MaxiiNet^{TM} Vi30208U
Operation and Installation Manual

4 +2+2 Port Series PoE+ L2 Plus Industrial Managed Switch

Firmware Version (V2.1.0925)
Revision Date (4-2024)

About This Manual

Copyright

Copyright © 2024 Vigitron, Inc. All rights reserved. The products and programs described in this user's manual are licensed products of Vigitron, Inc. This user's manual contains proprietary information protected by copyright, and this user's manual and all accompanying hardware, software and documentation are copyrighted. No parts of this user's manual may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable from by any means electronic or mechanical. This also Includes photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of Vigitron, Inc.

Purpose

This guide gives specific information on how to operate and use the management functions of the switch.

Audience

The guide is intended for use by network administrators who are responsible for operating and maintaining network equipment. Consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Conventions

The following conventions are used throughout this guide to show information:

NOTE: Emphasizes important information or calls your attention to related features or instructions.

WARNING: Alerts you to a potential hazard that could cause personal injury.

CAUTION: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warranty

See the Customer Support/Warranty booklet included with the product. A copy of the specific warranty terms applicable to Vigitron's products and replacement parts can be obtained from Vigitron's Sales and Service Office or authorized dealer.

Disclaimer

Vigitron does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. Vigitron disclaims liability for any inaccuracies or omissions that may have occurred. Information in this user's manual is subject to change without notice and does not represent a commitment on the part of Vigitron. Vigitron assumes no responsibility for any inaccuracies that may be contained in this user's manual. Vigitron makes no commitment to update or keep current the information in this user's manual and reserves the rights to make improvements to this user's manual and/or to the products described in this user's manual, at any time without notice.

FCC

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

FCC Caution

To assure continued compliance (example-use only shielded interface cables when connection to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Compliances and Safety Statements

FCC - Class

This equipment has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interferences in which case the user will be required to correct the interferences at his own expense.

CE Mark Declaration of Conformance for EMI and Safety (EEC)

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

You may use unshielded twisted-pair (UTP) for RJ-45 connections - Category 3 or better for 10 Mbps connections, Category 5 or better for 100 Mbps connections, and Category 5, 5e, or 6 for 1000 Mbps connections. For fiber optic connections, you may use 50/125- or 62.5/125-micron multimode fiber or 9/125 micron single- mode fiber.

EMC- Compliance

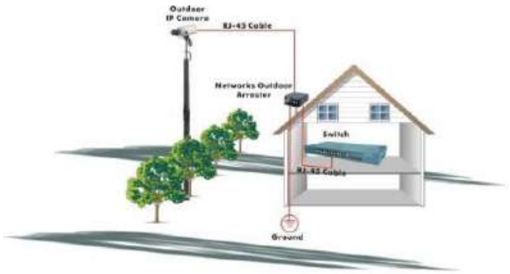
This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN61000-3 and the Generic European Immunity Standard EN55024.

EN55022(2006) +A1:2007/CISPR 22:2006+A1:2006	**Class A** **4K V CD, 8KV, AD**
IEC61000-4-2 (2001)	3V/m
IEC61000-4-3(2002)	1KV – (power line), 0.5KV – (signal line)
IEC61000-4-4(2004)	Line to Line: 1KV, Line to Earth: 2KV
IEC61000-4-5 (2001)	130dBuV(3V) Level 2
IEC61000-4-6 (2003)	1A/m
IEC61000-4-8 (2001)	Voltage dips: >95%, 0.5period, 30%, 25periods
IEC61000-4-11(2001)	Voltage interruptions: >95%, 250periods

CAUTION: Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge. To protect your device, always:

Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.

Pick up the device by holding it on the left and right edges only.
If you need to use an outdoor device to connect to this device with a cable, then you need to add an arrester on the cable between the outdoor device and this device.



Add an arrester between the outdoor device and this switch.

NOTE: The switch is an indoor device. If it will be used in an outdoor environment or connected with an outdoor device, then a lightning arrester must be used to protect the switch.

WARNING: Self-demolition on this product is strictly prohibited.
Damages caused by self-demolition will be charged for repair fees.

Do not place product outdoor or in a sandstorm.
Before installation, please make sure input power supply and product
Specifications are compatible to each other.
To reduce the risk of electric shock. Disconnect all AC or DC power cords 7and RPS cables to completely remove power from the unit.
Before importing/exporting configuration, please make sure the
firmware version is always the same. After the firmware upgrade, the switch will remove the configuration automatically to latest firmware version.

Introduction

Overview

The Vi30208U PoE switch, next generation network solutions, is an affordable managed switch that provides a reliable infrastructure for your business network. These switches deliver more intelligent features you need to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth to deliver information and applications more effectively. Easy to set up and use, it provides the ideal combination of affordability and capabilities for entry level networking, including small business or enterprise application. It also helps you create a more efficient and better- connected workforce.

The Vi30208U is an easy to implement managed Ethernet switch that provides ideal flexibility to design suitable network infrastructure for business requirement. However, unlike other entry-level switching solutions that provide advanced managed network capabilities only in the most expensive models, all Vigitron's series switches support the advanced security management capabilities and network features to support data, voice, security, and wireless technologies. These switches are easy to deploy and configure. They provide stable and quality performance network services your business needs.

The switch performs a wire-speed, non-blocking switching fabric. This allows wire- speed transport of multiple packets at low latency on all ports simultaneously. The switch also features full-duplex capability on all ports, which effectively doubles the bandwidth of each connection.
This switch uses store-and-forward technology to ensure maximum data integrity. With this technology, the entire packet must be received into a buffer and checked for validity before being forwarded. This prevents errors from being propagated throughout the network.

The switch can also be managed over the network with a web browser or a Telnet application. The switch includes a built-in network management agent that allows it to be managed in-band by using SNMP or RMON (Groups 1, 2, 3, 9) protocols. It also has an RJ-45 console port connector on the front panel for out-of-band management.

Table of Contents

Description of Hardware

The Vi30208U is a 4 +2+ 2 network switch. 4 UTP ports provide network connects with PoE. 2 UTP ports provide network connections, and 2 Fiber ports provide network connections. All ports are independent providing the ability to use both sets of UTP and Fiber as uplinks. All UTP ports are 1G and fiber ports at 1G/2.5G.

The switch contains 6/10 1000BASE-T RJ-45 ports. All RJ-45 ports support automatic MDI/MDI-X operation, auto-negotiation, and IEEE 802.3x auto-negotiation of flow control, so the optimum data rate, and transmission can be selected automatically.

Vi30208U supports the Small Form Factor Pluggable (SFP) transceiver slots. The SFP transceiver slots are shared with RJ-45 port 9 to 10. In the default configuration, if an SFP transceiver (purchased separately) is installed in a slot and has a valid link on the port, the associated RJ-45 port is disabled.

The following table shows a list of transceiver types that have been tested with the switch. For an updated list of vendors supplying these transceivers, contact your local dealer. For information on the recommended standards for fiber optic cabling, see "1000 Mbps Gigabit Ethernet Collision Domain".

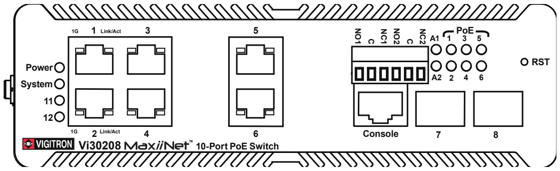
Media Standard	Fiber Diameter (microns)	Wavelength (nm)	Maximum Distance*
1000BASE-SX	50/125	850	550 m
	62.5/125	850	275 m
1000BASE-LX/ LHX/ XD/ZX	9/125	1310	10 km
	9/125	1550	30.50 km
	9/125	1300	10 km
1000BASE-LX Single Fiber	N/A	TX-1310/RX-1550	20 km
		Tx-1550/RX-1310	20 km
1000BASE-T	N/A	N/A	100 m
100-FX	50/125	850	2 km
	62.5/125	1550	15km

Table 1: Supported SFP Transceivers

NOTE: Maximum distance may vary for different SFP vendors.

NOTE: The Vi01000CH copper SFP will not interface with the Vi30208U.

Front Panel LED and Port Status



Note on Alarm LEDs

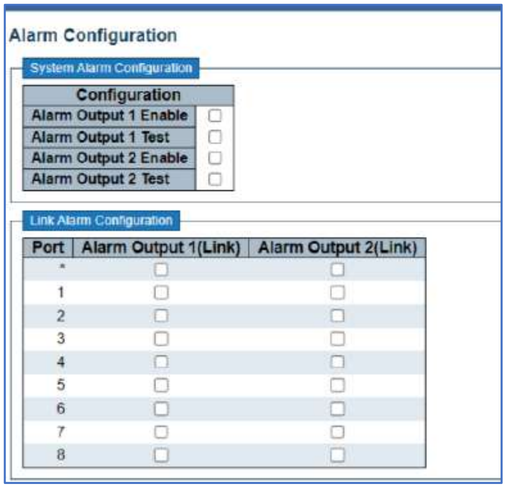
Power LED will indicate if power is on
System LED will be on if the CPU is operational.

The Vi30208U has two alarm LEDs. These LEDs are activity using the Configuration>System> System Log Configuration. When active the LED will flash even if not connection is present.
In order to extinguish the LED, the Admin must use the Configuration> System >System Log Configuration to disable the alarm Enable and the individual alarm link channel.

Select Save and after the alarm is extinguished reprogram the alarm.

