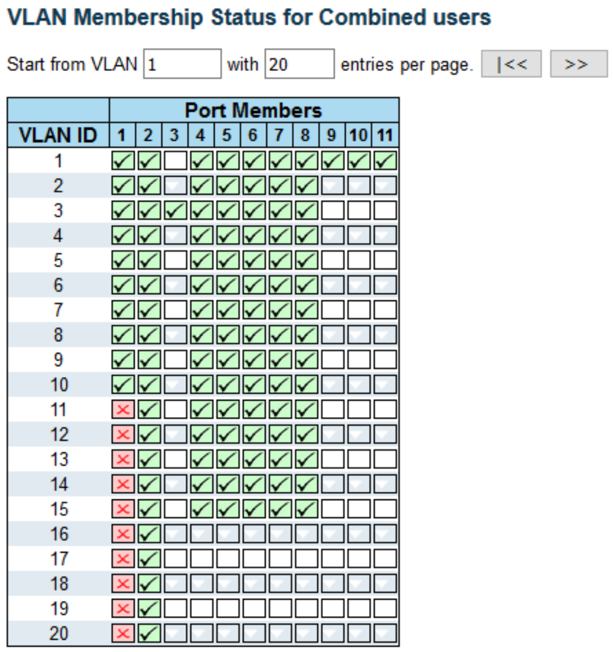
- **Untag Port VLAN:** Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.
- **Tag All:** All frames, whether classified to the Port VLAN or not, are transmitted with a tag. This option is only available for ports in Hybrid mode.

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

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

6.3 VLAN - View Members

This page displays which VLAN-IDs are linked to which Switch Ethernet ports.



VLAN Membership Status for Combined users

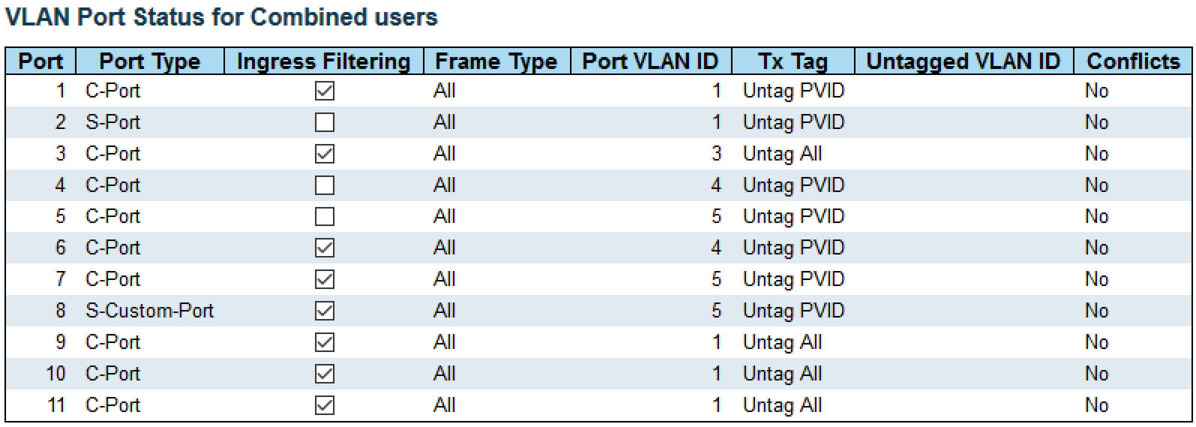
Start from VLAN 1 with 20 entries per page.

	Port Members										
VLAN ID	1	2	3	4	5	6	7	8	9	10	11
1	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	☑
2	☑	☑	□	☑	☑	☑	☑	☑	□	□	□
3	☑	☑	☑	☑	☑	☑	☑	☑	□	□	□
4	☑	☑	□	☑	☑	☑	☑	☑	□	□	□
5	☑	☑	□	☑	☑	☑	☑	☑	□	□	□
6	☑	☑	□	☑	☑	☑	☑	☑	□	□	□
7	☑	☑	□	☑	☑	☑	☑	☑	□	□	□
8	☑	☑	□	☑	☑	☑	☑	☑	□	□	□
9	☑	☑	□	☑	☑	☑	☑	☑	□	□	□
10	☑	☑	□	☑	☑	☑	☑	☑	□	□	□
11	☒	☑	□	☑	☑	☑	☑	☑	□	□	□
12	☒	☑	□	☑	☑	☑	☑	☑	□	□	□
13	☒	☑	□	☑	☑	☑	☑	☑	□	□	□
14	☒	☑	□	☑	☑	☑	☑	☑	□	□	□
15	☒	☑	□	☑	☑	☑	☑	☑	□	□	□
16	☒	☑	□	□	□	□	□	□	□	□	□
17	☒	☑	□	□	□	□	□	□	□	□	□
18	☒	☑	□	□	□	□	□	□	□	□	□
19	☒	☑	□	□	□	□	□	□	□	□	□
20	☒	☑	□	□	□	□	□	□	□	□	□

Figure 6-6: VLAN Membership Status

6.4 VLAN – View Ports

This page displays a summary of all ports VLAN configuration



VLAN Port Status for Combined users

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

Figure 6-7: VLAN Port Status for Combined users

7 POE-BT POWER

7.1 General PoE background

PoE-BT (IEEE 802.3-bt) is the latest PoE (Power Over Ethernet) specification offering up to 90[W] of power whenever power is delivered over all four RJ45 cable pairs. PoE-BT is backwards compatible with PoE-AT (IEE 802.3at) offering up to 30W over two out of four cable pairs of the RJ45 connector. PoE-BT is also backwards compatible with the first PoE specification known as PoE-AF (IEEE 802.3af) capable of delivering up to 15W on two out of four cable pairs inside the RJ45 connector.

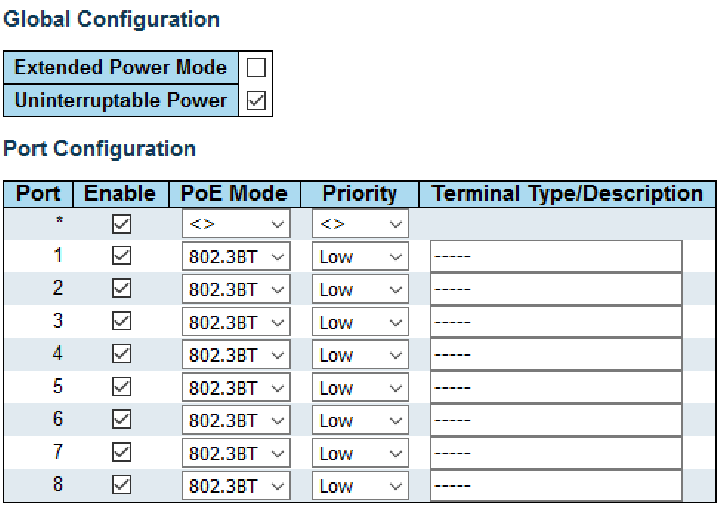
The maximum power offered for each PD (Powered device) as Access Point, IP-Cameras, etc. is determined by each PD classification named Class. The Switch detects the PoE class advertised by every PD and allocates Maximum-Power for each port accordingly.

Poe-PD Class	**Maximum allocated Power [W] by the Switch**	**PoE-BT support**	**PoE-AT Support**	**PoE-AF Support**
0	15.4 (same as class-3)	Yes	Yes	Yes
1	4	Yes	Yes	Yes
2	7	Yes	Yes	Yes
3	15.4	Yes	Yes	Yes
4	30	Yes	Yes	---
5	45	Yes	---	---
6	60	Yes	---	---
7	75	Yes	---	---
8	90	Yes	---	---

Table 7-1: PoE maximum power[W] per PD advertised class

7.2 PoE-BT - Set PoE-BT Power

All PoE configuration, both global and per port is carried out from this page.



Global Configuration

Extended Power Mode	☐
Uninterruptable Power	☑

Port Configuration

Port	Enable	PoE Mode	Priority	Terminal Type/Description
*	☑	<>	<>	
1	☑	802.3BT	Low	-----
2	☑	802.3BT	Low	-----
3	☑	802.3BT	Low	-----
4	☑	802.3BT	Low	-----
5	☑	802.3BT	Low	-----
6	☑	802.3BT	Low	-----
7	☑	802.3BT	Low	-----
8	☑	802.3BT	Low	-----

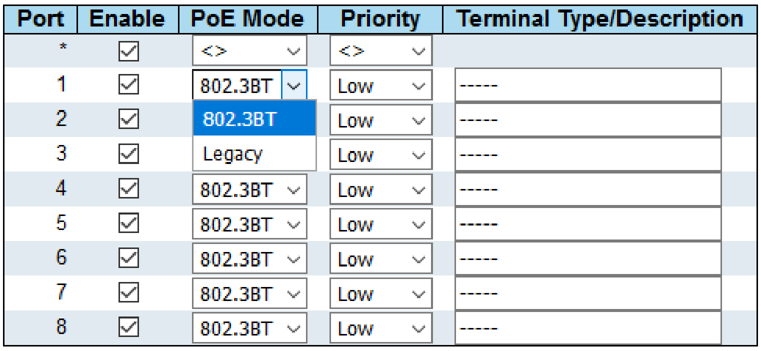
Figure 7-1: PoE-BT configuration

7.2.1 Global Configuration

Extended Power Mode – When checked, any PD device on any one of the ports may consume slightly extra power beyond class maximum power (for example, 93W instead of 90W). Whenever PoE PD device tries to consume power beyond its class max power, it will be shut down by the unit.

Uninterruptable Power – When checked (checked by default), the Switch is prevented from performing a PoE power down and up cycle as part of the Switch's startup process. This is applicable only whenever the Switch is performing software reset, meaning uninterruptable AC power during the entire software reset cycle.

7.2.2 Global Configuration



Port	Enable	PoE Mode	Priority	Terminal Type/Description
*	☑	<>	<>	
1	☑	802.3BT	Low	-----
2	☑		Low	-----
3	☑		Low	-----
4	☑	802.3BT	Low	-----
5	☑	802.3BT	Low	-----
6	☑	802.3BT	Low	-----
7	☑	802.3BT	Low	-----
8	☑	802.3BT	Low	-----

Figure 7-2: PoE Port Configuration

Port – Switch port number. Only PoE capable ports are listed (ports 9-11 are none PoE).

Enable – Enable/Disable POE power. Please note that the Ethernet port will remain active even when PoE port is disabled.

PoE Mode

- **802.3BT:** Powers only PoE-BT/PoE-AT/PoE-AF compliant PD (powered device) devices.

- **Legacy**: Powers PoE-BT/PoE-AT/PoE-AF compliant devices and PD (powered devices), which may not be fully compliant PD devices. Use this option whenever the Switch fails to power a PD device because of PD not fully PoE compliant.

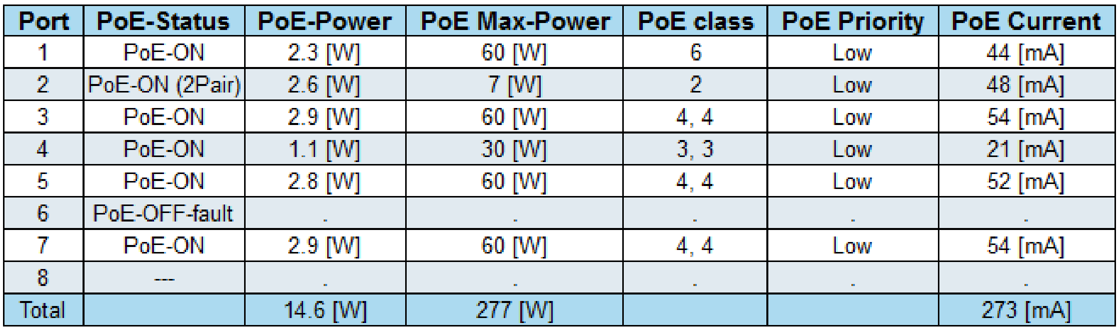
Priority – This parameter assigns the priority for a PD device connected to the Switch port over other PDs connected to the same Switch. This parameter will affect Switch PoE power delivery whenever Switch total power capacity becomes lower than the overall *actual power consumption* of all PDs. In such a scenario the Switch will have to shut down already powered PD device to let other POE devices continue to work uninterrupted.
Also during power up, PDs with higher priority will be powered first. As a result, PDs with lower priority may not be powered at all in case the already powered PDs consume already the total Switch PoE power capacity. There are three priority levels – Low, High, Critical.

- **Low**: The lowest PoE PD capacity. By default, all PoE ports are config to low priority.
- **High**: Higher priority than Low.
- **Critical**: Highest PoE port priority

Terminal Type/Description - a text string used to describe the PoE PD device. It has no effect on PoE functionality.

7.3 PoE-BT - View PoE-BT

This page displays PoE status for all Switch PoE ports.



Port	PoE-Status	PoE-Power	PoE Max-Power	PoE class	PoE Priority	PoE Current
1	PoE-ON	2.3 [W]	60 [W]	6	Low	44 [mA]
2	PoE-ON (2Pair)	2.6 [W]	7 [W]	2	Low	48 [mA]
3	PoE-ON	2.9 [W]	60 [W]	4, 4	Low	54 [mA]
4	PoE-ON	1.1 [W]	30 [W]	3, 3	Low	21 [mA]
5	PoE-ON	2.8 [W]	60 [W]	4, 4	Low	52 [mA]
6	PoE-OFF-fault	.	.	.	.	.
7	PoE-ON	2.9 [W]	60 [W]	4, 4	Low	54 [mA]
8	---	.	.	.	.	.
Total		14.6 [W]	277 [W]			273 [mA]

Figure 7-3: PoE status

Port - Switch port number. Only PoE-capable ports are listed (ports 9-11 are none PoE).

PoE-Status – The following PoE status displays are available

PoE Status	Description
PoE disabled	PoE power was disabled. However, the switch port remains operational as long it is connected to none PoE device (such as Laptop, etc.), and Ethernet port is enabled.
---	PoE is enabled, and no PoE device was detected. This is the normal PoE port state for unplugged Switch ports.
PoE-ON	PoE PD device was detected and power is delivered by the Switch to the PD device. This is the normal state when a typical four pair PD is connected.
PoE-ON (2Pair)	PoE PD device was detected and power is delivered by the Switch to the PD device. However, the power is delivered on only two out of four Ethernet pairs of the RJ45 jack.

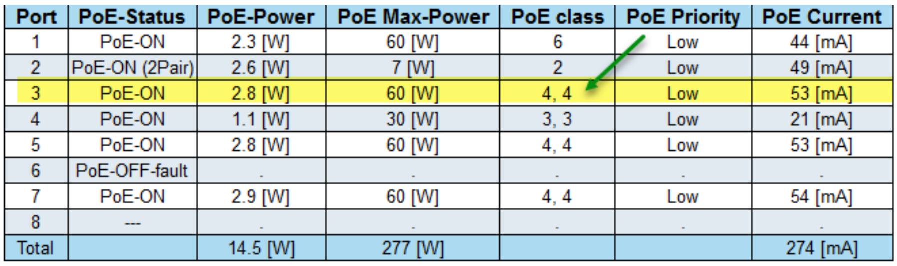
PoE-OFF-fault	For PoE-PD device - Failure to deliver power to a PoE-PD device due to one of the following reasons: • Power limit exceeded - The overall power consumption including the port in fault state, exceeds the maximum power the Power Supply can deliver. • PoE-PD overload - The PD class requests more power than the port can deliver, so the port PoE is down. **NOTE:** **1. To minimize false fault displays, whenever the Ethernet Link port is On with PoE power Off, it is safe to assume that the end device is a none PoE device such as a PC, Laptop, etc. In this case although the PoE detection hardware detected PoE-Fault (and as a result PoE power is not applied – this is OK), it will be displayed as "---" meaning the POE is in search mode, looking for a valid PoE PD device to connect.** **2. However, there are exceptions which may cause PoE Fault to be reported. An example to such an exception is a connected Laptop in sleep mode, since there is no Ethernet Link while the Laptop is in sleep mode.**
No PoE IC	The software failed to detect PoE ICs. This message should not appear during normal unit operation.
Detecting PoE	The software is in the middle of the process to detect PoE ICs over I2C bus. This message should not typically appear during normal operation. However, it may appear for a very short time in case the user logs in to the unit before the entire software initialization stage was completed.
PoE state unknown	PoE initial state. This message should not appear during normal unit operation.

Table 7-2: PoE Status

PoE Power – Reports PoE PD actual power consumption in Watt.

PoE Max-Power – Reports the maximum power in Watt that the PD device may consume. This value is derived from PD class 0-8.

PoE Class - Displays the PoE PD class that the PD device is signaling to the Switch PoE port. Possible values range from class 1-8 (class 0 is same as class 3). In case the PD hardware has double independent class signature hardware (independent class over each two out of four pairs) then two class numbers will be reported as in the figure bellow.