The following table details the functions and descriptions of various LED indicators:

Model Name	Vi30208U
Ports	6*1G POE Ports 1G RJ45 uplink +2*2.5G SFP uplink
Description of Function Slots	Port 1-6: 4 X RJ45 10/100/1000Mbps (PoE) Port 7-8: 2 X SFP 1000/2500 Mbps (uplink)
PoE Ports	1-6 port, each port supports af/at/bt, max 90W output
LED Indicator	Port #1-6: Yellow shows the Links/ACT, Green Shows the PoE
	SFP Slot Uplink #7-8: Green shows the LINK/ACT.
	Power: Green System: Green
	Alarm: A1 A2 **Red**



Alarm Configuration

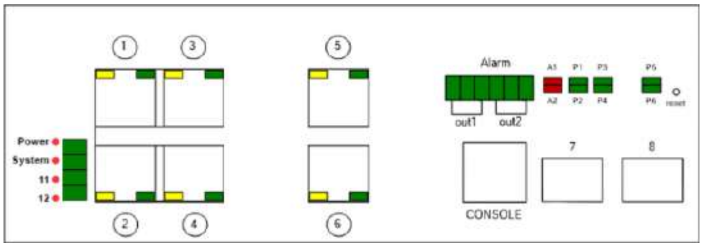
System Alarm Configuration

Configuration	
Alarm Output 1 Enable	□
Alarm Output 1 Test	□
Alarm Output 2 Enable	□
Alarm Output 2 Test	□

Link Alarm Configuration

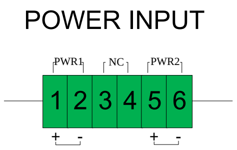
Port	Alarm Output 1(Link)	Alarm Output 2(Link)
*	□	□
1	□	□
2	□	□
3	□	□
4	□	□
5	□	□
6	□	□
7	□	□
8	□	□

The Vi30208U has a display panel for system and port indications that simplify installation and network troubleshooting. The LEDs are located on left hand side of the front panel for easy viewing. Details are shown below and described in the following tables.



Reset Button (Update)

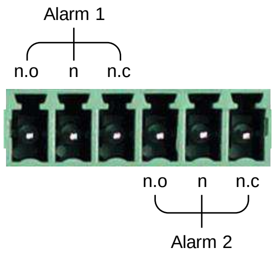
- Reset the Switch
    - To reboot and get the switch back to the previous configuration settings saved.
- Restore the Switch to Factory Defaults
    - To restore the original factory default settings back to the switch.



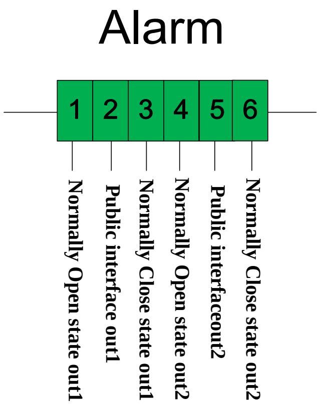
The Vi 30208U has two DC power inputs, each serving as a backup for the other. The maximum power input for each is limited to 500W. The power supply used must conform to the IEEE standard, requiring a DC voltage input between 52-57VDC.

Vigitron suggests three power supplies: Vi10120 (120 watts), Vi10240 (240 watts), and Vi10480 (480 watts). Please match the required input power to the requirements of your connected devices. The input DC will determine your available PoE budget and should be entered as part of your PoE setup.

Note on Alarm LEDs



For Normally Open contact connect wires to n.o and C (common)
For Normally Closed contact connect wires to n.c. and C (common)



Alarm							
Out1				**Out2**			
Normally open		Normally close		Normally open		Normally close	
PORT1	PORT2	PORT3	PORT2	PORT4	PORT5	PORT6	PORT5

Network Planning

Introduction to Switching

A network switch allows simultaneous transmission of multiple packets. It can partition a network more efficiently than bridges or routers. Therefore, the switch has been recognized as one of the most important devices for today's networking technology.

When performance bottlenecks are caused by congestion at the network access point such as file server, the device can be connected directly to a switched port. By using the full-duplex mode, the bandwidth of the dedicated segment can be doubled to maximize throughput.

When networks are based on repeater (hub) technology, the distance between end stations is limited by a maximum hop count. However, a switch can subdivide the network into smaller and more manageable segments and link them to the larger network. It then turns the hop count back to zero and removes the limitation.

A switch can easily be configured in any Ethernet, Fast Ethernet, or Gigabit Ethernet network to significantly increase bandwidth while using conventional cabling and network cards.

The Vi30208U has auto MDIX and 2 slots for the removable SFP module which support comprehensive types of fiber connection, such as LC and BiDi-LC modules. It is not only designed to segment your network, but also to provide a wide range of options in setting up network connections. Some typical applications are described below.

The switch is suitable for the following applications:

- Remote site application is used in enterprise or SMB.
- Peer-to-peer application is used in two remote offices.
- Office network.
- High-performance requirement environment.
- Advance security for network safety application.
- Suitable for data/voice and video conference applications.

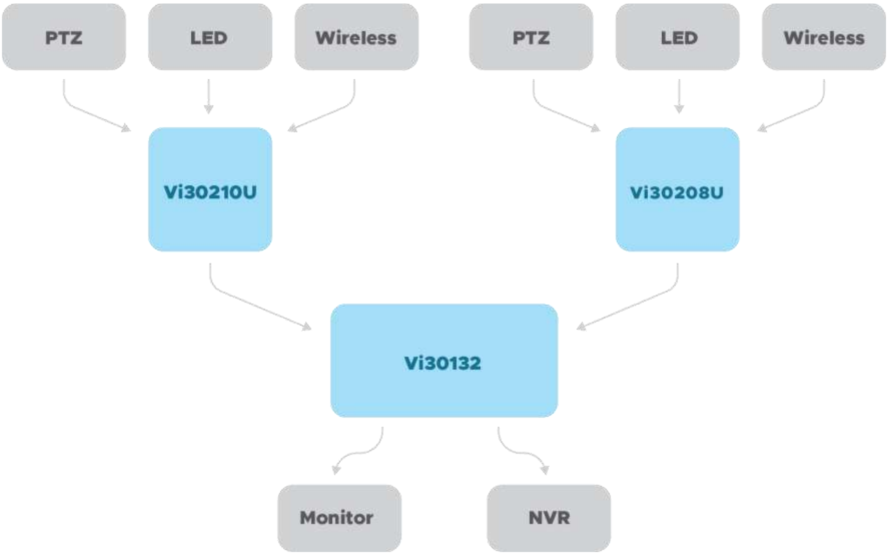
NOTE: Fiber ports are labeled as Ports 7 and 8 and are independent ports with copper posts can be used independent with any UTP ports

Application Examples

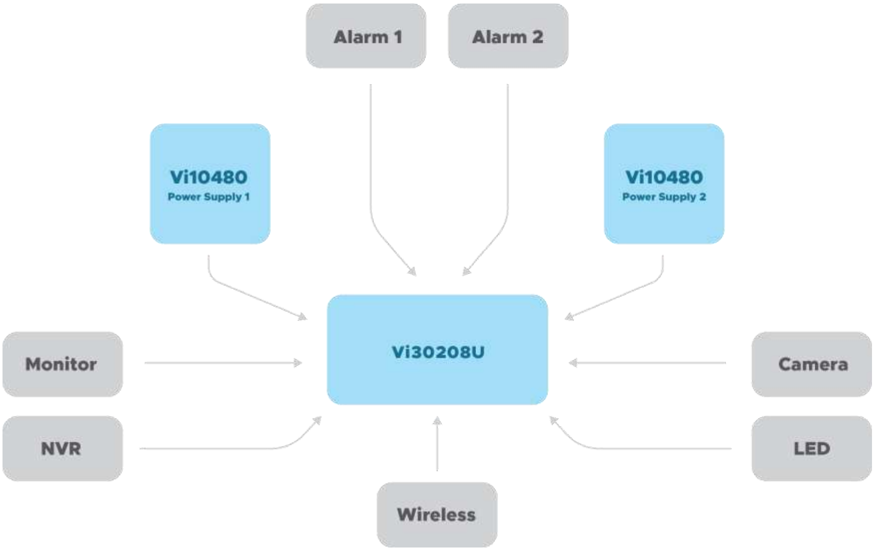
Network Connection between Remote Site and Central Site

This will be replaced with actual product images.

Peer to Peer
IDF to MDF Configuration



Single Headend Configuration



Installing the Switch

Selecting a Site
The switch can be mounted using DIN Rail mounts equipment or operated using the rack mount kit or on a flat surface. Be sure to follow the guidelines below when choosing a location.

The site should:

- Be at the center of all the devices that you want to link and near a power outlet.
- Be able to maintain its temperature within -30°C to 70C (-30C°F to 158°F) and its humidity within 10% to 90%, non-condensing.
- Be accessible for installing, cabling, and maintaining the devices.
- Allow the status LEDs to be clearly visible.

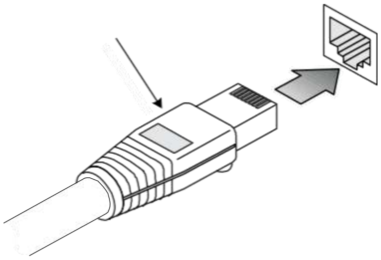
Make sure the twisted-pair Ethernet cable is always routed away from power lines, radios, transmitters, or any other electrical interference.
Make sure that Vi30208U is connected to a separate grounded power supply that provides 100 to 240 VAC, 50 to 60 Hz.
Make sure the power supply you are using provides the required power for your connected devices.

Ethernet Cabling
To ensure proper operation when installing the switch into a network, make sure that the current cables are suitable for 100BASE-TX or 1000BASE-T operation.
Check the following criteria against the current installation of your network:

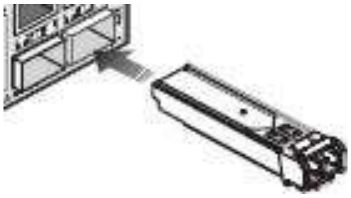
Cable type: Unshielded twisted pair (UTP) or shielded twisted pair (STP) cable with RJ-45 connectors; Category 5 or Category 5e with a maximum length of 100 meters is recommended 100BASE-TX, and Category 5e or 6 with a maximum length of 100 meters is recommended for 1000BASE-T.
Protection from radio frequency interference emissions.
Electrical surge suppression.
Separation of electrical wires and data-based network wiring.
Safe connections with no damaged cables, connectors, or shields.

Equipment Checklist

Rj-45 Connections



SFP Transceiver



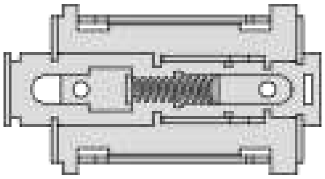
Package Contents
After unpacking the switch, please check the contents to make sure you have received all of the components. Also, make sure you have all other necessary installation equipment before beginning the installation process.

- Vi30208U GbE Management Switch
- Din Rail/ wall Adaptor

NOTE: Please notify your sales representative immediately if any of the aforementioned items are missing or damaged.

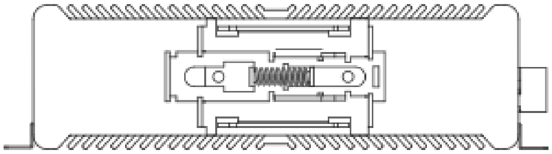
WARNING: The mini-GBICs are Class 1 laser devices. Avoid direct eye exposure to the beam coming from the transmit port.

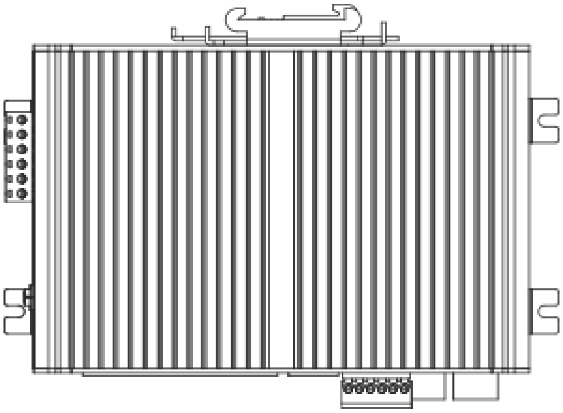
DIN Rail Mounting



Locate the mounting holds on the rear of the cabinet.

Desktop Mounting





Insert the four tabs as shown. Secure the Vi30208U to a flat surface.

Installing an Optional SFP Transceiver

You can install or remove a mini-GBIC SFP from a mini-GBIC slot without having to power off the switch. Use only manufacture mini-GBIC.

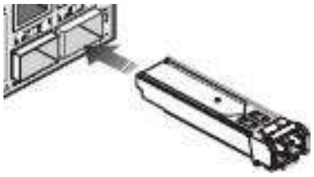
NOTE:

- The mini-GBIC slots are shared with the two 10/ 100/ 1000Base-T RJ-45 ports. If a mini-GBIC is installed in a slot, the associated RJ-45 port is disabled and cannot be used.
- The mini-GBIC ports operate only at full-duplex. Half-duplex operation is not supported.
- Ensure the network cable is NOT connected when you install or remove a mini-GBIC.

CAUTION:

Use only supported genuine manufacture mini- GBICs with your switch. Non-manufacture mini-GBIC might have compatibility issues and may result in product malfunction. SFPs should conform to the MSA standards.

Inserting an SFP Transceiver into a Slot



Description

SFP Slots Support the following SFPs- SFPs must match the Fiber Cable
1000Base-SX GE SFP Fiber Module, LC Multi-Mode 850nm
1000Base-SX GE SFP Fiber Module, LC Multi-Mode 1310nm 2km
1000Base-LX GE SFP Fiber Module, LC Single-Mode 10km
1000Base-LX GE SFP Fiber Module, LC Single-Mode 30km
1000Base-LX GE SFP Fiber Module, LC Single-Mode 50km
1000Base-LX GE SFP Fiber Module, LC Single-Mode 50km
1000Base-LX GE SFP Fiber Module, Bidi LC Single-Mode 10km, 1310nm
1000Base-LX GE SFP Fiber Module, Bidi LC Single-Mode 10km, 1550nm
1000Base-LX GE SFP Fiber Module, Bidi LC Single-Mode 20km, 1550nm
1000Base-LX GE SFP Fiber Module, Bidi LC Single-Mode 20km, 1310nm
100Base-FX FE SFP Fiber Module, LC Multi-Mode, 850nm
100Base-FX FE SFP Fiber Module, LC Single-Mode 20km, 1310nm
2500Base-LX SFP Fiber Module, LC – Single Mode 20Km, 1310nm

CAUTION:
Differences in manufacturers may result in different performance and reporting statuses.

To Install an SFP Transceiver, Do the Following:

Step1: Consider the network and cabling requirements to select an appropriate SFP transceiver type.

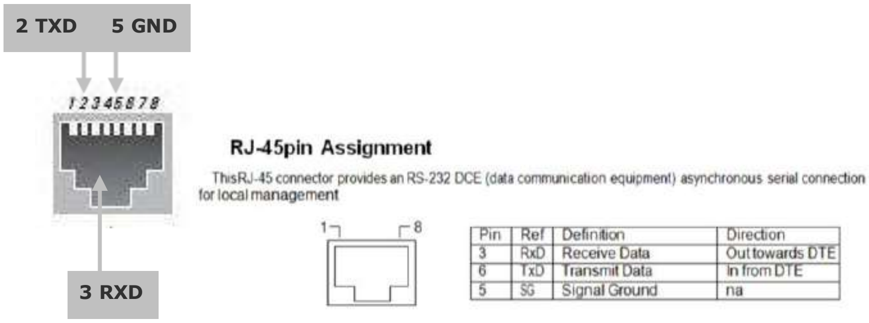
Step2: Insert the transceiver with the optical connector facing outward and the slot connector facing down. Note that SFP transceivers are keyed so they can only be installed in one orientation.

Step3: Slide the SFP transceiver into the slot until it clicks into place.

Note: SFP transceivers are not provided in the switch package.

The RJ-45 serial port on the switch’s front panel is used to connect to the switch for out-of-band console configuration. The command-line-driven configuration program can be accessed from a terminal or a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in the following table.

Connecting to the Console Port



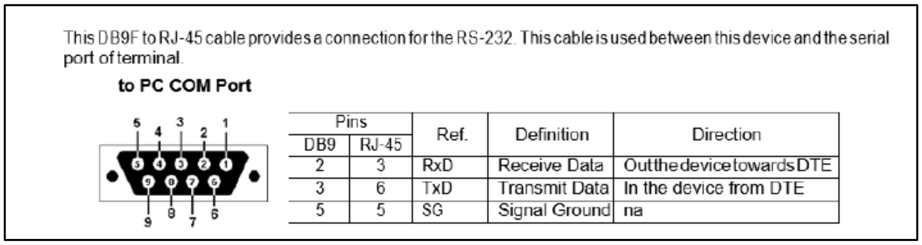
RJ-45pin Assignment

ThisRJ-45 connector provides an RS-232 DCE (data communication equipment) asynchronous serial connection for local management

Pin	Ref	Definition	Direction
3	RxD	Receive Data	Out towards DTE
6	TxD	Transmit Data	In from DTE
5	SG	Signal Ground	na

Serial Cable wiring

Switch's 8-Pin Serial Port	Null Modem	PC's 9-Pin DTE Port



This DB9F to RJ-45 cable provides a connection for the RS-232. This cable is used between this device and the serial port of terminal.

to PC COM Port

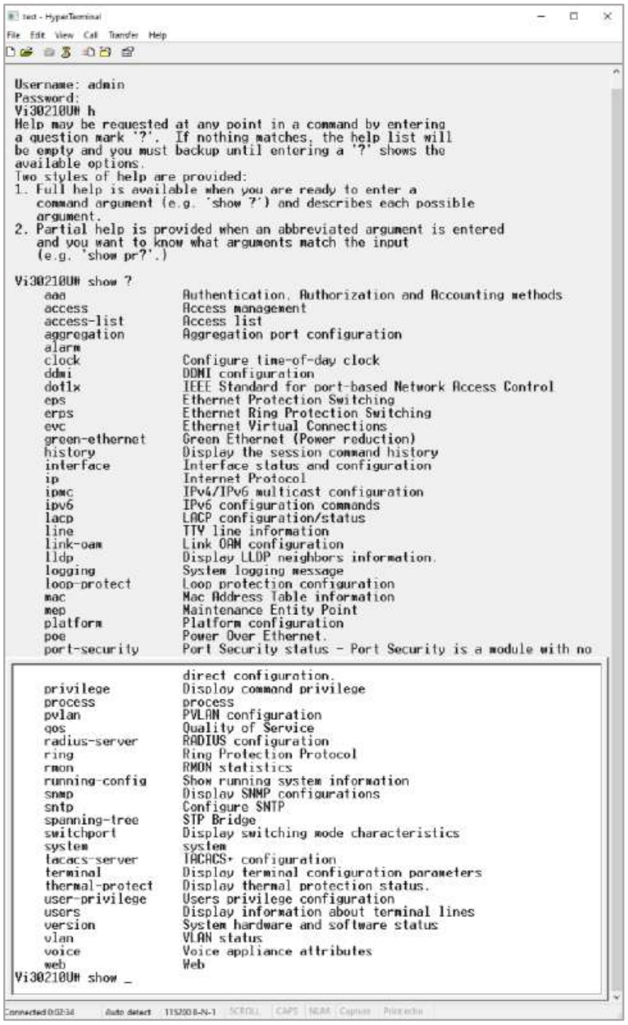
Pins		Ref.	Definition	Direction
DB9	RJ-45			
2	3	RxD	Receive Data	Outthedevicetowards DTE
3	6	TxD	Transmit Data	In the device from DTE
5	5	SG	Signal Ground	na

Serial Cable Wiring: Note no other connections are required.