Port	PoE-Status	PoE-Power	PoE Max-Power	PoE class	PoE Priority	PoE Current
1	PoE-ON	2.3 [W]	60 [W]	6	Low	44 [mA]
2	PoE-ON (2Pair)	2.6 [W]	7 [W]	2	Low	49 [mA]
3	PoE-ON	2.8 [W]	60 [W]	4, 4	Low	53 [mA]
4	PoE-ON	1.1 [W]	30 [W]	3, 3	Low	21 [mA]
5	PoE-ON	2.8 [W]	60 [W]	4, 4	Low	53 [mA]
6	PoE-OFF-fault	.	.	.	.	.
7	PoE-ON	2.9 [W]	60 [W]	4, 4	Low	54 [mA]
8	---	.	.	.	.	.
Total		14.5 [W]	277 [W]			274 [mA]

Figure 7-4: PoE Class report

PoE Priority – Displays the PoE priority as it was configured by the user. For a more detailed description please refer to the PoE Priority configuration description.

PoE – Reports the PoE current [mA] consumed by the PoE PD device.

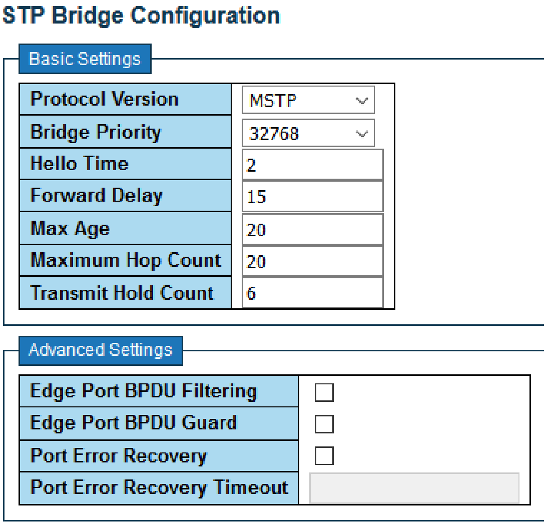
8 SPANNING TREE - STP

8.1 General

Spanning Tree Protocol (STP), and its variations as RSTP and MSTP, is used mainly for the following reasons:

1. To prevent possible network loops, which without STP will cause broadcast storming.
2. Offer redundancy path from Switch to Switch or path to path over multiple Switches by supporting network loops under the control of STP. The STP algorithm will make sure that at any given time only one path out of multiple possible loops will be active, those allowing the Switch to use multiple backup paths in case main connection path go down.

8.2 Spanning tree – Configuration - STP Config



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	32768
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

Figure 8-1: STP Configuration

8.2.1 Basic Settings

Protocol Version -The MSTP/RSTP/STP protocol version setting. Valid values are STP, RSTP, and MSTP.

Bridge Priority - Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Forward Delay - The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age - The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count - This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count - The number of BPDUs 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 BPDUs per second.

8.2.2 Advanced Settings

Edge Port BPDU Filtering - Controls whether a port is explicitly configured as Edge. It will transmit and receive BPDUs.

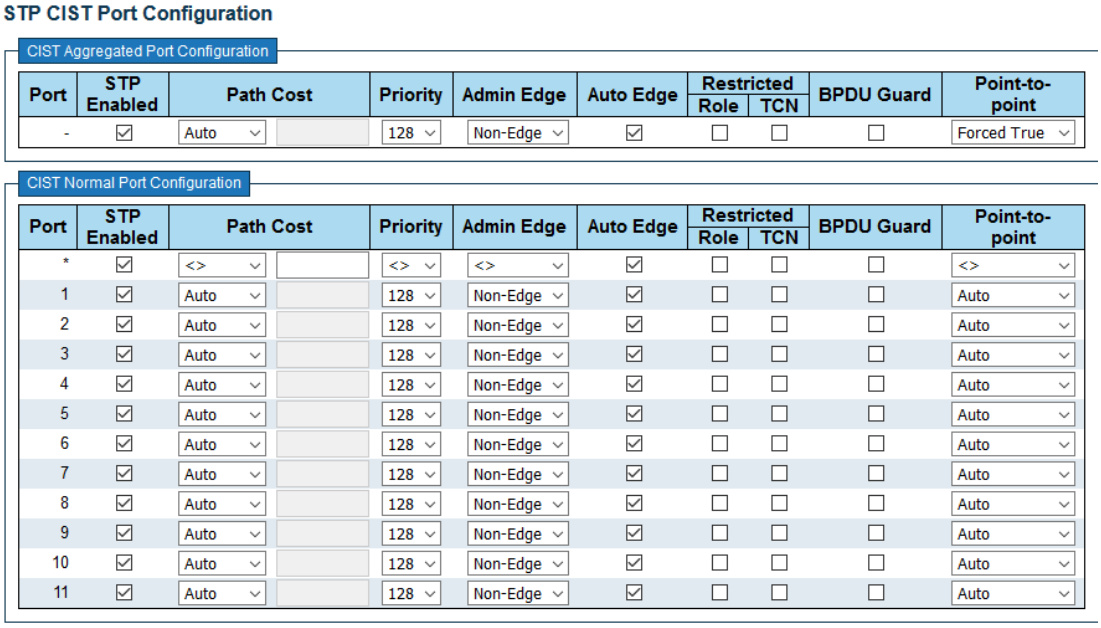
Edge Port BPDU Guard - Controls whether a port is explicitly configured as Edge. It will disable itself upon reception of a BPDU. The port will enter the error-disabled state and will be removed from the active topology.

Port Error Recovery - Controls whether a port in the error-disabled state will be automatically enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout - The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

8.3 Spanning Tree – Configuration - STP Port Config

This option allows you to inspect the current STP CIST port configurations and change them. It contains settings for physical and aggregated ports.



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		
-	☑	Auto		128	Non-Edge	☑	□	□	□	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	☑	<>		<>	<>	☑	□	□	□	<>
1	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
2	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
3	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
4	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
5	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
6	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
7	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
8	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
9	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
10	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
11	☑	Auto		128	Non-Edge	☑	□	□	□	Auto

Figure 8-2: STP Port Configuration

Port - The switch port number of the logical STP port.

STP Enabled - Controls whether STP is enabled on this switch port.

Path Cost - Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

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

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 → STP Detailed Bridge Status → Spanning Tree.

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

AutoEdge -Controls whether the bridge should enable automatic edge detection on the bridge port. This allows *operEdge* to be derived from whether BPDUs are received on the port or not.

Restricted Role - If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

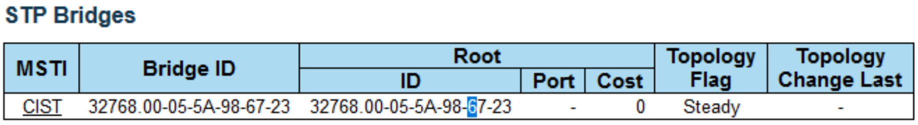
Restricted TCN - If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology because of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard - If enabled, causes the port to disable itself upon receiving valid BPDUs. Contrary to the similar bridge setting, the port Edge status does not affect this setting.

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.

8.4 Spanning tree – View - STP Bridges

This page provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance.

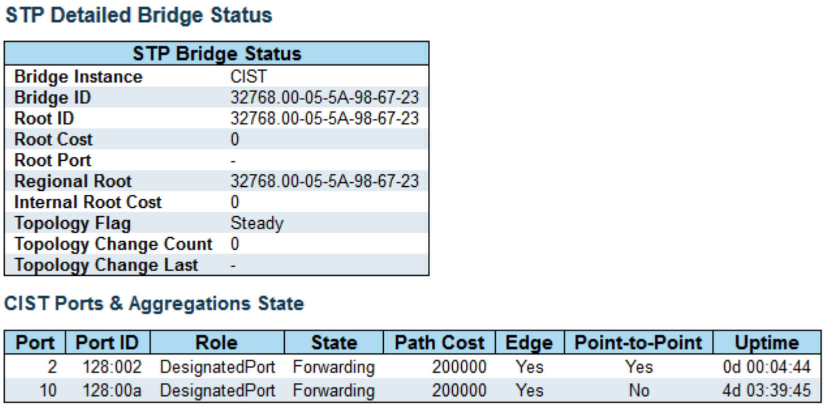


STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-05-5A-98-67-23	32768.00-05-5A-98-67-23	-	0	Steady	-

Figure 8-3: View STP Bridges

MSTI - The Bridge Instance. This is also a link to the *STP Detailed Bridge Status* as described below.



STP Detailed Bridge Status

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-05-5A-98-67-23
Root ID	32768.00-05-5A-98-67-23
Root Cost	0
Root Port	-
Regional Root	32768.00-05-5A-98-67-23
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
2	128:002	DesignatedPort	Forwarding	200000	Yes	Yes	0d 00:04:44
10	128:00a	DesignatedPort	Forwarding	200000	Yes	No	4d 03:39:45

Figure 8-4: View STP Detailed Bridge Status

8.4.1 STP Detailed Bridge Status

- **Bridge Instance** - The Bridge instance - CIST, MST1, ...

- **Bridge ID** - The Bridge ID of this Bridge instance.
- **Root ID -** The Bridge ID of the currently elected root bridge.
- **Root Port -** The switch port currently assigned the *root* port role.
- **Root Cost** - Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
- **Regional Root** - The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. *(For the CIST instance only)*.
- **Internal Root Cost -** The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. *(For the CIST instance only)*.
- **Topology Flag** -The current state of the Topology Change Flag of this Bridge instance.
- **Topology Change Count -** The number of times where the topology change flag has been set (during a one-second interval).
- **Topology Change Last** - The time passed since the Topology Flag was last set.

8.4.2 CIST Ports & Aggregation State

- **Port -** The switch port number of the logical STP port.
- **Port ID** - The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.
- **Role** - The current STP port role. The port role can be one of the following values:
  - AlternatePort
  - BackupPort
  - RootPort
  - DesignatedPort
- **State** - The current STP port state. The port state can be one of the following values: Discarding Learning Forwarding.
- **Path Cost** - The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.
- **Edge** - The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.
- **Point-to-Point** - The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.
- **Uptime** - The time since the bridge port was last initialized.

Bridge ID -The Bridge ID of this Bridge instance.

Root ID - The Bridge ID of the currently elected root bridge.

Root Port - The switch port currently assigned the root port role.

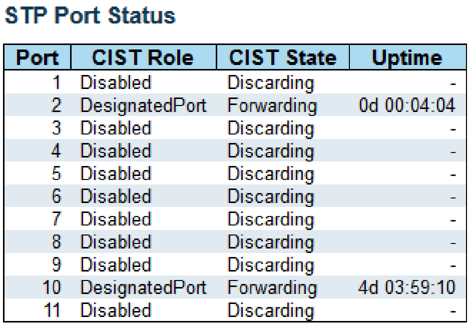
Root Cost - Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag - The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last - The time since last Topology Change occurred.

8.5 Spanning Tree - View - STP Port Status

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



STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	DesignatedPort	Forwarding	0d 00:04:04
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	DesignatedPort	Forwarding	4d 03:59:10
11	Disabled	Discarding	-

Figure 8-5: View STP Port Status

Port - The switch port number of the logical STP port.

CIST Role - The current STP port role of the CIST port. The port role can be one of the following values:

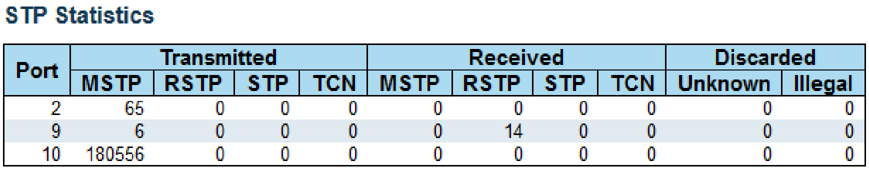
- AlternatePort
- BackupPort
- RootPort
- DesignatedPort
- Disabled.

CIST State - The current STP port state of the CIST port. The port state can be one of the following values: Discarding Learning Forwarding.

Uptime - The time since the bridge port was last initialized.

8.6 Spanning Tree - View - STP Port Statistics

This option displays the STP port statistics counters of bridge ports in the switch. The STP port statistics counters are described below.



STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
2	65	0	0	0	0	0	0	0	0	0
9	6	0	0	0	0	14	0	0	0	0
10	180556	0	0	0	0	0	0	0	0	0

Figure 8-6: View STP Port Statistics

Port - The switch port number of the logical STP port.

MSTP - The number of MSTP BPDUs received/transmitted on the port.

RSTP - The number of RSTP BPDUs received/transmitted on the port.

STP - The number of legacy STP Configuration BPDUs received/transmitted on the port.

9 SNMP

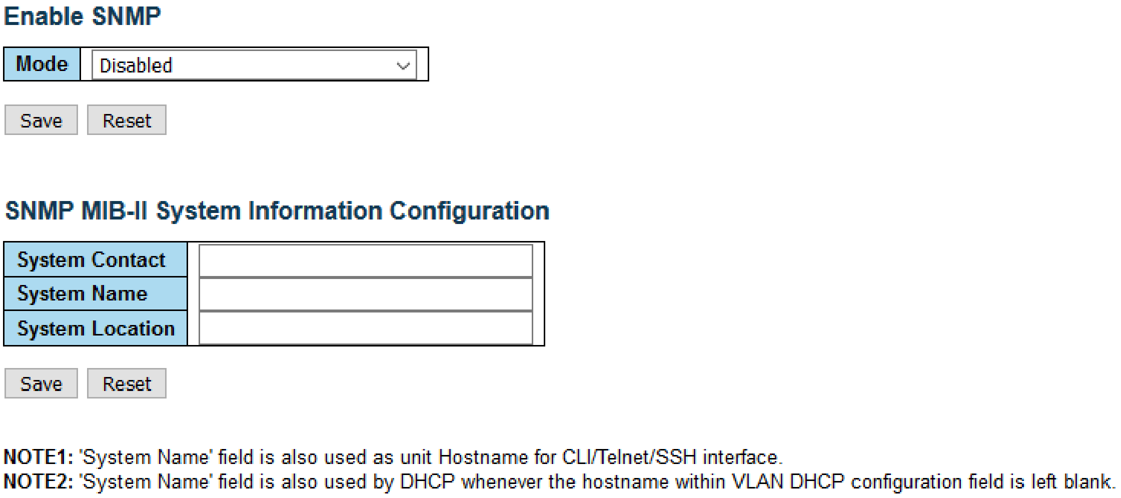
NOTES:

1. Detailed SNMP configuration example can be found at the end of the SNMP section.

2. SNMP is disabled by default for security concerns. In case SNMPv2 is used, please change SNMPv2 default public, private community strings (passwords) prior enabling SNMPv2.

9.1 SNMP- Enable SNMP

This page is responsible for enabling/disabling SNMP in general - SNMPv1, SNMPv2 and SNMPv3 and also configure several SNMP MIB-II System-Information OiD



Enable SNMP

Mode	Disabled

SNMP MIB-II System Information Configuration

System Contact	
System Name	
System Location	

NOTE1: 'System Name' field is also used as unit Hostname for CLI/Telnet/SSH interface.
NOTE2: 'System Name' field is also used by DHCP whenever the hostname within VLAN DHCP configuration field is left blank.

Figure 9-1: Enable SNMP

Enable SNMP – Enable/Disable SNMP in general (SNMP1, SNMPv2, SNMPv3).

System Contact – Textual identification of the contact person for this managed node. String length is 0 to 255, and valid ASCII characters range from 32 to 126.

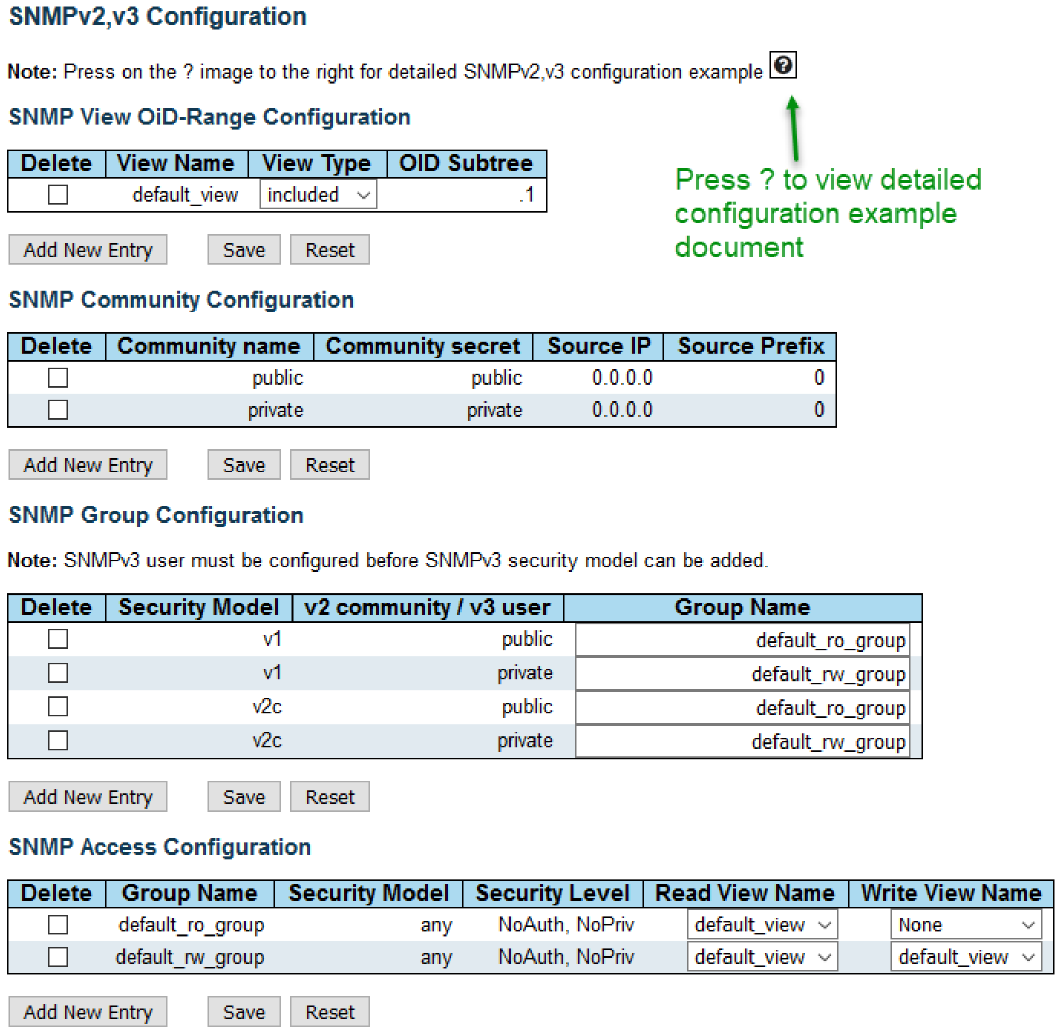
System Name - An administratively assigned name for this managed node. By convention, this is the nodes fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z,a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.

NOTES:

1. The System Name field is also used as unit Hostname for CLI/Telnet/SSH interface.
2. The System Name field is also used by DHCP whenever the hostname within VLAN DHCP configuration field is left blank.

System Location - The physical location of this unit. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

9.2 SNMP- SNMPv2-v3 configuration



SNMPv2,v3 Configuration

Note: Press on the ? image to the right for detailed SNMPv2,v3 configuration example ?

Press ? to view detailed configuration example document

SNMP View OiD-Range Configuration

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

SNMP Community Configuration

Delete	Community name	Community secret	Source IP	Source Prefix
□	public	public	0.0.0.0	0
□	private	private	0.0.0.0	0

SNMP Group Configuration

Note: SNMPv3 user must be configured before SNMPv3 security model can be added.

Delete	Security Model	v2 community / v3 user	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group

SNMP Access Configuration

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

Figure 9-2: SNMPv2-v3 Configuration

9.2.1 SNMP View OiD-Range Configuration

Configures which SNMP OiDs should be included/excluded from the entire SNMP OiD tree.

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

View Name - A string name identifying the view OiD branch to be included/excluded. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

View Type - Indicates if the named OiD branch should be included/excluded from the entire MIB OiD tree.

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(*).

9.2.2 SNMP Community Configuration

Configures SNMP community table used as part of SNMP Group Configuration. Entry index key is Community name.

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

Community Name - Indicates the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Community secondsret - Indicates the community secret (access string) to permit access using SNMPv1 and SNMPv2c to the SNMP agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

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 prefix.

Source Prefix - Indicates the SNMP access source address prefix.

9.2.3 SNMP Group Configuration

Configures SNMP group-name table based on *secondsurity Model* and *secondsurity Name*.

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

secondsurity Model - Indicates the security model that this entry should belong to. Possible security models are: SNMPv1, SNMPv2C, SNMPv3

V2 community / V3 user - SNMPv2: One of the security names from previous stage (SNMP Community Configuration) that this entry should belong to.
SNMPv3: One of the SNMPv3 users that were already configured by the help of SNMPv3 Users page.

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.

9.2.4 SNMP Access Configuration

Configures SNMP access table. The entry index keys are *Group Name, secondsurity Model* and *secondsurity Level***.**

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

Group Name - One of the Group-Name strings that were configured by SNMP Group Configuration table. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

secondsurity Model - Indicates the security model that this entry should belong to. Possible security models are: Any, V1, V2c, V3

secondsurity Level - Indicates the security model that this entry should belong to. Possible security models are:

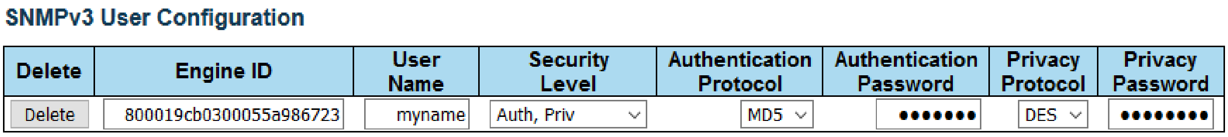
- **NoAuth, NoPriv**: No authentication and no privacy.
- **Auth, NoPriv**: Authentication and no privacy.
- **Auth, Priv**: Authentication and privacy.

Read View Name - The name of the MIB view defining the MIB objects for which this request may potentially read OiD values.

Write View Name - The name of the MIB view defining the MIB objects for which this request may potentially set OiD new values.

9.2.5 SNMP- SNMPv3 Users Configuration

Configures SNMPv3 user table. The entry index keys are Engine ID and User Name.



SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete	800019cb0300055a986723	myname	Auth, Priv	MD5	•••••••	DES	••••••••

Figure 9-3: SNMPv3 User Configuration

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

Engine ID - An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-Fs are not allowed. The SNMPv3 architecture uses the User-based secondsurity 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 keys. In a simple agent, usmUserEngineID is always that agents 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 its remote user.

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

secondsurity Level - Indicates the security model that this entry should belong to. Possible security models are:

- **NoAuth, NoPriv**: No authentication and no privacy.
- **Auth, NoPriv**: Authentication and no privacy.
- **Auth, Priv**: Authentication and privacy.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol - Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

- **None:** No authentication protocol.
- **MD5:** An optional flag to indicate that this user uses MD5 authentication protocol.
- **SHA:** An optional flag to indicate that this user uses SHA authentication protocol. The value of the security level cannot be modified if an entry already exists. That means must first ensure that the value is set correctly.

Authentication Password - A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

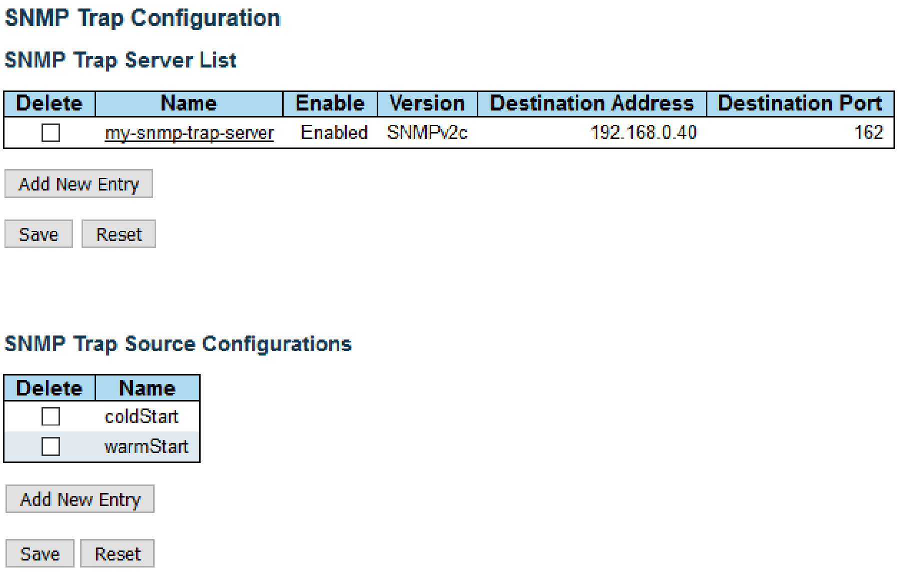
Privacy Protocol - Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

- **None:** No privacy protocol**.**
- **DES:** An optional flag to indicate that this user uses DES authentication protocol**.**
- **AES:** An optional flag to indicate that this user uses AES authentication protocol.

Privacy Password - A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

9.3 SNMP- Trap Configuration

Provides a summary of the already configured SNMP Trap Servers, with the option to add/delete remote SNMP trap Servers.



SNMP Trap Configuration

SNMP Trap Server List

Delete	Name	Enable	Version	Destination Address	Destination Port
□	my-snmp-trap-server	Enabled	SNMPv2c	192.168.0.40	162

SNMP Trap Source Configurations

Delete	Name
□	coldStart
□	warmStart

Figure 9-4: SNMP Trap Configuration

9.3.1 SNMP Trap Server List

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

Name - Every raw at the table has its own unique name.

Enable - Offers the option to keep SNMP Trap-Server record inside the table without necessary sending SNMP Trap to the SNMP Trap Server.

- **Enabled:** Send SNMP Trap to the IP address of the remote SNMP Trap-Server.
- **Disabled:** Keep SNMP Trap-Server record, without sending any traps to it.

Version - Indicates the type of SNMP trap version should be sent. The following options are **available:**

- **SNMPv1**: Send SNMP trap in SNMPv1 format.
- **SNMPv2c**: Send SNMP trap in SNMPv2c format.
- **SNMPv3**: Send SNMP trap in SNMPv3 format.

Destination Address - IPv4 or IPv6 or hostname (for example: my.server.com) address of remote SNMP Trap-Server. Valid hostname should be made of 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.

Destination port - Indicates the SNMP trap UDP destination port. The default value should be UDP port 162. Valid UDP port range is 1~65535.

9.3.2 SNMP Trap Source Configuration

Provides a list for all the events that may cause SNMP trap to be sent.

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

Name - Indicates the name of the event that will case SNMP trap to be sent. Possible options are:

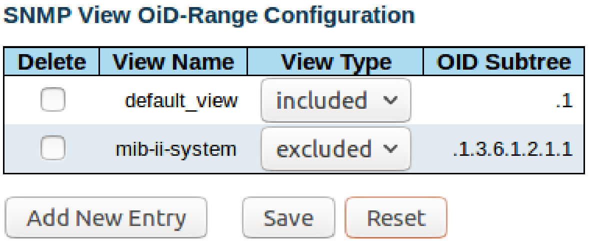
- **coldStart**: Unit up after power was applied to the unit.
- **warmStart**: SNMP was enabled in run time
- **linkUp**: Ethernet Link is up.
- **linkDown**: Ethernet Link is down
- **authenticationFailure**: Remote SNMP client was trying to access the unit using invalid username/pass values.
- **newRoot**: MSTP Spanning Tree Root was changed.
- **topologyChange**: network topology was changed.
- lldpRemTablesChange:

9.4 SNMP- Configuration example

9.4.1 SNMPv2 Configuration Example

Enabling SNMP is the only step required to enable SNMPv2 with default SNMPv2 configuration (using public/private community strings). The example bellow uses slightly different configuration strings for better description of the procedure to configure SNMPv2.

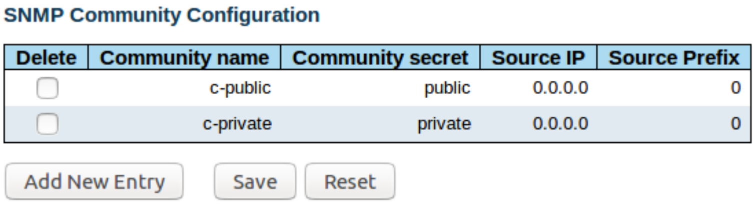
- Use default (.1) to allow the user access to all SNMP OiD or create your own **SNMP View OiD-Range,** limiting the user access to specific OiD. In the example the user has access to all SNMP OiD except for MIB-II system branch .1.3.6.1.2.1.1



SNMP View OiD-Range Configuration

Delete	View Name	View Type	OID Subtree
☐	default_view	included	.1
☐	mib-ii-system	excluded	.1.3.6.1.2.1.1

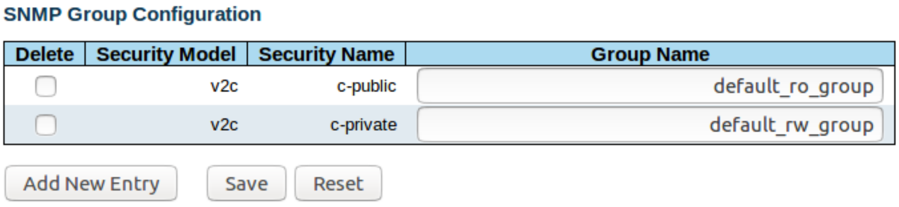
- Modify/create public/private community strings. Please note that the **Community name** field is just a reference to the **Community secondsret** password field



SNMP Community Configuration

Delete	Community name	Community secret	Source IP	Source Prefix
☐	c-public	public	0.0.0.0	0
☐	c-private	private	0.0.0.0	0

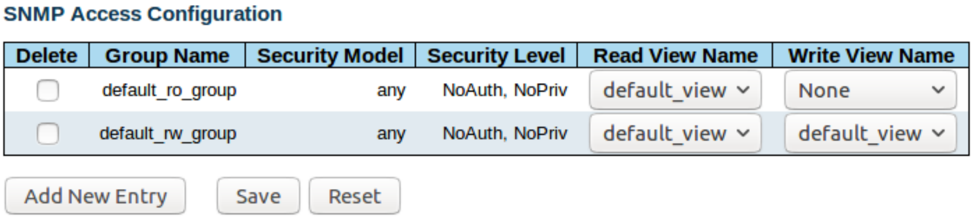
- Modify/create two groups using SNMPv2c security model and link them to the community name created in the previous step.



SNMP Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v2c	c-public	default_ro_group
☐	v2c	c-private	default_rw_group

- Modify/create **Access** configuration list to the groups created in the previous step.

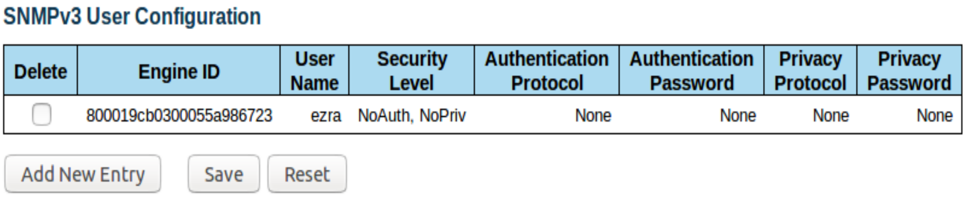


SNMP Access Configuration

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

9.4.2 SNMPv3 Configuration Example

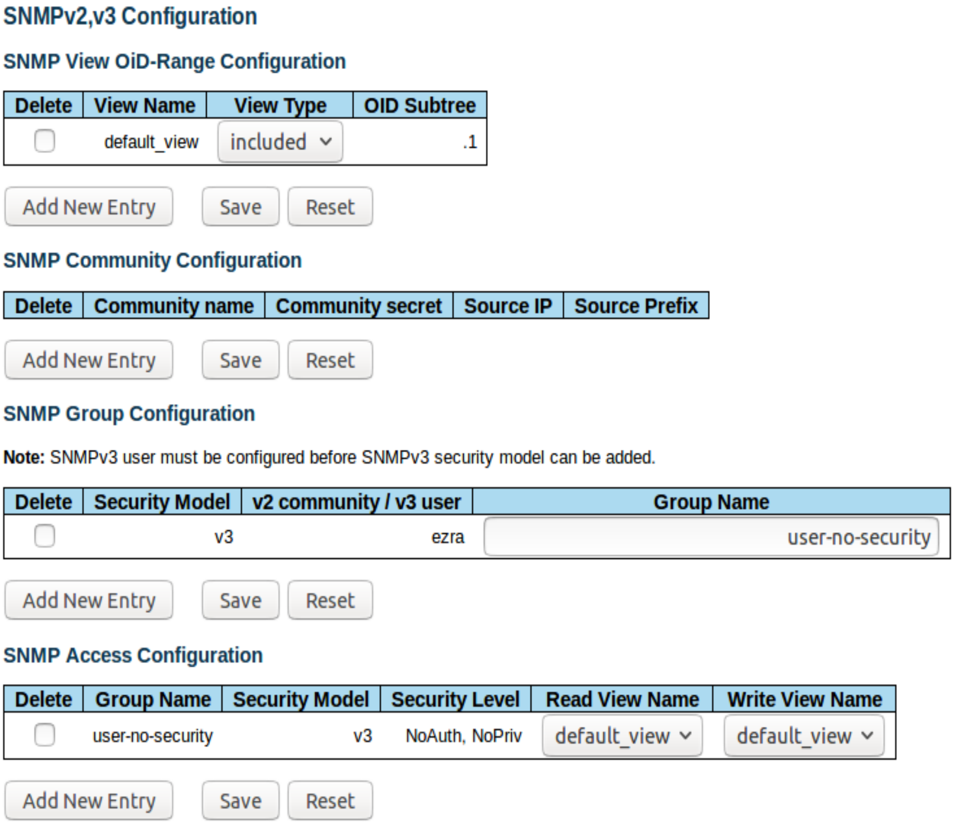
- Configure SNMPv3 user



SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	800019cb0300055a986723	ezra	NoAuth, NoPriv	None	None	None	None

- Remove SNMPv1, v2 from “group configuration”
- Add SNMPv3 security model, and assign to it a group name
- Add to “ANMP Access Configuration” the group name from previous stage, with security Level of SNMPv3, and assign to it the desired read/write options



SNMPv2,v3 Configuration

SNMP View OiD-Range Configuration

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

SNMP Community Configuration

Delete	Community name	Community secret	Source IP	Source Prefix

SNMP Group Configuration

Note: SNMPv3 user must be configured before SNMPv3 security model can be added.