Plug in the Console Port

The serial port's configuration requirements are as follows:

- Default Baud Rate: 115,200 bps
- Character Size: 8 Characters
- Parity: None
- Stop Bit: One
- Data Bits: 8
- Flow Control: None



```
Username: admin
Password:
Vi30210U# h
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)

Vi30210U# show ?
    aaa                 Authentication, Authorization and Accounting methods
    access              Access management
    access-list         Access list
    aggregation         Aggregation port configuration
    alarm
    clock               Configure time-of-day clock
    ddmi                DDMI configuration
    dot1x               IEEE Standard for port-based Network Access Control
    eps                 Ethernet Protection Switching
    erps                Ethernet Ring Protection Switching
    evc                 Ethernet Virtual Connections
    green-ethernet      Green Ethernet (Power reduction)
    history             Display the session command history
    interface           Interface status and configuration
    ip                  Internet Protocol
    ipmc                IPv4/IPv6 multicast configuration
    ipv6                IPv6 configuration commands
    lacp                LACP configuration/status
    line                TTY line information
    link-oam            Link OAM configuration
    lldp                Display LLDP neighbors information.
    logging             System logging message
    loop-protect        Loop protection configuration
    mac                 Mac Address Table information
    mep                 Maintenance Entity Point
    platform            Platform configuration
    poe                 Power Over Ethernet.
    port-security       Port Security status - Port Security is a module with no
                        direct configuration.
    privilege           Display command privilege
    process             process
    pvlan               PVLAN configuration
    qos                 Quality of Service
    radius-server       RADIUS configuration
    ring                Ring Protection Protocol
    rmon                RMON statistics
    running-config      Show running system information
    snmp                Display SNMP configurations
    sntp                Configure SNTP
    spanning-tree       STP Bridge
    switchport          Display switching mode characteristics
    system              system
    tacacs-server       TACACS+ configuration
    terminal            Display terminal configuration parameters
    thermal-protect     Display thermal protection status.
    user-privilege      Users privilege configuration
    users               Display information about terminal lines
    version             System hardware and software status
    vlan                VLAN status
    voice               Voice appliance attributes
    web                 Web
Vi30210U# show _
```

Once the console port is accessed the individual CLI commands will be shown

Connecting Network Devices
The switch is designed to be connected to 10, 100, or 1000Mbps network cards in PCs and servers, as well as, to other switches and hubs. It may also be connected to remote devices using optional SFP transceivers.

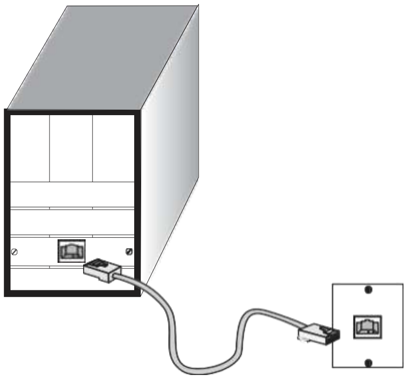
Each device requires an unshielded twisted-pair (UTP) cable with RJ-45 connectors at both ends. Use Category or c 5e, or 6 cables for 1000BASE-T connections, and Category 5 or better for 100BASE-TX connections.

Cabling Guidelines- UTP Copper Cabling
The RJ-45 ports on the switch support automatic MDI/MDI-X pin-out configuration, so you can use standard straight-through or cross twisted-pair cables to connect to any other network device (PCs, servers, switches, routers, or hubs).

See Appendix B for further information on cabling.

⚠ **CAUTION:** Do not plug a phone jack connector into an RJ-45 port. This will damage the switch. Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Connecting to PCs, Servers, Hubs and Switches
Step 1: Attach one end of a twisted-pair cable segment to the device’s RJ-45 connector.



Making Twisted-Pair Connections
Step 2: If the device is a network card and the switch is in the wiring closet, attach the other end of the cable segment to a modular wall outlet that is connected to the wiring closet. See the section “Network Wiring Connections.” Otherwise, attach the other end to an available port on the switch.

Make sure each twisted pair cable does not exceed 100 meters (328 ft) in length.

ⓘ **NOTE:** Avoid using flow control on a port connected to a hub, unless it is actually required to solve a problem. Otherwise, back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Step 3: The green LED notes both link and activity. When the link is 1G the LED will be amber.

Network Wiring Connections
Today, the punch-down block is an integral part of many of the newer equipment racks. It is actually part of the patch panel. Instructions for making connections in the wiring closet with this type of equipment are as follows.

Step 1: Attach one end of a patch cable to an available port on the switch, and the other end to the patch panel.

Step 2: If it’s not already in place, attach one end of a cable segment to the back of the patch panel where the punch-down block is located and the other end to a modular wall outlet.

Step 3: Label the cables to simplify future troubleshooting. See **“Cable Labeling and Connection Records”** on page 29.

Making Fiber Port Connections

An optional Gigabit SFP transceiver can be used as a backbone connection between switches, or as a connection to a high-speed server.

Each single-mode fiber port requires 9/125 micron single-mode fiber optic cable with an LC connector at both ends. Each multimode fiber optic port requires 50/125- or 62.5/125-micron multimode fiber optic cabling with an LC connector at both ends.

WARNING: This switch uses lasers to transmit signals over a fiber optic cable. The lasers are inherently eye-safe in normal operation. However, the user should never look directly at a transmit port when it is powered on.

WARNING: Considering safety, when selecting a fiber SFP device, please make sure that it can function at a temperature that is not less than the recommended maximum operating temperature of the product. You must also use an approved laser SFP transceiver.

Step 1: Remove and keep the LC port’s rubber plug. When it’s not connected to a fiber cable, the rubber plug should be replaced to protect the optics.

Step 2: Check that the fiber terminators are clean. You can clean the cable plugs by wiping them gently with a clean tissue or cotton ball moistened with a little ethanol. Dirty fiber terminators on fiber optic cables will impair the quality of the light transmitted through the cable and lead to degraded performance on the port.

Step 3: Connect one end of the cable to the LC port on the switch and the other end to the LC port on the other device. Since LC connectors are keyed, the cable can be attached in only one orientation.

Step 4: As a connection is made, check the Link LED on the switch corresponding to the port to be sure that the connection is valid.

The fiber optic ports operate at 1 Gbps. The maximum length for fiber optic cable operating at Gigabit speed will depend on the fiber type as listed under “1000 Mbps Gigabit Ethernet Collision Domain” on page 27.

Connectivity Rules

1000Base-T Cable Requirements

When adding hubs to your network, please note that because switches break up the path for connected devices into separate collision domains, you should not include the switch or connected cabling in your calculations for cascade length involving other devices.

All Category 5 UTP cables that are used for 100BASE-TX connections should also work for 1000BASE-T, provided that all four wire pairs are connected. However, it is recommended that for all critical connections, or any new cable installations,

Category 5e or Category 6 cable should be used. The Category 5e and 6 specifications include test parameters that are only recommendations for

Category 5. Therefore, the first step in preparing the existing Category 5 cable to run 1000BASE-T is to make sure that it complies with the IEEE 802.3-2005 standards.

Cable Type	Maximum Cable Length	Connector
Category 5, 5e or 6 100-ohm UTP or STP	100.m (328 ft)	RJ-45

Fiber Size	Fiber Bandwidth	Maximum Cable Length	Connector
62.5/125-micron multimode fiber	160 MHz/km	220 m (722 ft)	LC
	200 MHz/km	275 m (902 ft)	LC
50/125-micron multimode fiber	400 MHz/km	500 m (1641 ft)	LC
	500 MHz/km	550 m (1805 ft)	LC

Table 6: Maximum 1000BASE-SX Gigabit Fiber Cable Lengths

Fiber Size	Fiber Bandwidth	Maximum Cable Length	Connector
9/125 micron single-mode fiber 1310nm	N/A	10km (6.2 miles)	LC
9/125 micron single-mode fiber 1550nm	N/A	30km (18.64 miles) 50km (31.06 miles)	LC LC

Maximum 1000BASE-LX/LHX/XD/ZX Gigabit Fiber Cable Length

Fiber Size	Fiber Bandwidth	Maximum Cable Length	Connector
Single-mode TX-1310nm RX-1550nm	N/A	20km (12.42miles)	BIDI LC
Single-mode TX-1550nm RX-1310nm	N/A	20km (12.42miles)	BIDI LC

Maximum 1000BASE-LX Single Fiber Gigabit Fiber Cable Length

100 Mbps Fast Ethernet Collision Domain

Cable Type	Maximum Cable Length	Connector
Category 5, 5e or 6 100-ohm UTP or STP	100.m (328 ft)	RJ-45

Maximum Fast Ethernet Cable Lengths

Cable Labeling and Connection Records

When planning a network installation, it is essential to label the opposing ends of cables and record where each cable is connected. This will allow the user to easily locate inter-connected devices, isolate faults, and change the topology without the need for unnecessary time consumption.

To best manage the physical implementations of your network, follow these guidelines:

- Clearly label the opposing ends of each cable.
- Use your building's floor plans to draw a map of the locations of all network-connected equipment. For each piece of equipment, identify the devices to which it is connected.
- Note the length of each cable and the maximum cable length supported by the switch ports.
- For ease of understanding, use a location-based key when assigning prefixes to your cable labeling.
- Use sequential numbers for cables that originate from the same equipment.
- Differentiate between racks by naming accordingly.
- Label each separate piece of equipment.
- Display a copy of your equipment map, including keys to all abbreviations at each equipment rack.

Basic Troubleshooting Tips

Most problems are caused by the following situations. Check for these items first when starting your troubleshooting:
Connecting to devices that have a fixed full-duplex configuration.
The RJ-45 ports are configured as “Auto”. When connecting to the attached devices, the switch will operate in one of two ways to determine the link speed and the communication mode (half-duplex or full duplex):

- If the connected device is also configured to “Auto”, the switch will automatically negotiate both link speed and communication mode.
- If the connected device has a fixed configuration (e.g. 100Mbps at half or full duplex), the switch will automatically sense the link speed but will default to a communication mode of half-duplex.
- Because the series Vi30208U behave in this way (in compliance with the IEEE802.3 standard), if a device connected to the switch has a fixed configuration at full duplex, the device will not connect correctly to the switch. The result will be high error rates and very inefficient communications between the switch and the device.
- Make sure all devices connected to the Vi30208U are configured to auto-negotiate or are configured to connect at half-duplex (e.g. all hubs are configured this way).
- Faulty or lose cables. Look for loose or faulty connections. If they appear to be OK, make sure the connections are snug. If that does not correct the problem, try a different cable.
- Non-standard cables. Non-standard and mis wired cables may cause network collisions and other network problems and can seriously impair network performance. Use a new correctly wired cable for pin-outs and correct cable wiring. A category 5 cable tester is a recommended tool for every 100Base-TX and 1000Base-T network installation.
- Improper Network Topologies. It is important to make sure you have a valid network topology. If you no longer experience the problems, the new topology is probably at fault. In addition, you should make sure that your network topology contains no data path loops.
- Check the port configuration. A port on your switch may not be operating as you expect because it has been put into a “blocking” state by the Spanning Tree, the GVRP (automatic VLANs), or the LACP (automatic trunking). Note that the normal operation of the Spanning Tree, GVRP, and LACP features may put the port into a blocking state. Or the port just may have been configured as
    - “Disabled” through software.