Delete	Security Model	v2 community / v3 user	Group Name
□	v3	ezra	user-no-security

SNMP Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	user-no-security	v3	NoAuth, NoPriv	default_view	default_view

10 RADIUS, TACACS+

10.1 General

RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access Control System) are networking protocols that provide centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect to the unit over Web, telnet, SSH. The remote username and password are sent to RADIUS/TACACS+ Server for authentication (user + password match/do not match) and authorization (privilege level) rather than being tested locally using unit local configuration file.

NOTE:

RADIUS/TACACS+ configuration only will have no effect on remote user authentication over Web, Telnet, SSH. To complete the configuration user must configure also *authentication method* located under: Access Control→Telnet/SSH/Web

10.1.1 General - Authentication, Access-Level terminology

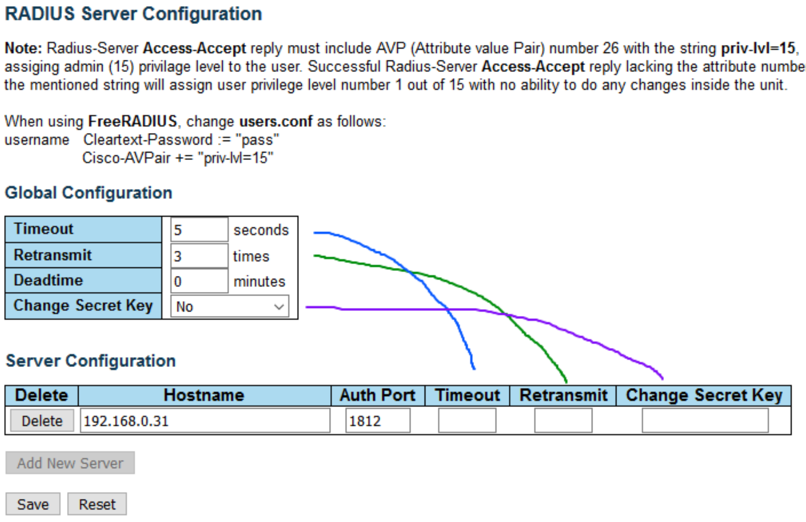
- **Authentication** - Remote username and password is sent to RADIUS-Server for authentication instead of tested locally by the unit. The RADIUS-Server determines if remote user should be accepted or rejected.
- **Access-Level** - Remote user access-level is determined by the RADIUS-Server. For normal unit operation, all remote users should obtain access level 15 (administrator) by remote RADIUS-Server.

10.1.2 General - Setting up remote RADIUS Server

- Successful RADIUS Server configuration must include two steps. The first step is to configure RADIUS Server to acknowledge remote user username and password. The second step is configuring the RADIUS Server so that RADIUS-Server *Access-Accept* reply message will include AVP (Attribute value Pair) number 26 with the string *priv-lvl=15*, assigning admin (15) privilege level to the user. Successful Radius-Server *Access-Accept* reply lacking the attribute number 26 with the mentioned string will assign user privilege level number 1 out of 15 with no ability to do any changes inside the unit.
- Configuring Free-Radius users.conf configuration file:
  Change **users.conf** as follows:

```
username   Cleartext-Password := "pass"
           Cisco-AVPair += "priv-lvl=15"
```

10.2 RADIUS TACACS+ - Configuration - RADIUS



RADIUS Server Configuration

Note: Radius-Server **Access-Accept** reply must include AVP (Attribute value Pair) number 26 with the string **priv-lvl=15**, assiging admin (15) privilage level to the user. Successful Radius-Server **Access-Accept** reply lacking the attribute number 26 with the mentioned string will assign user privilege level number 1 out of 15 with no ability to do any changes inside the unit.

When using **FreeRADIUS**, change **users.conf** as follows:

```
username   Cleartext-Password := "pass"
           Cisco-AVPair += "priv-lvl=15"
```

Global Configuration

Timeout	5 seconds
Retransmit	3 times
Deadtime	0 minutes
Change Secret Key	No

Server Configuration

Delete	Hostname	Auth Port	Timeout	Retransmit	Change Secret Key
Delete	192.168.0.31	1812			

Figure 10-1: RADIUS Configuration

10.2.1 Global Configuration

The global configuration section contains all RADIUS default values to be used whenever a user adds new RADIUS-Server and leaves identical fields blank.

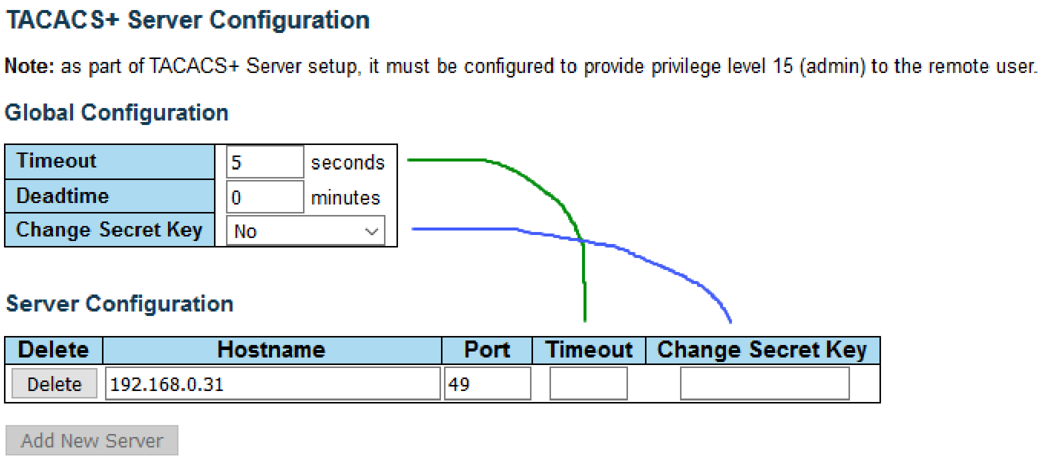
- **Timeout** - Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
- **Retransmit** - Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.
- **Deadtime** - Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request (dead). This should 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.
- **Change secondsret Key** - Specify to change the secret key or not. When "Yes" is selected for the option, you can change the secret key - up to 63 characters long - shared between the RADIUS server and the switch.

10.2.2 Server Configuration

- **Delete** - Check this box to delete a RADIUS server entry. The entry will be deleted during the next Save.
- **Hostname** - The IPv4/IPv6 addressor hostname of the RADIUS server.
- **Auth Port** - The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.
- **Timeout** - This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
- **Retransmit** - This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

- **Change secondsret Key** - Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.

10.3 RADIUS TACACS+ - Configuration – TACACS+



TACACS+ Server Configuration

Note: as part of TACACS+ Server setup, it must be configured to provide privilege level 15 (admin) to the remote user.

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Change Secret Key	No	

Server Configuration

Delete	Hostname	Port	Timeout	Change Secret Key
Delete	192.168.0.31	49		

Figure 10-2: TACACS+ Configuration

10.3.1 Global Configuration

The global configuration section contains all TACACS+ default values to be used whenever a user adds new TACACS+ Server and leaves identical fields blank.

- **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.

NOTE:
Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured

- **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 (dead). This should stop the switch from continually trying to contact a server that it has already determined as dead.
- **Change secondsret Key** - Specify to change the secret key or not. When "Yes" is selected, you can change the secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

10.3.2 Server Configuration

- **Delete** - Check this box to delete a TACACS+ server entry. The entry will be deleted during the next Save.
- **Hostname** - The IPv4/IPv6 addressor hostname of the TACACS+ server.
- **Port** - The TCP port to use on the TACACS+ server for authentication.
- **Timeout** - This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
- **Change secondsret Key** - Specify to change the secret key or not. When the checkbox is checked you can change the setting overrides the global key. Leaving it blank will use the global key.

10.4 RADIUS TACACS+ - View – RADIUS Status

This Page provides an overview of the status of the RADIUS servers that were configured. Pressing on the RADIUS Server index number will show detailed statistics for this specific RADIUS Server.

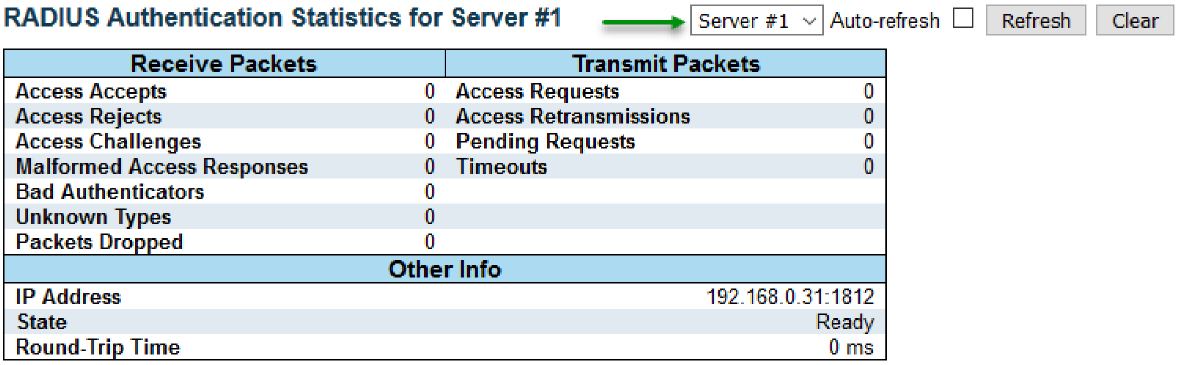
- **# -** Press the index number (1-5) for a detailed RADIUS status statistics report.
- **IP Address -** The IP address of the RADIUS Server that was configured.
- **Authentication Port -** The RADIUS Server UDP port number used for authentication.
- **Authentication Status -** The current status of the RADIUS server. This field takes one of the following values:
  - **Disabled** - RADIUS server is disabled.
  - **Not Ready** - RADIUS server is enabled, but IP communication is not yet up and running.
  - **Ready** - RADIUS server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
  - **Dead (X seconds left)** - RADIUS-Server fails to reply to authentication requests (timeout) and was placed in Dead state for Dead-time minutes. This should speed up future remote user access by skipping on **timeout x retry** waiting delay (in seconds) before switching to next (backup) Radius-Server. The Server will be re-enabled after dead-time expires.

NOTE:

Dead state is applicable only when there is more than one RADIUS-server, and dead-time time value is greater than 0

10.5 RADIUS TACACS+ - View – RADIUS Details

This page provides detailed statistics for a particular RADIUS server.



RADIUS Authentication Statistics for Server #1

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	192.168.0.31:1812
State	Ready
Round-Trip Time	0 ms

Figure 10-3: RADIUS Authentication Statistics

10.5.1 Packet Counters

Tx Rx	Name	RFC4668 Name	Description
	Access Accepts	radiusAuthClientExtAccessAccepts	RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	Access Rejects	radiusAuthClientExtAccessRejects	RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	Access Challenges	radiusAuthClientExtAccessChallenges	RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	Malformed Access Responses	radiusAuthClientExtMalformed AccessResponses	RADIUS malformed Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes.
Rx	Bad Authenticators	radiusAuthClientExtBadAuthenticators	RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	Unknown Types	radiusAuthClientExtUnknownTypes	RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	Packets Dropped	radiusAuthClientExtPacketsDropped	RADIUS packets that were received from the server on the authentication

Tx Rx	Name	RFC4668 Name	Description
			port and dropped for some other reason.
Tx	Access Requests	radiusAuthClientExtAccessRequests	RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	Access Retransmissions	radiusAuthClientExtAccessRetransmissions	RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	Pending Requests	radiusAuthClientExtPendingRequests	RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx	Timeouts	radiusAuthClientExtTimeouts	RADIUS authentication timeouts to the server. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
---	Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (mseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that round-trip communication hasn’t been established with the server yet.

Table 10-1: Packet Counters

10.5.2 Other Info (RADIUS-Server IP address and state)

Name	Description
IP Address	IP address and UDP port for the RADIUS-server.
State	The current status of the RADIUS server. This field takes one of the following values: Disabled: RADIUS server is disabled. Not Ready: RADIUS server is enabled, but IP communication is not yet up and running. Ready: RADIUS server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): RADIUS-Server failed to reply to authentication requests (timeout) and was placed in Dead state for Dead-time minutes. This should speed up future remote user access by skipping on timeout x retry waiting delay (in seconds) before switching to next (backup) Radius-Server. The Server will be re-enabled after dead-time expires. NOTE: Dead state is applicable only when there is more than one RADIUS-server, and dead-time time value is greater than 0.

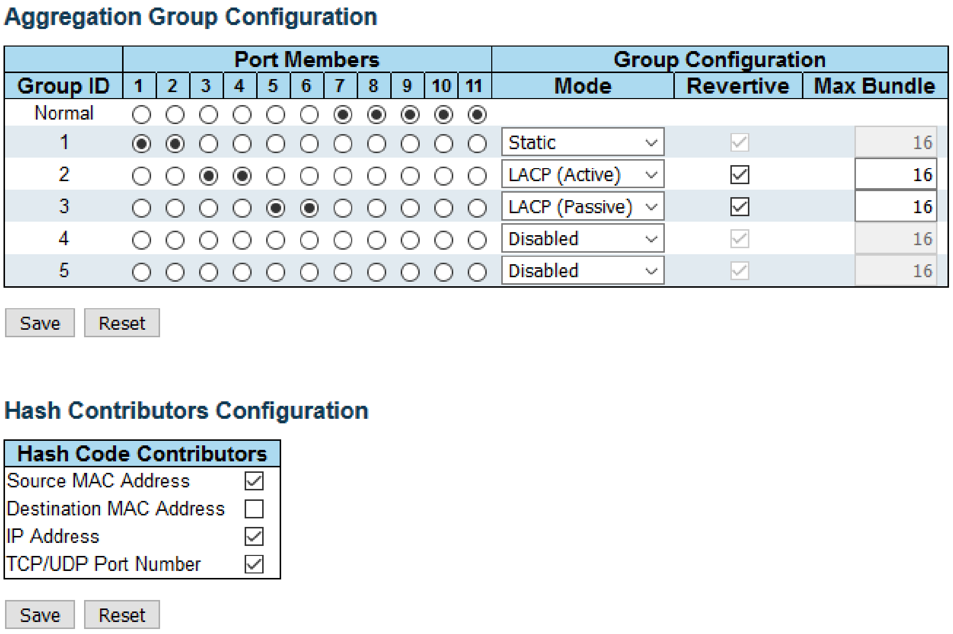
Table 10-2: Other Info

11 AGGREGATION/LACP

11.1 General

The Aggregation feature allows the user to configure aggregation as static, group and dynamic by using LACP.

11.2 Aggregation/LACP – Aggregation – Aggregation Configuration



Aggregation Group Configuration

	Port Members											Group Configuration		
Group ID	1	2	3	4	5	6	7	8	9	10	11	Mode	Revertive	Max Bundle
Normal	○	○	○	○	○	○	●	●	●	●	●			
1	●	●	○	○	○	○	○	○	○	○	○	Static	☑	16
2	○	○	●	●	○	○	○	○	○	○	○	LACP (Active)	☑	16
3	○	○	○	○	●	●	○	○	○	○	○	LACP (Passive)	☑	16
4	○	○	○	○	○	○	○	○	○	○	○	Disabled	☑	16
5	○	○	○	○	○	○	○	○	○	○	○	Disabled	☑	16

Hash Contributors Configuration

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

Figure 11-1: Aggregation Configuration

11.2.1 Aggregation Group Configuration

Group ID - Indicates the aggregation group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

Port Members - Each switch port is listed for each group ID. By default, no ports belong to any aggregation group.

- Only full duplex ports can join an aggregation
- The ports in each group must be in the same speed .

Mode - This parameter determines the mode for the aggregation group.

- **Disabled:** The group is disabled.
- **Static:** The group operates in static aggregation mode.
- **LACP (Active):** The group operates in LACP active aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.
- **LACP (Passive):** The group operates in LACP passive aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.

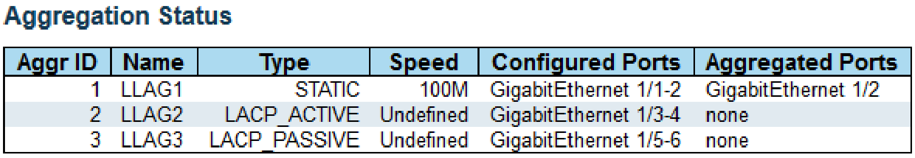
Revertive - This parameter only applies to LACP-enabled groups. It determines if the group will perform automatic link (re-)calculation when links with higher priority become available.

Max Bundle - This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation.

11.2.2 Hash Contributors Configuration

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

11.3 Aggregation Status



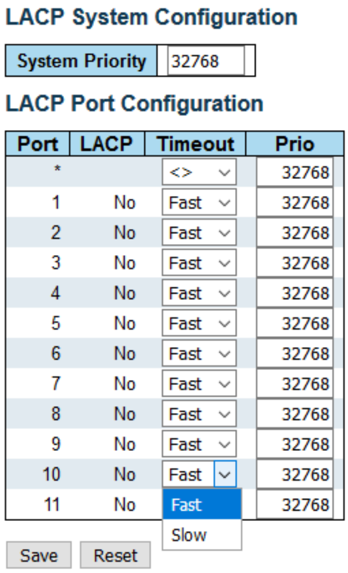
Aggregation Status

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
1	LLAG1	STATIC	100M	GigabitEthernet 1/1-2	GigabitEthernet 1/2
2	LLAG2	LACP_ACTIVE	Undefined	GigabitEthernet 1/3-4	none
3	LLAG3	LACP_PASSIVE	Undefined	GigabitEthernet 1/5-6	none

Figure 11-2: Aggregation Status

- **Aggr ID** - The Aggregation ID associated with this aggregation instance.
- **Name** - Name of the Aggregation group ID.
- **Type** - Type of the Aggregation group (Static or LACP).
- **Speed** - Speed of the Aggregation group.
- **Configured ports** - Configured member ports of the Aggregation group.
- **Aggregated ports** - Aggregated member ports of the Aggregation group.

11.4 Aggregation/LACP - LACP- Configure LACP



LACP System Configuration

System Priority	32768

LACP Port Configuration

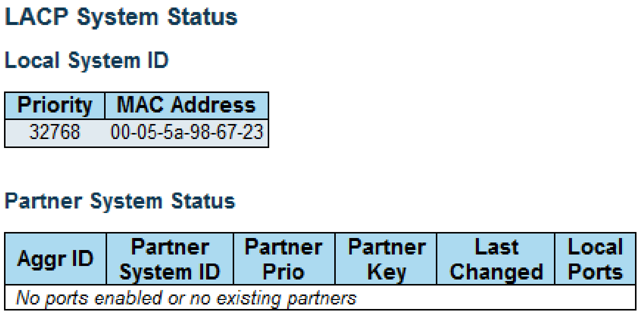
Port	LACP	Timeout	Prio
*		<>	32768
1	No	Fast	32768
2	No	Fast	32768
3	No	Fast	32768
4	No	Fast	32768
5	No	Fast	32768
6	No	Fast	32768
7	No	Fast	32768
8	No	Fast	32768
9	No	Fast	32768
10	No	Fast	32768
11	No	Fast	32768

Figure 11-3: LACP Configuration

- **Port** - The switch port number.
- **LACP** - Show whether LACP is currently enabled on this switch port.
- **Timeout** - The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.
- **Prio** - The Priority controls the priority of the port, range 1-65535. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

11.5 Aggregation/LACP – LACP – View – System Status

This Page provides a status overview for the system-level LACP information.



LACP System Status

Local System ID

Priority	MAC Address
32768	00-05-5a-98-67-23

Partner System Status

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

Figure 11-4: View LACP System Status

11.5.1 Local System ID

This table displays both the local system priority and the local system MAC address which forms the local LACP System ID.

11.5.2 Partner System Status

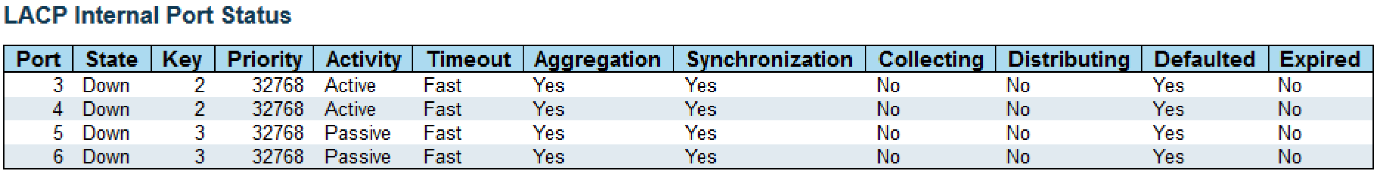
This table display the partner system information for each LACP aggregation group.

Aggr ID - The Aggregation ID associated with this aggregation instance.

- **Partner System ID** - The system ID (MAC address) of the aggregation partner.
- **Partner Prio** - The priority that the partner has assigned to this aggregation ID.
- **Partner Key** - The key that the partner has assigned to this aggregation ID.
- **Last changed** - The time since this aggregation changed.
- **Local Ports** - Shows which ports are a part of this aggregation for this switch.

11.6 Aggregation/LACP – LACP – View – Internal Status

This Page provides a status overview for the LACP internal (i.e. local system) status for all ports. Only ports that are part of an LACP group are shown.



LACP Internal Port Status

Port	State	Key	Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
3	Down	2	32768	Active	Fast	Yes	Yes	No	No	Yes	No
4	Down	2	32768	Active	Fast	Yes	Yes	No	No	Yes	No
5	Down	3	32768	Passive	Fast	Yes	Yes	No	No	Yes	No
6	Down	3	32768	Passive	Fast	Yes	Yes	No	No	Yes	No

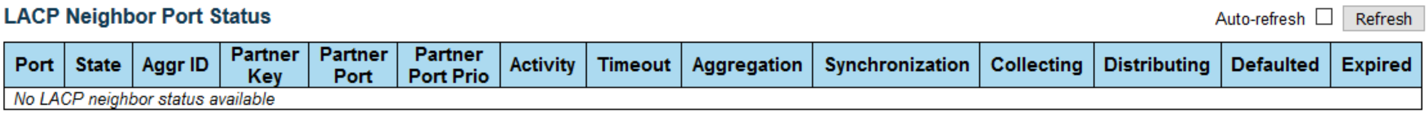
Figure 11-5: View LACP Internal Port Status

- **Port** - The switch port number.
- **State** - The current port state:
- **Down** - The port is not active.
- **Active** - The port is in active state.
- **Standby** - The port is in standby state.
- **Key** - The key assigned to this port. Only ports with the same key can aggregate together.
- **Priority** - The priority assigned to this aggregation group.
- **Activity** - The LACP mode of the group (Active or Passive).
- **Timeout** - The timeout mode configured for the port (Fast or Slow).
- **Aggregation** - Shows whether the system considers this link to be "aggregateable"; i.e., a potential candidate for aggregation.
- **Synchronization** - Shows whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.
- **Collecting** - Shows if collection of incoming frames on this link is enabled.
- **Distributing** - Shows if distribution of outgoing frames on this link is enabled.

- **Defaulted** - Shows if the Actors Receive machine is using Defaulted Operational Partner information.
- **Expired** - Shows if that the Actors Receive machine is in the EXPIRED state.

11.7 Aggregation/LACP – LACP – View – Neighbor Status

This page provides a status overview for the LACP neighbor status for all ports. Only ports that are part of an LACP group are shown



LACP Neighbor Port Status

Auto-refresh □ Refresh

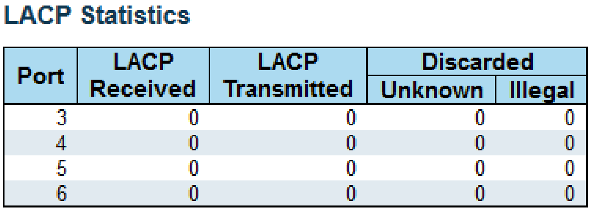
Port	State	Aggr ID	Partner Key	Partner Port	Partner Port Prio	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
No LACP neighbor status available													

Figure 11-6: View LACP Neighbor Port Status

- **Port** - The switch port number.
- **State** - The current port state:
- **Down** - The port is not active.
- **Active** - The port is in active state.
- **Standby** - The port is in standby state.
- **Aggr ID** - The aggregation group ID which the port is assigned to.
- **Partner Key** - The key assigned to this port by the partner.
- **Partner Port** - The partner port number associated with this link.
- **Partner Port Priority** - The priority assigned to this partner port .
- **Activity** - The LACP mode of the group (Active or Passive).
- **Timeout** - The timeout mode configured for the partner port (Fast or Slow).
- **Aggregatio**n - Shows whether the partner considers this link to be "aggregateable"; i.e., a potential candidate for aggregation.
- **Synchronization** - Shows whether the partner considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.
- **Collecting** - Shows if collection of incoming frames on this link is enabled.
- **Distributing** - Shows if distribution of outgoing frames on this link is enabled.
- **Defaulted** - Shows if the partners Receive machine is using Defaulted Operational Partner information.
- **Expired** - Shows if that the partners Receive machine is in the EXPIRED state.

11.8 Aggregation/LACP – LACP – View – Port Statistics

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



LACP Statistics

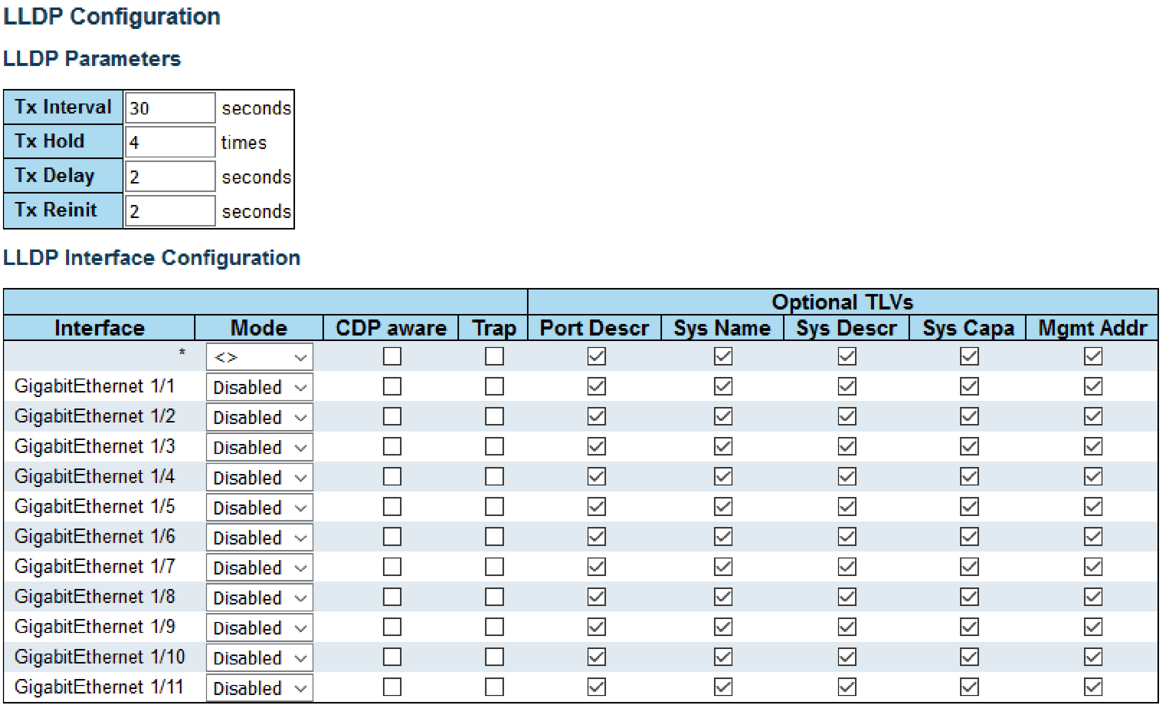
Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0

Figure 11-7: View LACP Port Statistics

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

12 LLDP

12.1 LLDP – Configure LLDP



LLDP Configuration

LLDP Parameters

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

LLDP Interface Configuration

				Optional TLVs				
Interface	Mode	CDP aware	Trap	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Disabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/2	Disabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Disabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Disabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/5	Disabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/6	Disabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/7	Disabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/8	Disabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/9	Disabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/10	Disabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/11	Disabled	□	□	☑	☑	☑	☑	☑

Figure 12-1: LLDP Configuration

12.1.1 LLDP Parameters

- **Tx Interval** - The switch periodically transmits LLDP frames to its neighbors to update the network discovery information. The interval between the LLDP frames is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds.
- **Tx Hold** - Each LLDP frame contains information that determines how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. Valid values are restricted to 2 - 10 times.
- **Tx Delay** - If a configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds.
- **Tx Reinit** - When an interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information is not valid anymore. **Tx Reinit** controls the number of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

12.1.2 LLDP Interface Configuration

- **Interface** - The name of the switch's logical LLDP interface.
- **Mode** - Select LLDP mode.
  - **Rx only:** The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.

- **Tx only:** The switch will drop LLDP information received from neighbors, but will send out LLDP information.
- **Disabled:** The switch will not send out LLDP information, and will drop LLDP information received from neighbors.
- **Enabled:** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

- **CDP Aware** - Select CDP awareness.
  The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the interface 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.

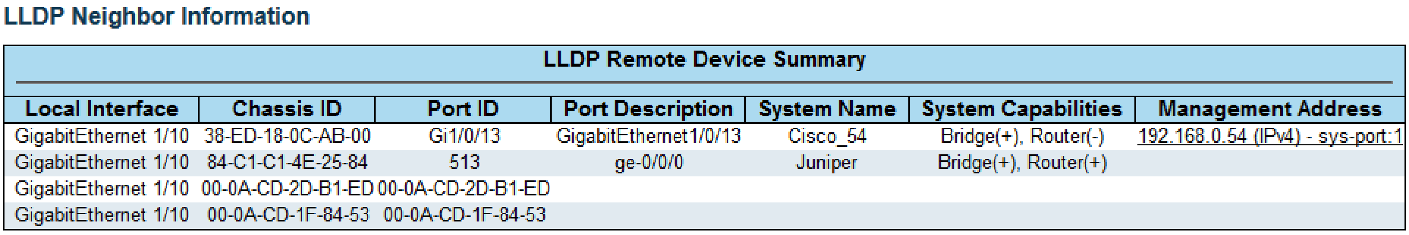
If all interfaces have CDP awareness disabled, the switch forwards CDP frames received from neighbor devices. If at least one interface has CDP awareness enabled all CDP frames are terminated by the switch.

NOTE:
When CDP awareness on an interface is disabled, the CDP information is not removed immediately, but gets removed when the hold time is exceeded

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

12.2 LLDP – View Neighbor Information

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



LLDP Neighbor Information

LLDP Remote Device Summary

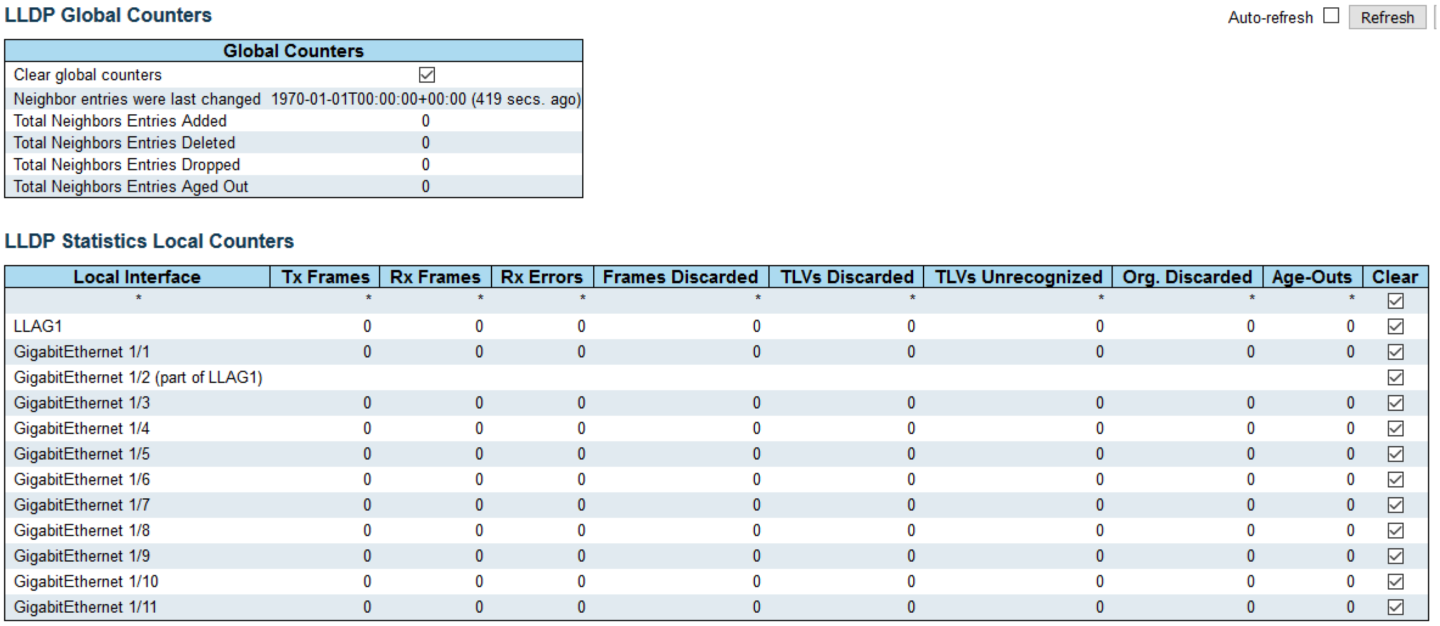
Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
GigabitEthernet 1/10	38-ED-18-0C-AB-00	Gi1/0/13	GigabitEthernet1/0/13	Cisco_54	Bridge(+), Router(-)	192.168.0.54 (IPv4) - sys-port:1
GigabitEthernet 1/10	84-C1-C1-4E-25-84	513	ge-0/0/0	Juniper	Bridge(+), Router(+)	
GigabitEthernet 1/10	00-0A-CD-2D-B1-ED	00-0A-CD-2D-B1-ED				
GigabitEthernet 1/10	00-0A-CD-1F-84-53	00-0A-CD-1F-84-53				

Figure 12-2: LLDP Neighbor

- **Local Interface** - The interface on which the LLDP frame was received.
- **Chassis ID** - The identification of the neighbors LLDP frames.
- **Port ID** - The identification of the neighbor port.
- **Port Description** - The port description advertised by the neighbor unit.
- **System Name** - The name advertised by the neighbor unit.
- **System Capabilities** - Describes the neighbor units capabilities. Enabled capability is followed by (+) and disabled capability is followed by (-). The possible capabilities are:
    - Other
    - Repeater
    - Bridge
    - WLAN Access Point
    - Router
    - Telephone
    - DOCSIS cable device
    - Station only
    - Reserved
- **Management Address** - The neighbor units address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbors IP address.