Basic Troubleshooting Chart

Symptom	Action
POWER LED is Off	o Check connections between the switch, the power cord, and the wall outlet. o Contact your dealer for assistance.
Link LED is Off	o Verify that the switch and attached device are powered on. o Be sure the cable is plugged into the switch and corresponding device. o If the switch is installed in a rack, check the o connections to the punch-down block and the patch panel. o Verify that the proper cable type is used and its length does not exceed specified limits. o Check the adapter on the attached device and cable o connections for possible defects. Replace the defective adapter or cable if necessary.

If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or internal power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses, or surges at the power outlet. If you still cannot isolate the problem, the internal power supply may be defective. Verify that all system components have been properly installed. If one or more components appear to be malfunctioning (e.g. the power cord or network cabling), test them in an alternate environment where you are sure that all the other components are functioning properly.

You can access the management agent in the switch from anywhere within the attached network using Telnet, a web browser. However, you must first configure the switch with a valid IP address, subnet mask, and default gateway. If you have trouble establishing a link to the management agent, check to see if you have a valid network connection. Then verify that you've entered the correct IP address. Also, be sure the port that you are connecting to the switch has not been disabled. If it has not been disabled, then check the network cabling that runs between your remote location and the switch.

IP Addressing: In order to access the Vi30208U's GUI, your connected computer must be on the same network as the switch. As the default IP address is 192.168.0.1, the computer you use can be addressed as 192.168.0.xxx (any number except (1).

Power and Cooling Problems

Installation

The Vi30208U can operator under high temperature ranging from -30C to 70C. The unit is not weatherproof and requires installation in weatherproof housing. Consideration must be given to the potential internal temperature within the housing that will affect operations. The Vi30208U does provide operation settings which monitor the switches internal temperature and will affect individual port shutdowns based on the actual settings. It is recommended these settings not exceed 115C.

Twisted-Pair Cable and Pin Assignment
For 10/100BASE-TX connections, the twisted-pair cable must have two pairs of wires. For 1000BASE-T connections, the twisted-pair cable must have four pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

⚠ **CAUTION:** DO NOT plug a phone jack connector into any RJ- 45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

⚠ **CAUTION:** Each wire pair must be attached to the RJ-45 connectors in a specific orientation.

The figure below illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

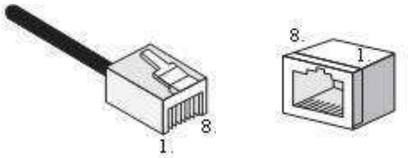


Figure 19: RJ-45 Connector Pin Numbers

10BASE-T/100Base-Tx Pin Assignments
Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100-ohm Category 3 or better cable for 10 Mbps connections, or 100- ohm Category 5 or better cable for 100 Mbps connections. Also, be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

The RJ-45 ports on the switch base unit support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3, and 6 at the other end of the cable. When using any RJ-45 port on this switch, you can use either a straight-through or crossover cable.

Pin	MDI Signal Name	MDI-X Signal Name
1	Transmit Data plus (TD+)	Receive Data plus (RD+)
2	Transmit Data minus (TD-)	Receive Data minus (RD-)
3	Receive Data plus (RD+)	Transmit Data plus (TD+)
6	Receive Data minus (RD-)	Transmit Data minus (TD-)
4,5,7,8	Not used	Not used

NOTE: The “+” and “-” signs represent the polarity of the wires that make up each wire pair.

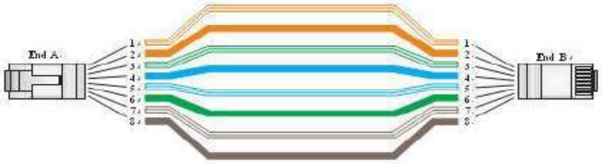
EIA/TIA 568B RJ-45 Wiring Standard

Straight-Through Wiring

If the twisted-pair cable is to join two ports and only one of the ports has an internal crossover (MDI-X), the two pairs of wires must be straight-through (when auto-negotiation is enabled for any RJ-45 port on this switch, you can use either straight-through or crossover cable to connect to any device type).

You must connect all four wire pairs as shown in the following diagram to support Gigabit Ethernet.

EIA/TIA 568B RJ-45 Wiring Standard 10/100BASE-TX
Straight-through Cable
Figure 20: Straight-through Wiring



If the twisted-pair cable is to join two ports and either both ports are labeled with an “X” (MDI-X) or neither port is labeled with an “X” (MDI), a crossover must be implemented in the wiring (when auto-negotiation is enabled for any RJ-45 port on this switch, you can use either straight-through or crossover cable to connect to any device type).

You must connect all four wire pairs as shown in the following diagram to support Gigabit Ethernet

Crossover Wiring

10/100BASE-TX Crossover Cable

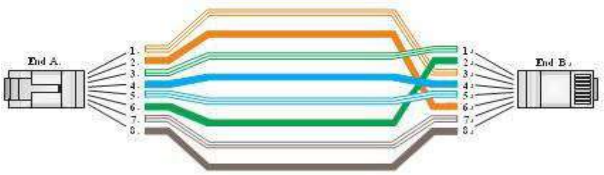


Figure 21: Crossover Wiring

1000Base-T Pin Assignments

If your existing Category 5 installation does not meet one of the test parameters for 1000Base-T, there are three measures that can be applied to try and correct the problem:

Replace any Category 5 patch cables with high-performance Category 5e or Category 6 cables.
Reduce the number of connectors used in the link.
Reconnect some of the connectors in the link.

1000BASE-T MDI and MDI-X Port Pin-Out

All 1000BASE-T ports support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs.
The table below shows the 1000BASE-T MDI and MDI-X port pin outs. These ports require that all four pairs of wires be connected. Note that for 1000BASE-T operation, all four pairs of wires are used for both transmit and receive.
Use 100-ohm Category 5, 5e, or 6 unshielded twisted-pair (UTP) or shielded twisted- pair (STP) cable for 1000BASE-T connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 ft).

Pin	MDI Signal Name	MDI-X Signal Name
1	Bi-directional Pair A Plus (BI_DA+)	Bi-directional Pair B Plus (BI_DB+)
2	Bi-directional Pair A Minus (BI_DA-)	Bi-directional Pair B Minus (BI_DB-)
3	Bi-directional Pair B Plus (BI_DB+)	Bi-directional Pair A Plus (BI_DA+)
4	Bi-directional Pair C Plus (BI_DC+)	Bi-directional Pair D Plus (BI_DD+)
5	Bi-directional Pair C Minus (BI_DC-)	Bi-directional Pair D Minus (BI_DD-)
6	Bi-directional Pair B Minus (BI_DB-)	Bi-directional Pair A Minus (BI_DA-)
7	Bi-directional Pair D Plus (BI_DD+)	Bi-directional Pair C Plus (BI_DC+)
8	Bi-directional Pair D Minus (BI_DD-)	Bi-directional Pair C Minus (BI_DC-)

(NEXT), and Far-End Crosstalk (FEXT). This cable testing information is specified in the ANSI/TIA/EIA-TSB-67 standard. Additionally, cables must also pass test
parameters for Return Loss and Equal-Level Far-End Crosstalk (ELFEXT). These tests are specified in the ANSI/TIA/EIA-TSB-95 Bulletin, “The Additional Transmission Performance Guidelines for 100 Ohm 4-Pair Category 5 Cabling.

NOTE: That when testing your cable installation, be sure to include all patch cables between switches and end devices.

Fiber Standards

Important Note: Fiber SFPs have no standards regarding interface with network switches with the exception of the Multi standard Agreement (MSA) with is limited to the physical interface between the SFP and a switch port. Data transmission may require adjusting port bandwidth settings on your switch.

When installing SFP match certain the SFP matches the installed fiber and are the same on both ends of the cable

The International Telecommunication Union (ITU-T) has standardized various fiber types for data networks. These are summarized in the following table.

Fiber Standards

ITU-T Standard	Description	Application
G.651	**Multimode Fiber** 50/125-micron core	Short-reach connections in the 1300- nm or 850-nm band.
G.652	**Non-Dispersion-Shifted Fiber** Single-mode, 9/125- micron core	Longer spans and extended reach. Optimized for operation in the 1310- nm band, but can also be used in the 1550-nm band.
G.652.C	**Low Water Peak Non- Dispersion-Shifted Fiber** Single-mode, 9/125-micron core	Longer spans and extended reach. Optimized for wavelength-division multiplexing (WDM) transmission across wavelengths from 1285 to 1625 nm. The zero-dispersion wavelength is in the 1310-nm region.
G.653	**Dispersion-Shifted Fiber** Single-mode, 9/125- micron core	Longer spans and extended reach. Optimized for operation in the region from 1500 to 1600-nm.
G.654	**1550-nm Loss- Minimized Fiber** Single-mode, 9/125- micron core	Extended long-haul applications. Optimized for high-power transmission in 1500 to 1600-nm region, with low loss in the 1550-nm band.
G.655	**Non-Zero Dispersion- Shifted Fiber** Single-mode, 9/125- micron core	Extended long-haul applications. Optimized for high-power dense wavelength-division multiplexing (DWDM) operation in the region from 1500 to 1600-nm.