12.3 LLDP – View LLDP Status

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 interface counters for the currently selected port.



LLDP Global Counters

Global Counters	
Clear global counters	☑
Neighbor entries were last changed	1970-01-01T00:00:00+00:00 (419 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 Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
*	*	*	*	*	*	*	*	*	☑
LLAG1	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/2 (part of LLAG1)									☑
GigabitEthernet 1/3	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/4	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/5	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/6	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/7	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/8	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/9	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/10	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/11	0	0	0	0	0	0	0	0	☑

Figure 12-3: View LLDP Status

12.3.1 Global Counters

- **Clear global counters** - If checked the global counters are cleared when Clear is pressed.
- **Neighbor entries were last changed** - Shows the time when the last entry was deleted or added. It also shows the time elapsed since the last change was detected.
- **Total Neighbors Entries Added** - Shows the number of new entries added since switch reboot.
- **Total Neighbors Entries Deleted** - Shows the number of new entries deleted since switch reboot.
- **Total Neighbors Entries Dropped** - Shows the number of LLDP frames dropped due to the entry table being full.
- **Total Neighbors Entries Aged Out** - Shows the number of entries deleted due to Time-To-Live expiring.

12.3.2 Local Counters

- **Local Interface** - The interface on which LLDP frames are received or transmitted.
- **Tx Frames** - The number of LLDP frames transmitted on the interface.
- **Rx Frames** - The number of LLDP frames received on the interface.
- **Rx Errors** - The number of received LLDP frames containing some kind of error.
- **Frames Discarded** - If an LLDP frame is received on a interface, 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 interfaces link is down, an LLDP shutdown frame is received, or when the entry ages out.

- **TLVs Discarded** - Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
- **TLVs Unrecognized** - The number of well-formed TLVs, but with an unknown type value.
- **Org. Discarded** - If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.
- **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.
- **Clear** - If checked, the counters for the specific interface are cleared when Clear is pressed.

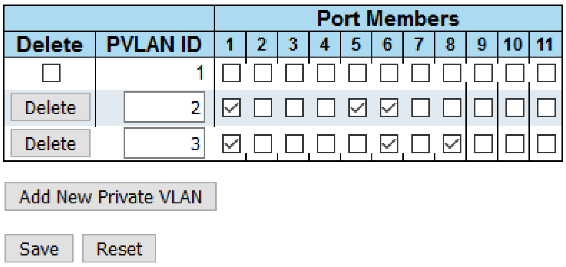
13 PORT ISOLATION

13.1 Port Isolation – Configure Private VLAN

13.1.1 General

Private VLAN **has nothing to do with traditional VLANs**, meaning that Private-VLAN ID can be identical to VLAN-ID.
Private-VLAN filters outgoing destination port traffic. Packet received on port X can be sent only to destination ports which are marked as part of port X group, **considering multiple PVLAN-ID table rows configuration (union)**.
Private-VLAN does not affect unit management over IP.

Example - PVLAN-ID2 = marked ports 1,5,6. PVLAN-ID3 = marked ports 1,6,8. All other ports are unchecked.
As a result, ports-2,3,4,7,9,10,11 will not send any outgoing packets except for packets created internally.
incoming traffic on port 1 will be sent only to ports 5,6,8.
Incoming traffic on port 5 will be sent only to ports 1,6.
Incoming traffic on port 6 will be sent to ports 1,5,8
Incoming traffic on port 8 will be sent to ports 1,6



		Port Members										
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11
□	1	□	□	□	□	□	□	□	□	□	□	□
Delete	2	☑	□	□	□	☑	☑	□	□	□	□	□
Delete	3	☑	□	□	□	□	☑	□	☑	□	□	□

Figure 13-1: Private VLAN Membership Configuration

13.1.2 Private VLAN - configuration parameters

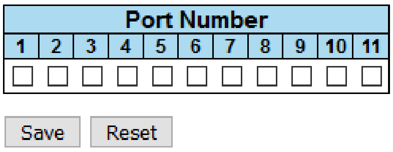
- **Delete** - To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
- **PVLAN ID** - Indicates the ID of this Private-VLAN.
- **Port Members** - Used to show/select the unit Ethernet ports assigned to be members for this specific Private-VLAN ID.

13.2 Port Isolation – Configure Port Isolation

13.2.1 General

Marked ports are prevented from sending packets to each other - isolated. However, they can communicate normally with all the other Switch ports.

Example - Marking ports 1,2 will block any traffic from port 1 to reach to port 2 and vice versa. However, each one of them can communicate normally with ports 3-11



Port Number										
1	2	3	4	5	6	7	8	9	10	11
□	□	□	□	□	□	□	□	□	□	□

Figure 13-2: Port Isolation Configuration

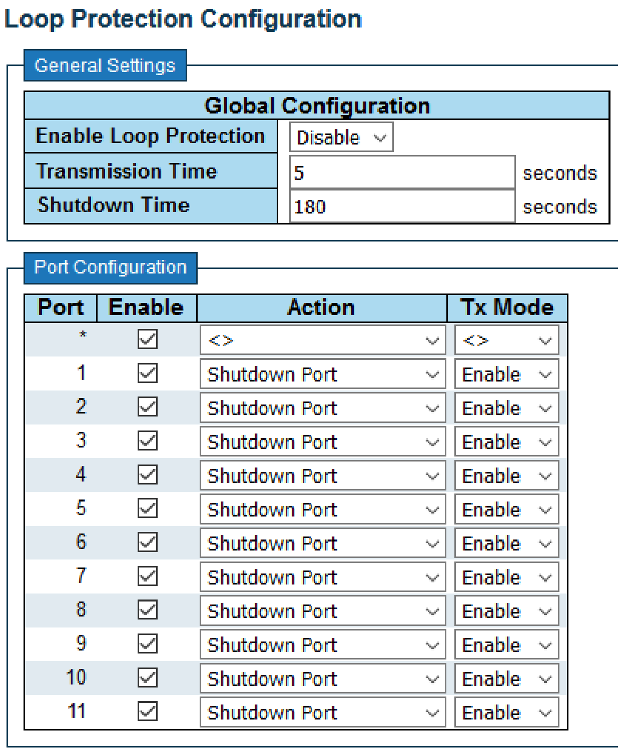
13.2.2 Port Isolation - configuration parameters

- **Port Members** - Select the ports that are not allowed to communicate with each other (isolated).

14 LOOP PROTECTION

14.1 Loop Protection – Configure Protection

This Page allows the user to inspect the current Loop Protection configurations, and change them if needed.



Loop Protection Configuration

General Settings

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

Port Configuration

Port	Enable	Action	Tx Mode
*	☑	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable
7	☑	Shutdown Port	Enable
8	☑	Shutdown Port	Enable
9	☑	Shutdown Port	Enable
10	☑	Shutdown Port	Enable
11	☑	Shutdown Port	Enable

Figure 14-1: Loop Protection Configuration

14.1.1 General Settings

- **Enable Loop Protection** - Controls whether loop protections is enabled (as a whole).
- **Transmission Time** - The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. Default value is 5 seconds.
- **Shutdown Time** - The period (in seconds) for which a port will be kept disabled in 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). Default value is 180 seconds.

14.1.2 Port Configuration

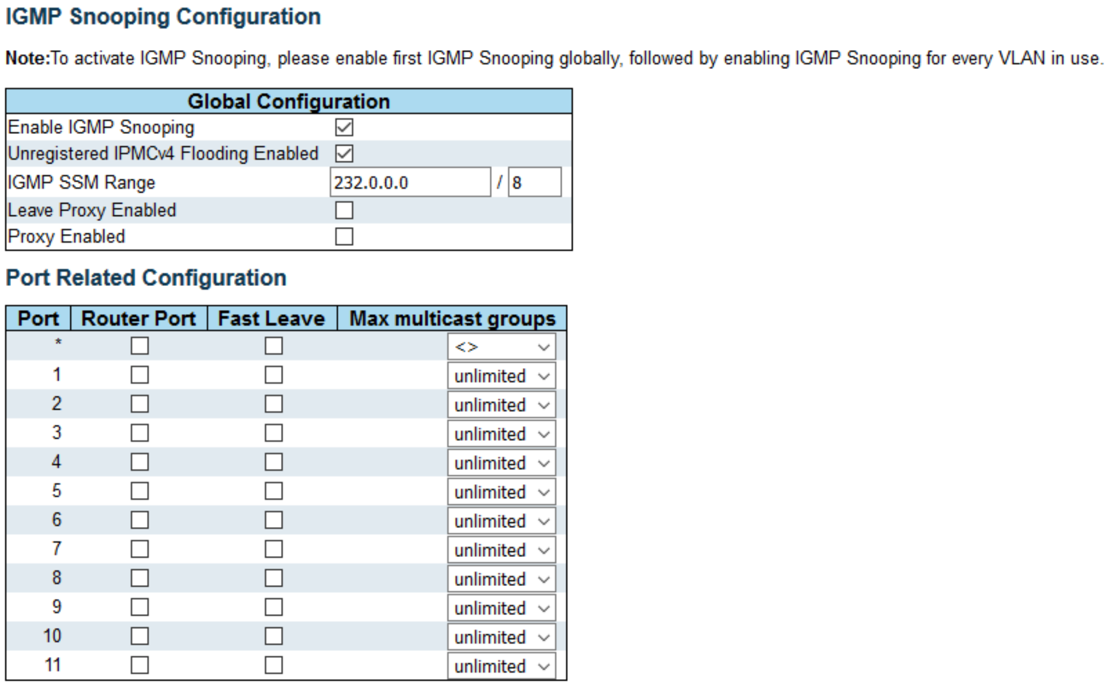
- **Port** - The switch port number of the port.
- **Enable** - Controls whether loop protection is enabled on this switch port.
- **Action** - Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.
- **Tx Mode** - Controls whether the port is actively generating loop protection PDUs, or whether it is just passively looking for looped PDUs.

15 IGMP SNOOPING

15.1 General

Snooping is the process of listening to IGMP (Internet Group Management Protocol) network traffic to control delivery of IP multicast packets. Network switches supporting IGMP snooping listen to IGMP conversation between hosts and routers and maintain a map of the ports that the IP multicast traffic should go through, while filter the IP multicast traffic from other Switch ports which do not need those IP Multicast packets, conserving bandwidth on those links.

15.2 IGMP Snooping – Configuration – Global Settings



IGMP Snooping Configuration

Note: To activate IGMP Snooping, please enable first IGMP Snooping globally, followed by enabling IGMP Snooping for every VLAN in use.

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

Port Related Configuration

Port	Router Port	Fast Leave	Max multicast groups
*	□	□	<>
1	□	□	unlimited
2	□	□	unlimited
3	□	□	unlimited
4	□	□	unlimited
5	□	□	unlimited
6	□	□	unlimited
7	□	□	unlimited
8	□	□	unlimited
9	□	□	unlimited
10	□	□	unlimited
11	□	□	unlimited

Figure 15-1: IGMP Global Settings

15.2.1 IGMP Snooping Configuration

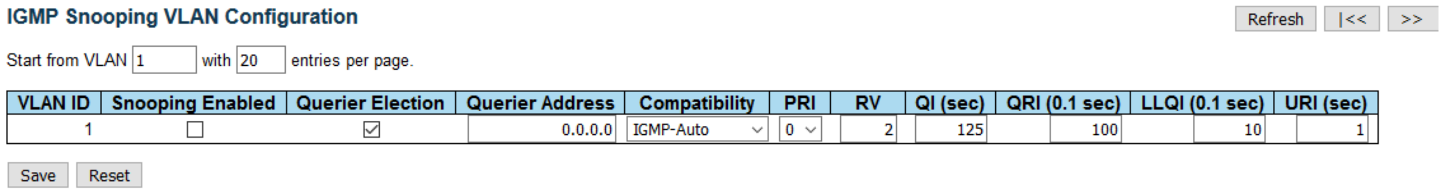
- **Enable IGMP Snooping** - Enable the Global IGMP Snooping.
- **Unregistered IPMCv4 Flooding Enabled** - Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active despite this setting.
- **IGMP SSM Range** - SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range.
- **Leave Proxy Enabled** - Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
- **Proxy Enabled** - Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

15.2.2 Port Related Configuration

- **Port** - The switch port number of the port.
- **Router Port** - Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP Querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
- **Fast Leave** - Enable the fast leave on the port. The system will remove the group record and stop forwarding data upon receiving the IGMPv2 leave message, without sending last member query messages. It is recommended to enable this feature only when a single IGMPv2 host is connected to the specific port.
- **Max multicast groups (Throttling)** - Enable to limit the number of multicast groups to which a switch port can belong, ranging from 1,2,3…10, unlimited.

15.3 IGMP Snooping – Configuration – Enable per VLAN

The user may change IGMP Snooping computability ranging from IGMPv1-v3, Auto, set Querier, etc. for the VLANs which is already configured. The page shows up to VLAN 99 entries sorted from lowest highest VLAN-ID.



IGMP Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

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

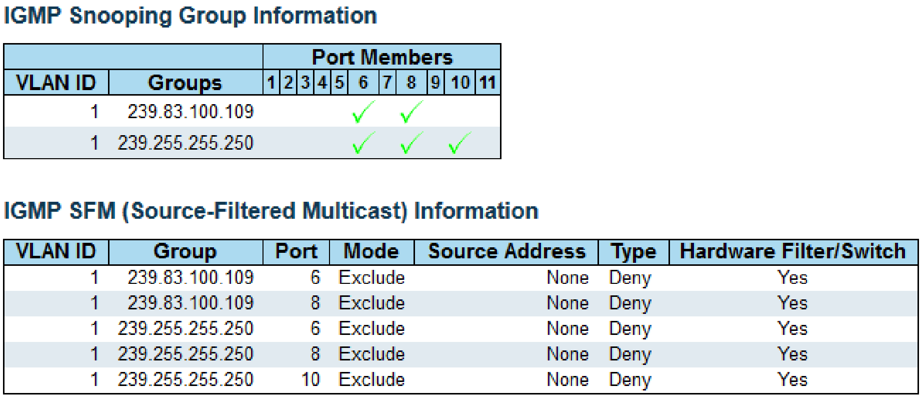
Figure 15-2: IGMP Snooping VLAN Configuration

15.3.1 IGMP Snooping Enable per VLAN

- **VLAN ID** - The VLAN ID of the entry.
- **IGMP Snooping Enabled** - Enable the per-VLAN IGMP Snooping. Up to 8 VLANs can be selected for IGMP Snooping.
- Querier Election:
  - **Enable - When enabled, the unit will send every time interval *IGMP Membership Query, General* packets, and as a result retrieve IGMP membership sent back from active members.** The reply packets from active members will cause the membership table to be updated dynamically.
  - **Disable** – Stops acting as IGMP Querier; do not send *IGMP Membership Query* packets and clear members table.
- **Querier Address** – Configures the IPv4 source address being used when transmitting IGMP Query packets.
  - **IPv4 address was set -** Uses configured IPv4 Querier Address as the source address in all transmitted *IGMP Membership Query* packets.
  - **0.0.0.0 (not set)** - uses VLAN IPv4 management address.
  - **0.0.0.0 (not set) and no VLAN IPv4 management address** – uses the first available IPv4 management address, and if there is no such IPv4 address, then uses 192.0.2.1 as default IPv4 source IP address.

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

15.4 IGMP Snooping – View – Groups Information



IGMP Snooping Group Information

		Port Members										
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11
1	239.83.100.109						✓		✓			
1	239.255.255.250						✓		✓		✓	

IGMP SFM (Source-Filtered Multicast) Information

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
1	239.83.100.109	6	Exclude	None	Deny	Yes
1	239.83.100.109	8	Exclude	None	Deny	Yes
1	239.255.255.250	6	Exclude	None	Deny	Yes
1	239.255.255.250	8	Exclude	None	Deny	Yes
1	239.255.255.250	10	Exclude	None	Deny	Yes

Figure 15-3: View IGMP Snooping Groups Information

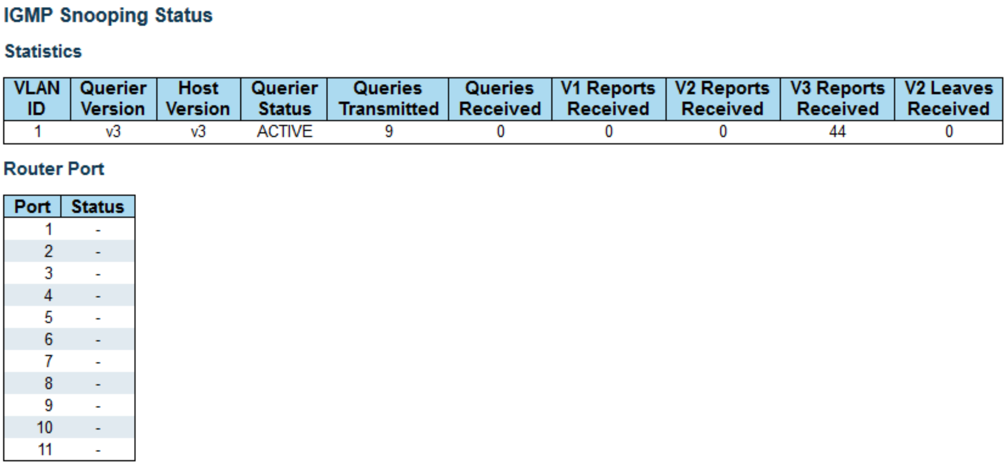
15.4.1 IGMP Snooping Group Information

- **VLAN ID** - VLAN ID of the group.
- **Groups** - Group address of the group displayed.
- **Port Members** - Ports under this group.