Specifications

Physical Characteristics

Ports	2 100/1000Mbps SFP Fiber ports 6 UTP 1G ports with PoE
Network Interface	Ports 1-6: RJ-45 Connector 10BASE-T: RJ-45 (100-ohm, UTP cable; Category 3 or better) 100BASE-TX: RJ-45 (100-ohm, UTP cable; Category 5 or better) 1000BASE-T: RJ-45 (100-ohm, UTP or STP cable. Category 5, 5e or 6) *Maximum Cable Length - 100 m (328 ft) Ports 7-8: RJ-45 connector/ (100/1000M) SFP 1000M/2500M
Buffer Architecture	1392KB on-chip frame buffer
Aggregate Bandwidth	20 Gbps
Switching Database LEDs	8K MAC address entries System: POWER TP Port: status (LINK/ACT), 10/100/1000M SFP Port: status (LINK/ACT/SPD), 100/1000M
Weight	1.9 lbs.
Size	4 3/8" x 2" x 6 5/8"
Temperature	Operating: -30°C to 70°C (-22°F to 158°F)
Humidity	Operating: 5% to 90% (non-condensing)
Power Input	Not to exceed 480 watts @ 57VDC
Power Supply	External DC input
Power Consumption	20W maximum

Switch Features

Forwarding Mode	Store-and-forward
Throughput	35.712Mpps
Flow Control	Full-Duplex: IEEE 802.3x Half-Duplex: Back pressure

Management Features

In-Band Management	SSH/SSL, Telnet, SNMP, or HTTP
Out-Of-Band Management	RS-232 (RJ-45) console port
Software Loading	HTTP, TFTP in-band, Console out-of-band

Standards	IEEE 802.3 => 10Base-T Ethernet (Twisted-pair Copper) IEEE 802.3u => 100Base-TX Ethernet (Twisted-pair Copper) IEEE 802.3ab => 1000Base-TX Ethernet (Twisted-pair Copper) IEEE 802.3z => 1000Base-X Ethernet IEEE 802.3x => Flow Control Capability ANSI/IEEE 802.3 => Auto-negotiation IEEE 802.1Q => VLAN IEEE 802.1p => Class of Service IEEE 802.1X => Access Control IEEE 802.1D => Spanning Tree IEEE 802.1w => Rapid Spanning Tree IEEE 802.1s => Multiple Spanning Tree IEEE 802.3ad => ink Aggregation Control Protocol (LACP) IEEE 802.1AB => Link Layer Discovery Protocol (LLDP)
Emissions	IEEE 802.3at/af /.bt=> Power Over Ethernet (PoE)
Immunity	EN55022 (CISPR 22) Class A EN 61000-3 FCC Class A CE Mark
	EN 61000-4-2/3/4/5/6/8/11 EN 55024

Compliances

10Base-T	IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3, 4, or 5 UTP cable.
100Base-T	IEEE 802.3u specification for 100 Mbps Ethernet over two pairs of Category 5 UTP cable.
1000Base-LH	Specification for long-haul Gigabit Ethernet over two strands of 9/125 micron core fiber cable.
1000Base-LX	IEEE 802.3z specification for Gigabit Ethernet over two strands of 50/125, 62.5/125, or 9/125-micron core fiber cable.
1000Base-SX	IEEE 802.3z specification for Gigabit Ethernet over two strands of 50/125 or 62.5/125-micron core fiber cable.
1000Base-T	IEEE 802.3ab specification for Gigabit Ethernet over 100-ohm Category 5, 5e, or 6 twisted-pair cable (using all four wire pairs).
Auto-Negotiation	Signaling method allowing each node to select its optimum operational mode (e.g. speed and duplex mode) based on the capabilities of the node to which it is connected.
Bandwidth	The difference between the highest and lowest frequencies available for network signals. Also synonymous with wire speed, the actual speed of the data transmission along the cable.
Collision Domain	Single CSMA/CD LAN segment.
CSMA/CD	CSMA/CD (Carrier Sense Multiple Access/Collision Detect) is the communication method employed by Ethernet, Fast Ethernet, and Gigabit Ethernet.
End Station	A workstation, server, or other device that does not forward traffic.
Ethernet	A network communication system developed and standardized by DEC, Intel, and Xerox, were using baseband transmission, CSMA/CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration into the OSI model and extends the physical layer and media with repeaters and implementations that operate on fiber, thin coax, and twisted-pair cable.

Fast Ethernet	A 100 Mbps network communication system based on Ethernet and the CSMA/ CD access method.
Full Duplex	Transmission method that allows two network devices to transmit and receive concurrently, effectively doubling the bandwidth of that link.
Gigabit Ethernet	A 1000 Mbps network communication system based on Ethernet and the CSMA/ CD access method.
IEEE	Institute of Electrical and Electronic Engineers.
IEEE 802.3	Defines carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.
IEEE 802.3AB	Defines CSMA/CD access method and physical layer specifications for 1000BASE-T Gigabit Ethernet (now incorporated in IEEE 802.3-2005).
IEEE 802.3U	Defines CSMA/CD access method and physical layer specifications for 100BASE- TX Fast Ethernet (now incorporated in IEEE 802.3- 2005).
IEEE 802.3X	Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links (now incorporated in IEEE 802.3-2005).
IEEE 802.3Z	Defines CSMA/CD access method and physical layer specifications for 1000BASE Gigabit Ethernet (now incorporated in IEEE 802.3-2005).
IEEE 802.3at/af	Defines Power Over Ethernet is used to transmit electrical power, PoE IEEE 802.3af (Class 4 PDs limited to 15.4W), PoE++ IEEE 802.3at (Class 4 PDs limited to 30W).
Lan Segment	Separate LAN or collision domain.
LED	Light emitting diode used for monitoring a device or network condition.
Local Area Network (LAN)	A group of interconnected computer and support devices.
Media Access Control (MAC)	A portion of the networking protocol that governs access to the transmission medium, facilitating the exchange of data between network nodes.
MIB	An acronym for Management Information Base. It is a set of database objects that contain information about the device.
Modal Bandwidth	Bandwidth for multimode fiber is referred to as modal bandwidth because it varies with the modal field (or core diameter) of the fiber. Modal bandwidth is specified in units of MHz per km, which indicates the amount of bandwidth supported by the fiber for a one km distance.
Network Diameter	Wire distance between two end stations in the same collision domain.
RJ-45 Connector	A connector for twisted-pair wiring.
Switched Ports	Ports that are on separate collision domains or LAN segments.

TIA	Telecommunications Industry Association.
Transmission Control Protocol/Internet Protocol (TCP/IP)	Protocol suite that includes TCP as the primary transport protocol and IP as the network layer protocol.
User Datagram Protocol (UDP)	UDP provides a datagram mode for the packet-switched communications. It uses the IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection- less data grams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.
UTP	Unshielded twisted-pair cable.
Virtual LAN (VLAN)	A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, allowing users to share information and resources as though located on the same LAN.

Warranty

Vigitron, Inc. guarantees that all Vigitron products (“Product”), if used in accordance with these instructions, will be free of defects in material and workmanship for a lifetime defined as the duration period of time until product end of life is announced.

After which, Vigitron will continue to provide warranty services for a period of 3 years. The period covering valid warranty will be determined by proof of purchase in the form of an invoice from an authorized Vigitron dealer.

Warranty will only be provided for as long as the original end-user purchaser owns the product. The warranty is not transferrable. At Vigitron's option, the defective product will be repaired, replaced, or substituted with a product of equal value. This warranty does not apply if in the judgment of Vigitron, Inc., the Product fails due to damage from shipment, handling, storage, accident, abuse, or misuse, or if it has been used or maintained not conforming to product manual instructions, has been modified, or serial number removed or defaced. Repair by anyone other than

Vigitron, Inc. or an approved agent will void this warranty. Vigitron, Inc. shall not under any circumstances be liable to any person for any incidental, indirect, or consequential damages, including damages resulting from use or malfunction of the product, loss of profits or revenues, or costs of replacement goods. The maximum liability of Vigitron, Inc. under this warranty is limited to the original purchase price of the product only.

Contact Information

Vigitron, Inc.

]7810 Trade Street, Suite 100 San Diego, CA 92121
Phone: 858-484-5209
Fax: (858) 484-1205
www.vigitron.com
support@vigitron.com

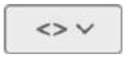
GUI Header Controls

When completing a programming function press the "Save" button. This will save the function when you exit the mode or if power is lost.

Use this in the event you what to change the programming. Note all programming with a mode will be reset and require reprogramming.

Some programming functions can have more than one setting mode. Selecting Add allows for programming additional settings. Remember to use the Save or Rest functions for each setting you add.

Use the Refresh to update the screen.



Where active this indicates, the programming selected applies to all ports or actions.

The house Icon returns the GUI to the home page which shows a graphical display of the Vi30208U and its active ports- Moving the curser over a port will display its name. Clicking on the port will show its its detailed Statistics.

The Arrow icon will ask if you want to log out of the website.

The Question icon will provide details on the page you are on

WEB Configuration
Chapter1: Configuration Preparation

1.1 Access to Switch by WEB

Important Note: Your choice of Internet browser can affect your ability to access the switch and/or certain switch functions. If you experience these problems, please check the browser security settings.

Ensure it is coincident with the following requirements while accessing to the switch by Web browser.

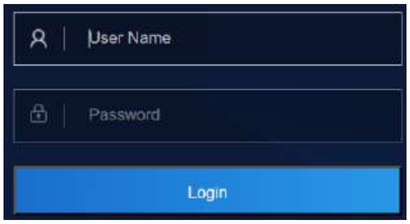
- HTML Version 4.0
- HTTP Version 1.1
- JavaScript™ Version 1.5

Besides, ensure the operation of the main program file supports to access to the switch, and the computer is connecting to the network of a switch.

First time access to switch, you don't need additional configuration but access to switch directly by WEB if this the first time to use. Revise the IP address of your computer ethernet adapter to"192.168.0. xxx" there the last three digits are different from the Vi30208U. The subnet mask is "255.255.255.0".

Open the WEB browser, enter the "192.168.0.1" in the address bar, note that "192.168.1.130" is the defaulted IP address of switch.

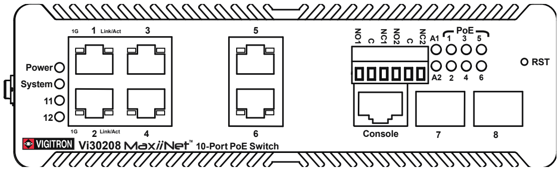
The dialog is appeared like picture 1 if you use Internet Explorer. Enter the account and passwords in the authenticated dialog, the original user name is "admin" and the password is "admin". Please distinguish the capital and small letter.



Picture 1: WEB Authentication Dialog.

Default username: admin
Default password: admin

Reset key – default function:



1. Press the front panel reset button.
2. Within 10 seconds press and hold the reset button on the front panel
3. The LED front panel lights will turn on.
4. When the front panel LEDs turn on release the reset button
5. When the front panel LEDs turn off the switch will be reset to default settings

The browser will display the system information page if it's authenticated successfully.
After Reset is complete, recheck your programming as some setting may need to be reprogrammed.