15.4.2 IGMP SFM (Source-Filtered Multicast) Information

- **VLAN ID** - VLAN ID of the group.
- **Group** - Group address of the group displayed.
- **Port** - Switch port number.
- **Mode** - Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either *Include* or *Exclude*. In IGMPv3, a host can send a membership report that includes a list of source addresses. When the host sends a membership report in INCLUDE mode, the host is interested in group multicast traffic only from those sources in the source address list. If a host sends a membership report in EXCLUDE mode, the host is interested in group multicast traffic from any source *except* the sources in the source address list.
  A host can also send an EXCLUDE report in which the source-list parameter is empty, which is known as an EXCLUDE NULL report. **An EXCLUDE NULL report indicates that the host wants to join the multicast group and receive packets from all sources**
- **Source Address** - IP Address of the source. Currently, the maximum number of IPv4 source address for filtering (per group) is 8. When there is no any source filtering address, the text "None" is shown in the Source Address field.
- **Type** - It can be either *Allow* or *Deny;* checking the source address of the received multicast packets, permitting or denying packets from those multicast source Addresses.
- **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.

15.5 IGMP Snooping - View - Status



IGMP Snooping Status

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
1	v3	v3	ACTIVE	9	0	0	0	44	0

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-

Figure 15-4: View IGMP Snooping Status

15.5.1 IGMP Snooping Status

- **VLAN ID** - The VLAN ID of the entry.
- **Querier Version** – Current Working Querier version.
- **Host Version** - Current Working Host version.
- **Querier Status** - Shows the Querier status as "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface, which is administratively disabled.
- **Queries Transmitted** - The number of Transmitted Queries.

- **Queries Received** - The number of Received Queries.
- **V1 Displays Received** - The number of Received V1 Displays.
- **V2 Displays Received** - The number of Received V2 Displays.
- **V3 Displays Received** - The number of Received V3 Displays.
- **V2 Leaves Received -** The number of Received V2 Leaves.

15.5.2 Router Port

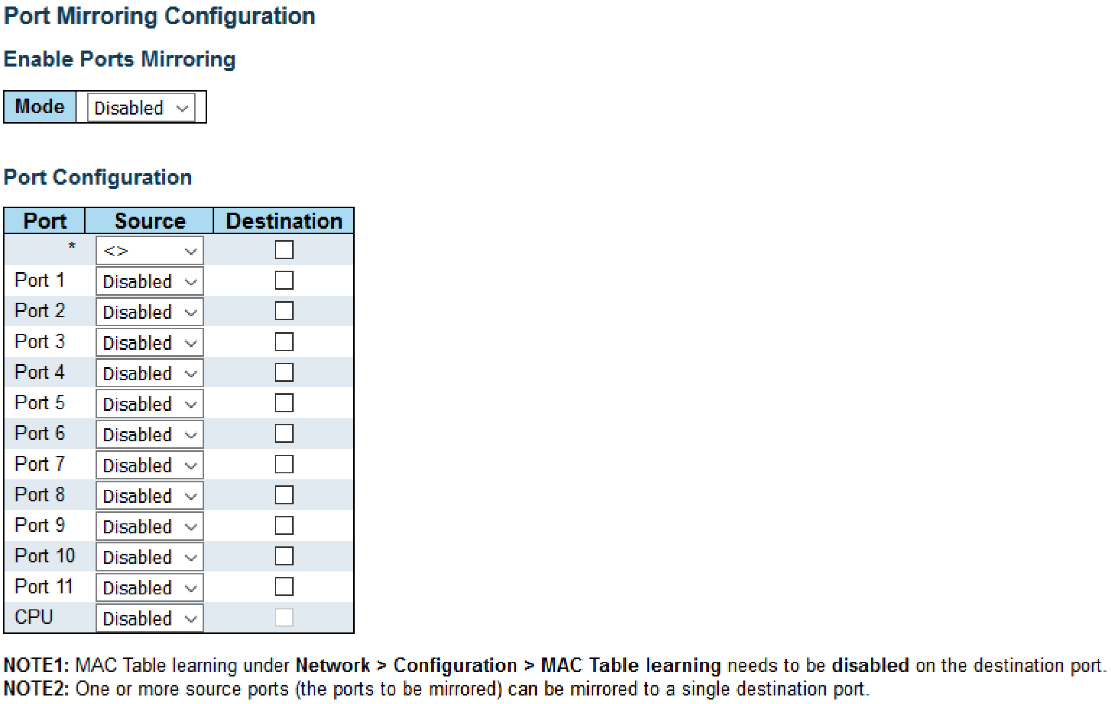
Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP Querier. *Static* means that the specific port is configured to be a router port. *Dynamic* means the specific port is learnt to be a router port. Both denote the specific configured or learnt port as a router port.

- **Port -** Switch port number.
- **Status -** Indicates whether a specific port is a router port or not.

16 PORT MIRRORING

16.1 Port Mirroring - General

Port Mirroring allows you to mirror (duplicate) Rx/Tx/Both traffic from one or more ports to another dedicated debug port, where a network analyzer can be attached to analyze the network traffic.



Port Mirroring Configuration

Enable Ports Mirroring

Mode	Disabled

Port Configuration

Port	Source	Destination
*	<>	□
Port 1	Disabled	□
Port 2	Disabled	□
Port 3	Disabled	□
Port 4	Disabled	□
Port 5	Disabled	□
Port 6	Disabled	□
Port 7	Disabled	□
Port 8	Disabled	□
Port 9	Disabled	□
Port 10	Disabled	□
Port 11	Disabled	□
CPU	Disabled	□

NOTE1: MAC Table learning under **Network > Configuration > MAC Table learning** needs to be **disabled** on the destination port.
NOTE2: One or more source ports (the ports to be mirrored) can be mirrored to a single destination port.

Figure 16-1: Port Mirroring

16.1.1 Enable Ports Mirroring

- **Mode -** Enabled/Disabled Rx/Tx/Both traffic mirroring from one or more ports to a dedicated mirroring port.

16.1.2 Port Configuration

- **Source** – Source port mirroring mode:
  - o **Disabled:** No mirroring of the traffic on this port.
  - o **Both:** Frames received and frames transmitted are mirrored on the destination port.
  - o **Rx only:** Frames received on this port are mirrored on the destination port. Frames transmitted are not mirrored.
  - o **Tx only:** Frames transmitted on this port are mirrored on the destination port. Frames received are not mirrored.

NOTE:
Multiple source ports can be mirrored to a single destination mirroring port

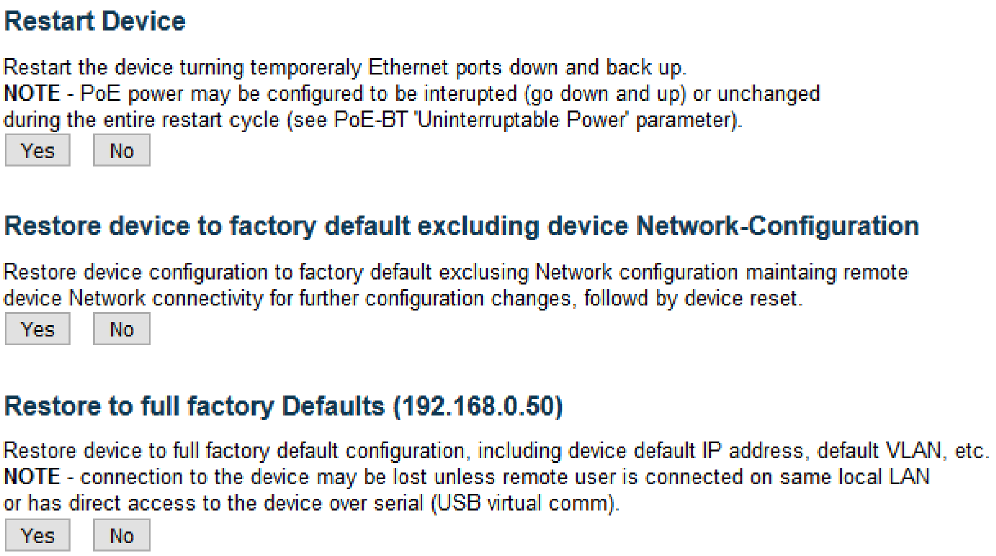
- **Destination -** The destination port will receive a copy of the traffic from the all selected source ports.

NOTE:

MAC Table learning under network > Configuration > MAC - Table learning needs to be disabled on the destination port.

17 MAINTENANCE

17.1 Maintenance - Reset & restore unit



Restart Device

Restart the device turning temporeraly Ethernet ports down and back up.
NOTE - PoE power may be configured to be interupted (go down and up) or unchanged during the entire restart cycle (see PoE-BT 'Uninterruptable Power' parameter).

Restore device to factory default excluding device Network-Configuration

Restore device configuration to factory default exclusing Network configuration maintaing remote device Network connectivity for further configuration changes, followd by device reset.

Restore to full factory Defaults (192.168.0.50)

Restore device to full factory default configuration, including device default IP address, default VLAN, etc.
NOTE - connection to the device may be lost unless remote user is connected on same local LAN or has direct access to the device over serial (USB virtual comm).

Figure 17-1: Maintenance - Reset and Restore unit

Restart Device - Performs software reset and restarts to the switch, followed by normal operation.

NOTE:
PoE power may remain unchanged, or go down and up according to the PoE Uninterruptable Power parameter configuration

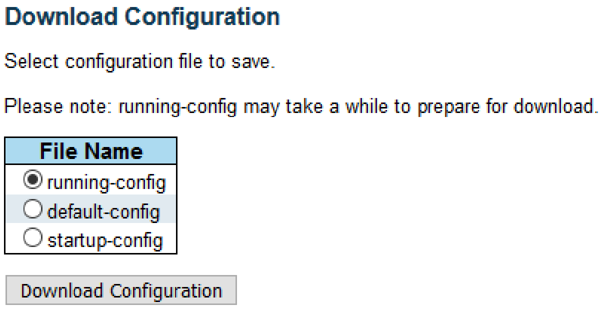
Restore device to factory Defaults excluding device network-Configuration – Restores device configuration to factory default excluding network configuration, while maintaining the emote device network connectivity for further configuration changes, followed by device reset.

Restore to full factory Defaults – Restores the device to full factory default configuration, including device default IP address, default VLAN, etc.

NOTE:
Connection to the device may be lost unless the remote user is connected on same local LAN, or has direct access to the device over serial (USB virtual COMM).

17.2 Maintenance – Unit Configuration

17.2.1 Download Unit configuration



Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

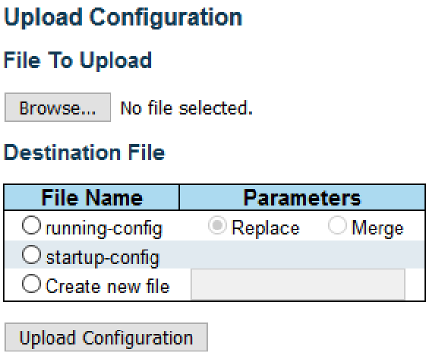
File Name
● running-config
○ default-config
○ startup-config

Figure 17-2: Maintenance – Download unit configuration

This page allows you to download the unit configuration to your own laptop, desktop, etc. Before downloading the unit configuration, you must select which configuration should be downloaded.

- **running-config** – The configuration being used by the unit. The user may change the unit configuration without saving the changes, meaning that after unit's power down-up it may operate with completely different settings. Selecting this option will save the unit's current running configuration to the user's local drive on a laptop, desktop, etc. Download of running-config may take a while to complete, as the file must be prepared for download.
- **startup-config** – The configuration to be used by the unit after power down/up cycle or software reset. In case the user saved the latest unit running-configuration, and had not made any additional changes, then the running-config and startup-config will be the same.
- **Default config** – Unit configuration to be used whenever startup-config and running-config files were erased. This is the unit's factory default configuration.

17.2.2 Upload Unit Configuration



Upload Configuration

File To Upload

No file selected.

Destination File

File Name	Parameters	
○ running-config	● Replace	○ Merge
○ startup-config		
○ Create new file		

Figure 18-3: Maintenance – Upload unit configuration

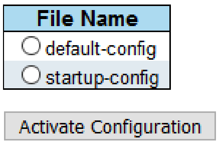
It is possible to upload a file from the web browser to all the files on the switch, except *default-config*, which is read-only.
Select the file to upload, select the destination file on the target, then click *Upload Configuration*.

If the destination is *running-config*, the file will be applied to the switch configuration. This can be done in two ways:

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

If the flash file system is full (i.e., contains *default-config* and 32 other files, usually including *startup-config*), it is not possible to create new files. Instead, an existing file must be overwritten or another file must be deleted.

17.2.3 Activate Unit Configuration

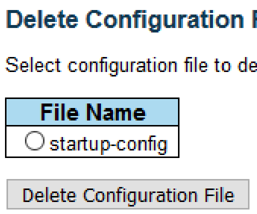


File Name
○ default-config
○ startup-config

Figure 17-3: Maintenance – Activate unit configuration

It is possible to activate any of the configuration files present on the switch, except for *running-config,* which represents the currently active configuration. Select the file to activate and click *Activate Configuration*. This will initiate the process of completely replacing the existing configuration with that of the selected file.

17.2.4 Delete Unit Configuration



Delete Configuration File

Select configuration file to delete.

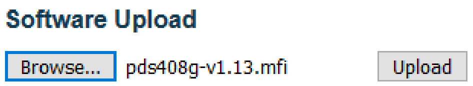
File Name
○ startup-config

Figure 18-5: Maintenance – Delete configuration

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.

17.3 Maintenance – Software Update

17.3.1 Upload New Version

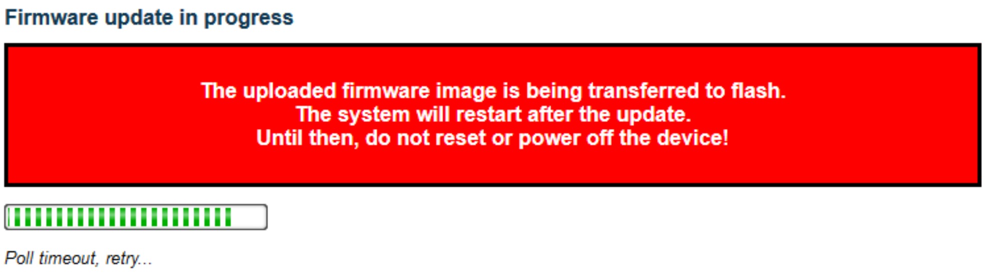


Software Upload

pds408g-v1.13.mfi

Figure 18-6: Software Update – Upload new version

This Page allows the user to update the software used to run the Switch. Switch software use the **mfi** extension. For example, *my-switch-software.mfi*. After the software image is uploaded, a message is displayed that the firmware update is initiated. After about a minute or so, the software is updated and the switch restarts.



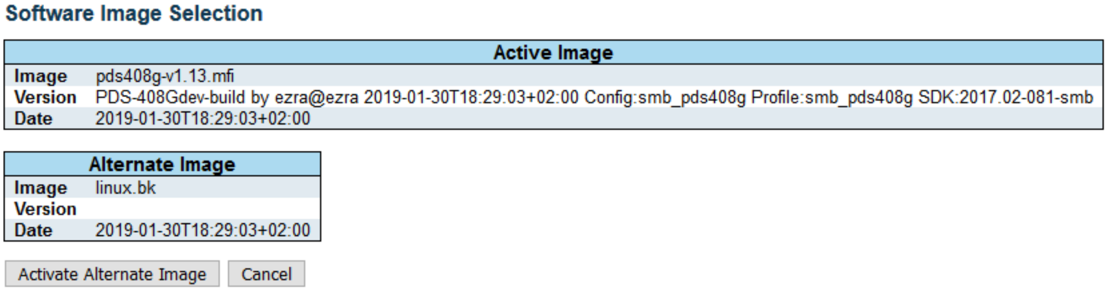
Firmware update in progress

The uploaded firmware image is being transferred to flash.
The system will restart after the update.
Until then, do not reset or power off the device!

Poll timeout, retry...

Figure 17-4: Software Update – in progress indication

17.3.2 Select active image

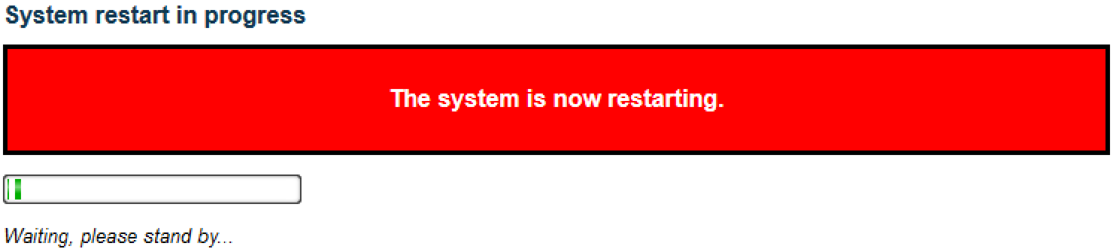

Software Image Selection

Active Image	
Image	pds408g-v1.13.mfi
Version	PDS-408Gdev-build by ezra@ezra 2019-01-30T18:29:03+02:00 Config:smb_pds408g Profile:smb_pds408g SDK:2017.02-081-smb
Date	2019-01-30T18:29:03+02:00

Alternate Image	
Image	linux.bk
Version	
Date	2019-01-30T18:29:03+02:00

Figure 17-5: Selecting active software image

This page allows you to revert to the previous (alternate) image before the latest software update. Pressing on the *Activate Alternate Image* will issue a warning message with an option to cancel the reverting process. If you opt to continue the reverting process, the image bellow will be displayed during the software reverting process.


System restart in progress

The system is now restarting.

Waiting, please stand by...

Figure 17-6: Switching active image

NOTES:

1 - If 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.

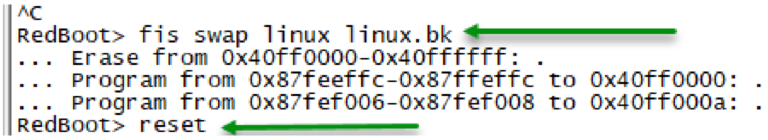
2 - If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.

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

17.3.3 Recovering from endless unit reboot after software update

In case of a rare failure, in which the unit enters endless software reboot cycles after software update preventing access to the web interface, it is still possible to revert to the previous version before performing software update by executing the following steps:

1. Connect to the unit USB interface with a USB→Serial Virtual COMM interface with baud rate of 115200.
2. Upon Switch reboot, press CTRL+C, to stop the boot from launching the Switch software.
   A **RedBoot>** prompt should appear.
3. Type **fis swap linux linux.bk** to revert the Switch to the older software version.
4. Type **reset** to restart the Switch using the reverted software version.

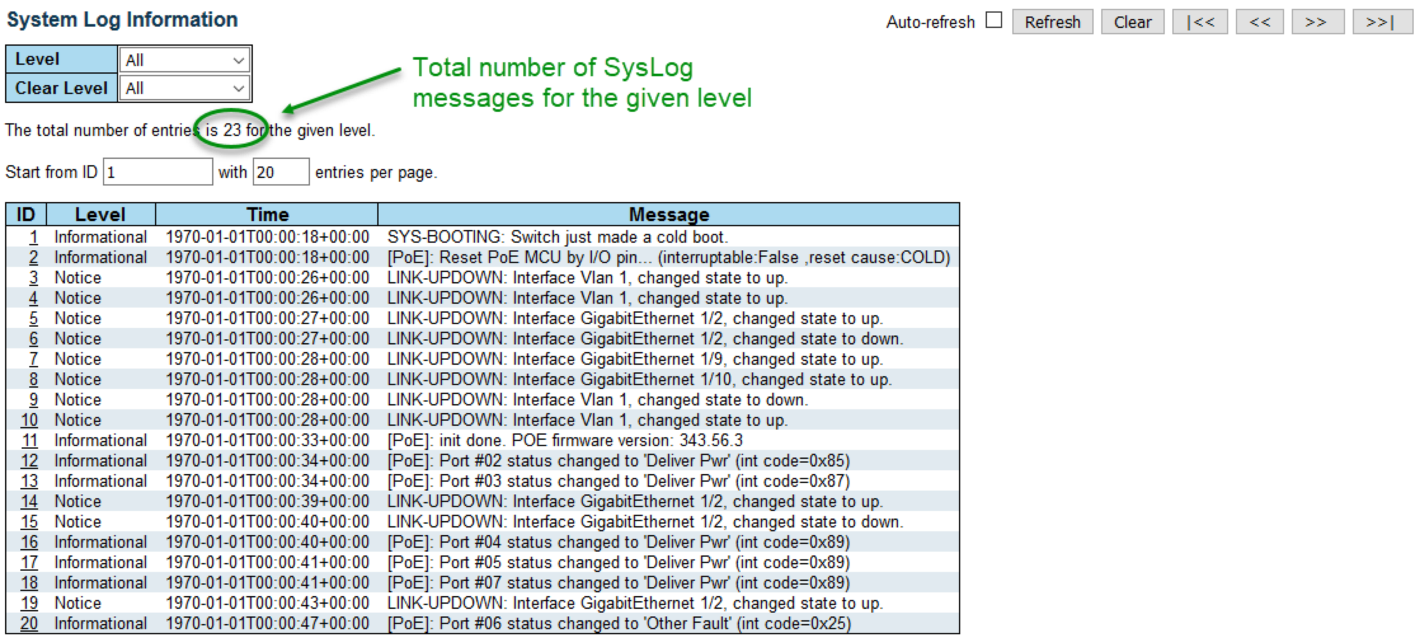


```
^C
RedBoot> fis swap linux linux.bk
... Erase from 0x40ff0000-0x40ffffff: .
... Program from 0x87feeffc-0x87ffeffc to 0x40ff0000: .
... Program from 0x87fef006-0x87fef008 to 0x40ff000a: .
RedBoot> reset
```

Figure 17-7: Recovering from endless reboot after software update

18 DIAGNOSTICS

18.1 Diagnostics - View log file



System Log Information

Level	All
Clear Level	All

Total number of SysLog messages for the given level

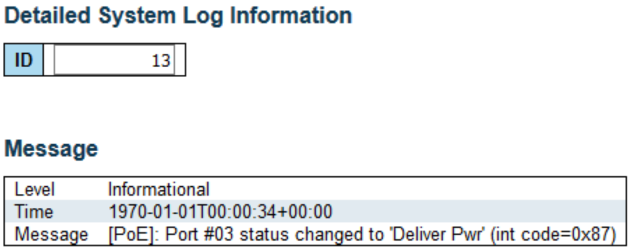
The total number of entries is 23 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
1	Informational	1970-01-01T00:00:18+00:00	SYS-BOOTING: Switch just made a cold boot.
2	Informational	1970-01-01T00:00:18+00:00	[PoE]: Reset PoE MCU by I/O pin... (interruptable:False ,reset cause:COLD)
3	Notice	1970-01-01T00:00:26+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
4	Notice	1970-01-01T00:00:26+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
5	Notice	1970-01-01T00:00:27+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to up.
6	Notice	1970-01-01T00:00:27+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to down.
7	Notice	1970-01-01T00:00:28+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/9, changed state to up.
8	Notice	1970-01-01T00:00:28+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/10, changed state to up.
9	Notice	1970-01-01T00:00:28+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
10	Notice	1970-01-01T00:00:28+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
11	Informational	1970-01-01T00:00:33+00:00	[PoE]: init done. POE firmware version: 343.56.3
12	Informational	1970-01-01T00:00:34+00:00	[PoE]: Port #02 status changed to 'Deliver Pwr' (int code=0x85)
13	Informational	1970-01-01T00:00:34+00:00	[PoE]: Port #03 status changed to 'Deliver Pwr' (int code=0x87)
14	Notice	1970-01-01T00:00:39+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to up.
15	Notice	1970-01-01T00:00:40+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to down.
16	Informational	1970-01-01T00:00:40+00:00	[PoE]: Port #04 status changed to 'Deliver Pwr' (int code=0x89)
17	Informational	1970-01-01T00:00:41+00:00	[PoE]: Port #05 status changed to 'Deliver Pwr' (int code=0x89)
18	Informational	1970-01-01T00:00:41+00:00	[PoE]: Port #07 status changed to 'Deliver Pwr' (int code=0x89)
19	Notice	1970-01-01T00:00:43+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to up.
20	Informational	1970-01-01T00:00:47+00:00	[PoE]: Port #06 status changed to 'Other Fault' (int code=0x25)

Figure 18-1: View SysLog file

Each page shows up to 999 table entries, selected through the "entries per page" input field. Pressing on one of the numbers under the ID column will show the specific SysLog message in greater detail.



Detailed System Log Information

ID	13

Message

Level	Informational
Time	1970-01-01T00:00:34+00:00
Message	[PoE]: Port #03 status changed to 'Deliver Pwr' (int code=0x87)

Figure 18-2: Detailed single SysLog message

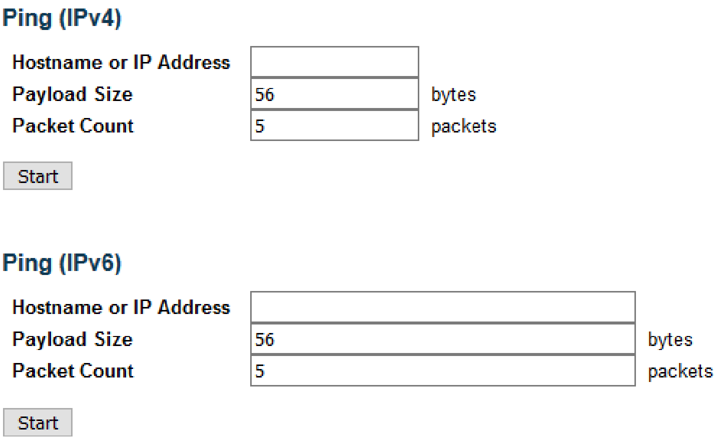
- **Level –**Select which specific SysLog message severity level to display. Possible SysLog message levels are:
  - **Informational** – lowest priority SysLog message level.
  - **Notice** – higher than Informational.
  - **Warning** – higher than Notice.
  - **Error** – higher than Warning.
  - **All** – shows SysLog messages from all levels.
- **Clear Level –** clear all SysLog messages from a specific SysLog level, or from all levels. You need to press the Clear button for clear to be executed.
- **Start from ID** – the input field allows you to change the starting point in the SysLog table report. Clicking the Refresh button will update the displayed table starting from that or the closest next entry match.

- **ID** - The identification of the system log entry.
- **Level** - The level of the system log entry.
- **Time** - The occurred time of the system log entry.
- **Message** - The detail message of the system log entry.

NOTE:
SysLog messages are kept in the RAM File System, meaning that SysLog messages will be lost whenever the Switch power is down, or the Switch restart command is initiated.

18.2 Diagnostics - Ping

This page allows you to issue ICMP (IPv4, ICMPv6) PING packets to troubleshoot IP connectivity issues.
It should be used to test network connectivity between the unit and a remote network device.



Ping (IPv4)

Hostname or IP Address		
Payload Size	56	bytes
Packet Count	5	packets

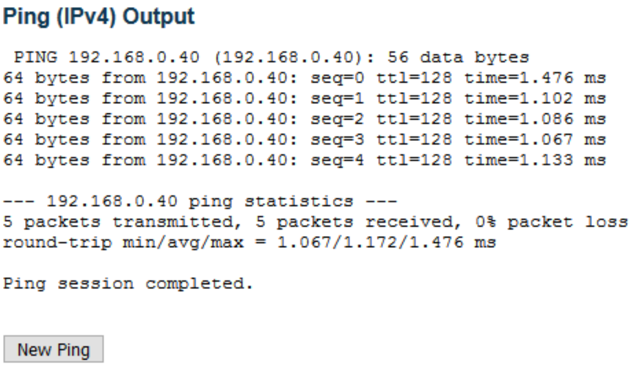
Ping (IPv6)

Hostname or IP Address		
Payload Size	56	bytes
Packet Count	5	packets

Figure 18-3: Ping Web interface

- **Hostname or IPv4/IPv6 Address** - The address of the destination host such as 192.168.0.50 for IPv4 or 2345::15 for IPv6, or Hostname such as **my-computer.com**.
- **Payload Size** - Sets the size of the ICMPv4/v6 data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.
- **Packet Count** - Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.

Pressing the *Start* button will initiate a series of pings as shown in the figure bellow.



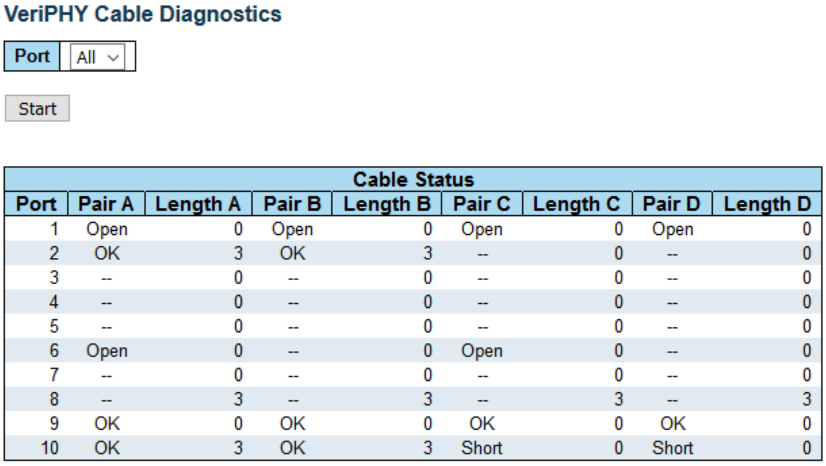
Ping (IPv4) Output

```
 PING 192.168.0.40 (192.168.0.40): 56 data bytes
64 bytes from 192.168.0.40: seq=0 ttl=128 time=1.476 ms
64 bytes from 192.168.0.40: seq=1 ttl=128 time=1.102 ms
64 bytes from 192.168.0.40: seq=2 ttl=128 time=1.086 ms
64 bytes from 192.168.0.40: seq=3 ttl=128 time=1.067 ms
64 bytes from 192.168.0.40: seq=4 ttl=128 time=1.133 ms

--- 192.168.0.40 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.067/1.172/1.476 ms

Ping session completed.
```

Figure 18-4: Ping in action

18.3 Diagnostics - RJ45 Cable test

This page is used for running the VeriPHY RJ45 Cable Diagnostics test for 10/100 and 1G copper ports.
Pressing *Start* will start the diagnostics. This will take approximately 15 seconds for a single port. If all ports are selected, this can take approximately 30 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table.



VeriPHY Cable Diagnostics

Port: All

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	Open	0	Open	0	Open	0	Open	0
2	OK	3	OK	3	--	0	--	0
3	--	0	--	0	--	0	--	0
4	--	0	--	0	--	0	--	0
5	--	0	--	0	--	0	--	0
6	Open	0	--	0	Open	0	--	0
7	--	0	--	0	--	0	--	0
8	--	3	--	3	--	3	--	3
9	OK	0	OK	0	OK	0	OK	0
10	OK	3	OK	3	Short	0	Short	0

Figure 18-5: RJ45 cables test

NOTE:
VeriPHY RJ45 cable test is only accurate for cables in the length range of 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 the VeriPHY RJ45 test is complete

- **Port** - The port where you are requesting VeriPHY Cable Diagnostics.
- **Cable Status** – Cable status for each of the four pairs inside the Ethernet cable
  - 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

18.4 Diagnostics – View CPU Load

This page shows the Switch CPU load.

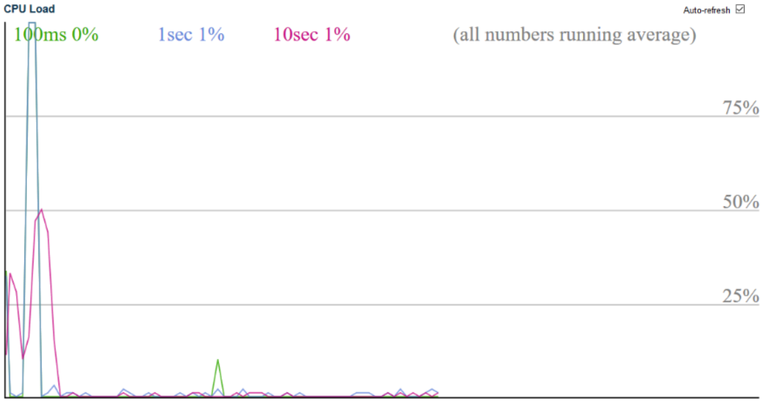


Figure 18-6: Switch CPU load

19 SAVE RUNNING CONFIG

Pressing on *save running config* saves the switch's *running-config* configuration to the Switch's *startup-config* configuration, so that next time the Switch is powered off and on or software rebooted, it will use the same configuration as before it had been restarted.

NOTE:
All switch runtime configuration changes will be lost upon switch reboot, unless *Save-Running-Config* was pressed, or CLI command *copy running-config startup-config* was entered.

Revision History

Revision Level / Date	Para. Affected	Description
1.0.1 19-3-19	Whole Document	initial document

For support contact: PoEsupport@microsemi.com

Visit our web site at: PoE Midspans, PoE Injectors & PoE Switches

Document PN: PD_PDS-408G_NMS_UG