Ports 1-6 are independent UTP uplink ports. Ports 7 and 8 are independent fiber ports.

After Reset is complete, recheck your programming as some setting may need to be reprogrammed.

Insert Information Page

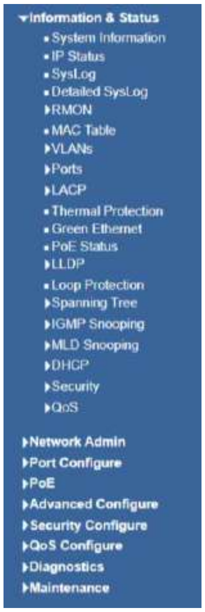
System Information Page of Switch

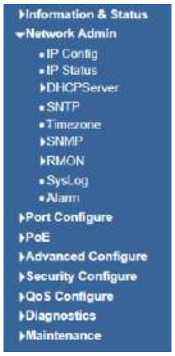
WEB Page Introduction
Order, Guide, Configuration System Display, Top Control and etc.

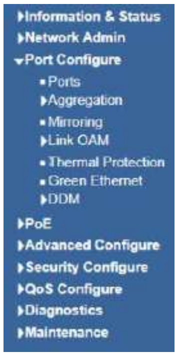
This is the log out button and will log out of the GUI.

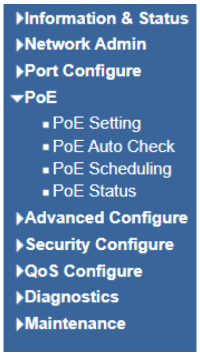
This Show Help button. It helps engineers to set the specification of devices. There's a specific page of each function set page. You can click it to display the function page anytime.

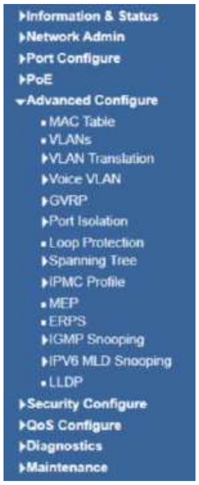
1.2 Guide

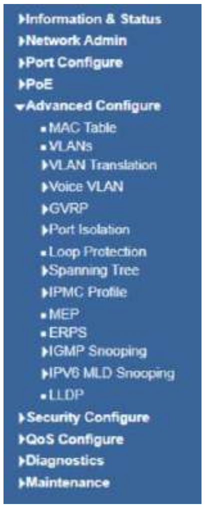


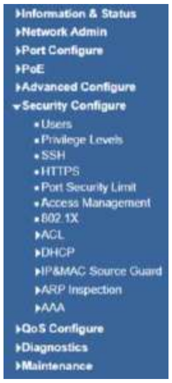


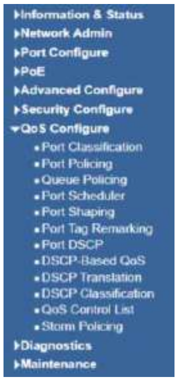


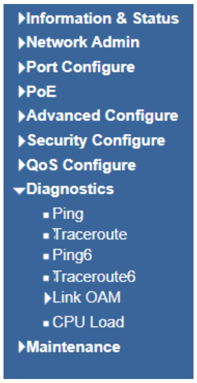


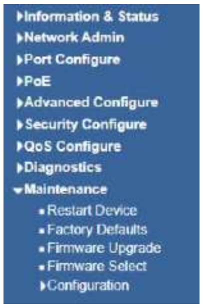








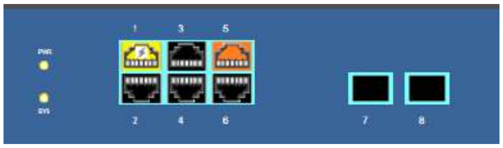




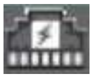
1.3 Top Control

UPDATE

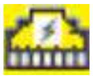
Note: The restricted user can't revise the device configuration but only visits the state. If they log in to the WEB, the other groups are disappeared but only the device state.



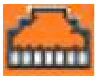
The state information and configuration of the device are shown in the Configuration Display. You can change the details by clicking the list items.



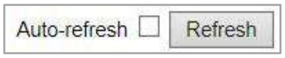
Link down but PoE Present



Link up and PoE Present



Link up, no PoE and Bandwidth indication



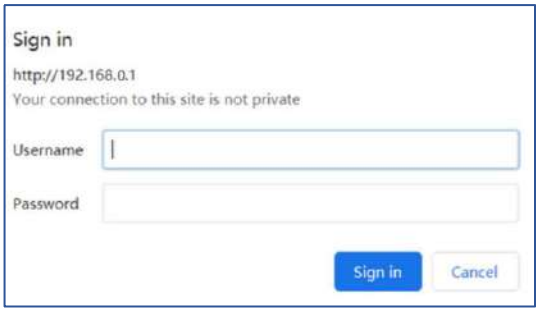
Achieving the Auto-refresh of Configuration Display is the vital function of Top Control. For example, you can monitor the port statistics continuedly by selecting view firstly and clicking Auto-refresh later. The screen will auto-refresh 1/3s.

Click “Clear” button can clear. It’s suggested that don’t use the Auto-refresh function for it’ll surely result in traffic unless it’s connected in LAN directly.

After program is complete it must be saved to start up otherwise it powers it lost settings will revert back to default.

To Save your programming use Maintenance>Configuration>Save startup.

1.4 Login Windows



Sign in

http://192.168.0.1

Your connection to this site is not private

Username

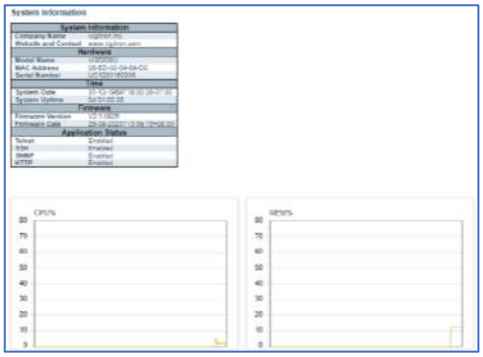
Password

Figure1-4 Login Window

Default Username: admin Default Password: admin

1.5 Access the GUI

After entering the username and password, the main screen appears as follows.



System Information

System Information	
Company Name	[illegible]
Website and Contact	[illegible]
Hardware	
Model Name	[illegible]
MAC Address	[illegible]
Serial Number	[illegible]
Time	
System Date	[illegible]
System Uptime	[illegible]
Firmware	
Firmware Version	[illegible]
Firmware Date	[illegible]
Application Status	
Telnet	Disabled
SSH	Enabled
SNMP	Enabled
HTTP	Enabled

Figure1-5 Web Management Main Page interface.

This Main Page interface includes mainly 3 parts. Here is description:

Part	Description
Part 1	Company Logo; Working Indicators; Port Indicators, including PoE and link working status; Language selection button (Chinese/English); Help document;
Part 2	The Main Menu, lets you access all the commands and statistics.
Part 3	Main Screen, showing configuration details.
Part 4	Screen shows CPU % and Memory Capacity

The Web agent displays an image of the Managed Switch's ports. Different colors mean different states, they are illustrated as follows:

Using the onboard Web agent, you can define system parameters, manage, and control the Managed Switch, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can set up the managed Switch by selecting the functions those listed in the Main Menu. Following is short description:

🟨 :10/100M linked, 🟩 :1000M Linked; ⬛ :No Link; ⚡ :PoE Link;

1.6 Main Menu

Information & status - Users can check switch information and working status under this menu.
Network Admin - Users can check and configure related features of network under this menu.

Port Configure - Users can check and configure specification of ports under this menu.

PoE - Users can check and configure related features of Power-over-Ethernet (PoE) under this menu.

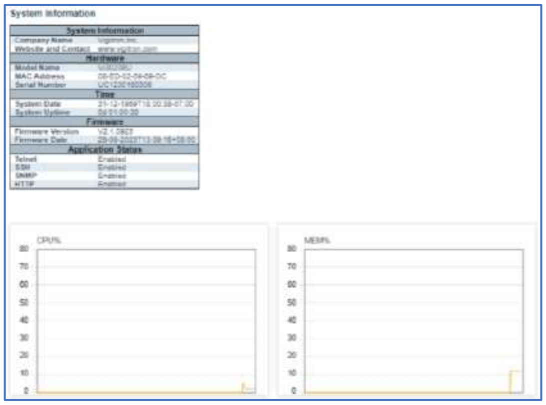
Advanced Configure - Users can check and configure L2 advanced features under this menu.
Security Configure - Users can check and configure security features of the switch under this menu.

Qos Configure - Users can check and configure Qos features of the switch under this menu.

Chapter 2: Information & Status

2.1 System information

In this section, the pages show the basic information of the switch and status of functions/features setting. Clients can go to different sections to check detailed guidance to make the function work.



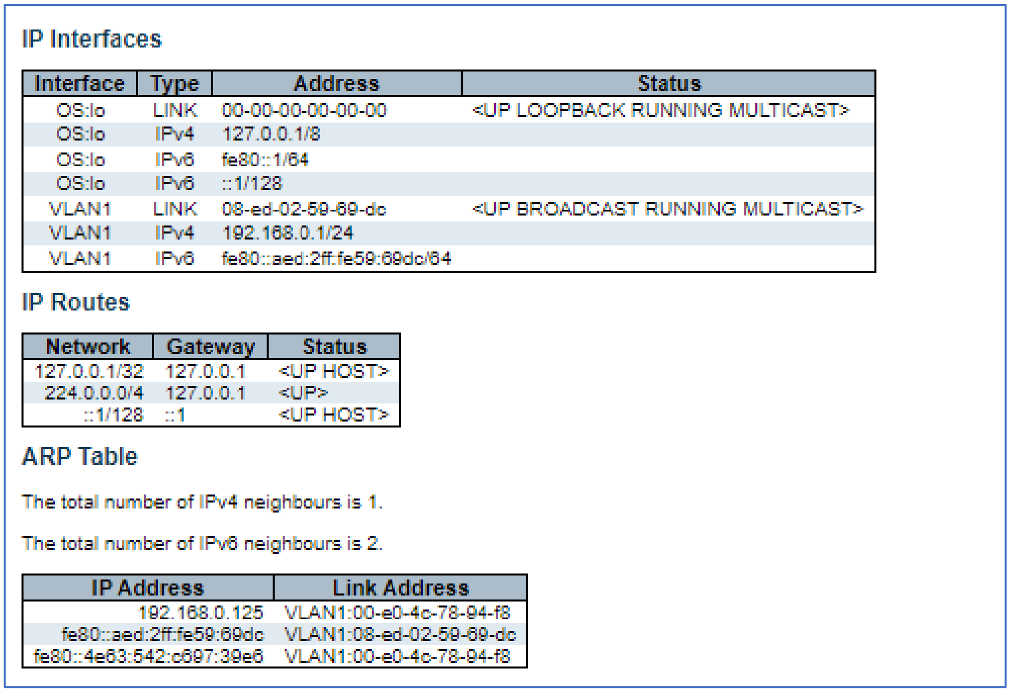
System Information

System Information	
Company Name	Vigitron Inc.
Website and Contact	www.vigitron.com
Hardware	
Model Name	[illegible]
MAC Address	08-ED-02-59-69-DC
Serial Number	UC1220180308
Time	
System Date	31-12-1969T16:20:38-07:00
System Uptime	0d 01:00:20
Firmware	
Firmware Version	V2.1.0807
Firmware Date	29-08-2022T13:09:16+08:00
Application Status	
Telnet	Enabled
SSH	Enabled
SNMP	Enabled
HTTP	Enabled

Figure 2-1 System Information Screen

After click "Information & Status" > "IP Status", followed screen will appear as:
Clients can go to Section" Network Admin" > "IP Configuration" to do the detailed management.

2.2 IP Statues



IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	08-ed-02-59-69-dc	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.1/24	
VLAN1	IPv6	fe80::aed:2ff:fe59:69dc/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

ARP Table

The total number of IPv4 neighbours is 1.

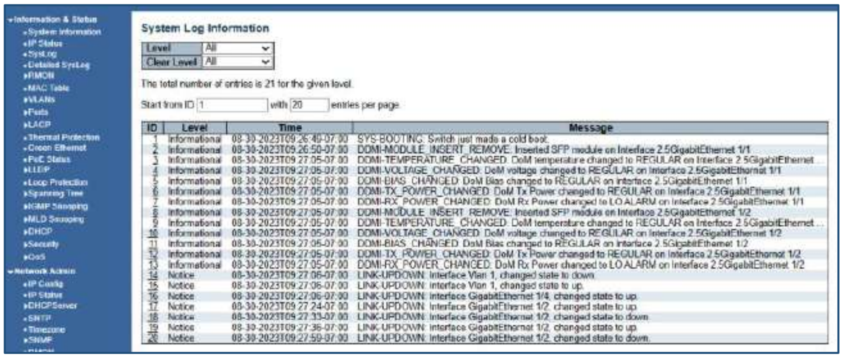
The total number of IPv6 neighbours is 2.

IP Address	Link Address
192.168.0.125	VLAN1:00-e0-4c-78-94-f8
fe80::aed:2ff:fe59:69dc	VLAN1:08-ed-02-59-69-dc
fe80::4e63:542:c697:39e6	VLAN1:00-e0-4c-78-94-f8

Figure 2-2 System Information Screen

2.3 Syslog

After click "Information & Status" > "System Information", followed screen will appear as:
Clients can go to Section" Network Admin" > "System Log Configuration" to do the detailed management.



System Log Information

Level	All
Clear Level	All

The total number of entries is 21 for the given level.

Start from ID 1 with 20 entries per page.

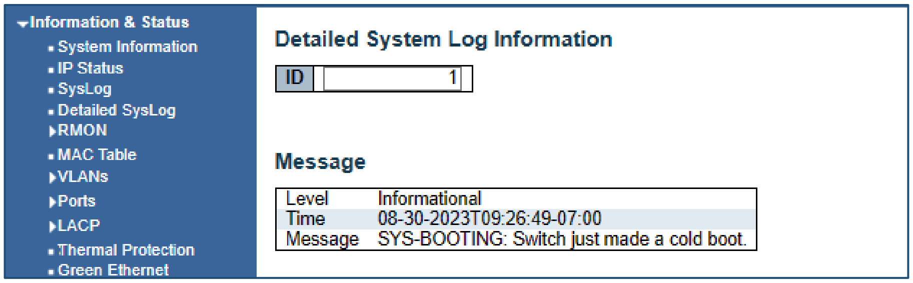
ID	Level	Time	Message
1	Informational	08-30-2023T09:26:49-07:00	SYS-BOOTING: Switch just made a cold boot.
2	Informational	08-30-2023T09:26:50-07:00	DOMI-MODULE_INSERT_REMOVE: Inserted SFP module on Interface 2.5GigabitEthernet 1/1
3	Informational	08-30-2023T09:27:05-07:00	DOMI-TEMPERATURE_CHANGED: DoM temperature changed to REGULAR on Interface 2.5GigabitEthernet ...
4	Informational	08-30-2023T09:27:05-07:00	DOMI-VOLTAGE_CHANGED: DoM voltage changed to REGULAR on Interface 2.5GigabitEthernet 1/1
5	Informational	08-30-2023T09:27:05-07:00	DOMI-BIAS_CHANGED: DoM Bias changed to REGULAR on interface 2.5GigabitEthernet 1/1
6	Informational	08-30-2023T09:27:05-07:00	DOMI-TX_POWER_CHANGED: DoM Tx Power changed to REGULAR on Interface 2.5GigabitEthernet 1/1
7	Informational	08-30-2023T09:27:05-07:00	DOMI-RX_POWER_CHANGED: DoM Rx Power changed to LO ALARM on Interface 2.5GigabitEthernet 1/1
8	Informational	08-30-2023T09:27:05-07:00	DOMI-MODULE_INSERT_REMOVE: Inserted SFP module on Interface 2.5GigabitEthernet 1/2
9	Informational	08-30-2023T09:27:05-07:00	DOMI-TEMPERATURE_CHANGED: DoM temperature changed to REGULAR on Interface 2.5GigabitEthernet ...
10	Informational	08-30-2023T09:27:05-07:00	DOMI-VOLTAGE_CHANGED: DoM voltage changed to REGULAR on Interface 2.5GigabitEthernet 1/2
11	Informational	08-30-2023T09:27:05-07:00	DOMI-BIAS_CHANGED: DoM Bias changed to REGULAR on interface 2.5GigabitEthernet 1/2
12	Informational	08-30-2023T09:27:05-07:00	DOMI-TX_POWER_CHANGED: DoM Tx Power changed to REGULAR on Interface 2.5GigabitEthernet 1/2
13	Informational	08-30-2023T09:27:05-07:00	DOMI-RX_POWER_CHANGED: DoM Rx Power changed to LO ALARM on Interface 2.5GigabitEthernet 1/2
14	Notice	08-30-2023T09:27:06-07:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
15	Notice	08-30-2023T09:27:06-07:00	LINK-UPDOWN: interface Vlan 1, changed state to up.
16	Notice	08-30-2023T09:27:06-07:00	LINK-UPDOWN: interface GigabitEthernet 1/4, changed state to up.
17	Notice	08-30-2023T09:27:24-07:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to up.
18	Notice	08-30-2023T09:27:33-07:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to down.
19	Notice	08-30-2023T09:27:36-07:00	LINK-UPDOWN: interface GigabitEthernet 1/2, changed state to up.
20	Notice	08-30-2023T09:27:50-07:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to down.

Figure 2-3 Syslog Screen

Note the correct time/date displayed is dependent upon setting the Time Zone programming found in the Network Administration section.

2.4 Detailed Syslog

After click "Information & Status" > "Detailed Syslog", followed screen will appear as:
Clients can go to Section” Network Admin” > "System Log Configuration" to do the detailed management.



Detailed System Log Information

ID	1

Message

Level	Informational
Time	08-30-2023T09:26:49-07:00
Message	SYS-BOOTING: Switch just made a cold boot.

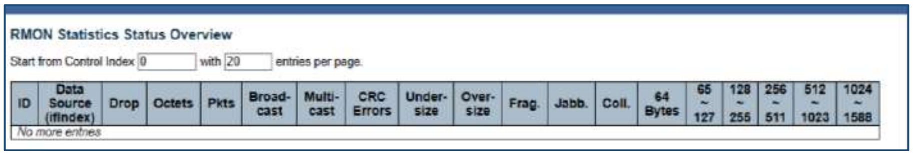
2.4 Detailed Syslog

2.5 RMON

Remote Monitoring (RMON) is a standard specification that facilitates the monitoring of network operational activities through the use of remote devices known as monitors or probes. RMON assists network administrators (NA) with efficient network infrastructure control and management.

The follow will show results if RMON monitoring is programmed in the Network Administration section.

2.5.1 Statistics



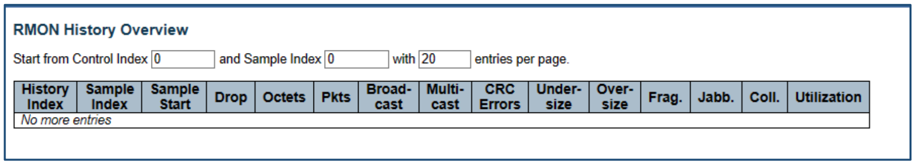
RMON Statistics Status Overview

Start from Control Index 0 with 20 entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

2.5.1 Statistics

2.5.2 History Overview

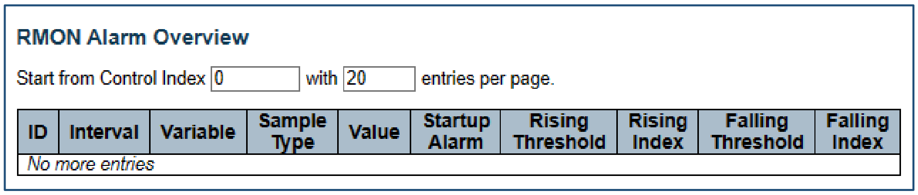


RMON History Overview

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

2.5.2 History Overview

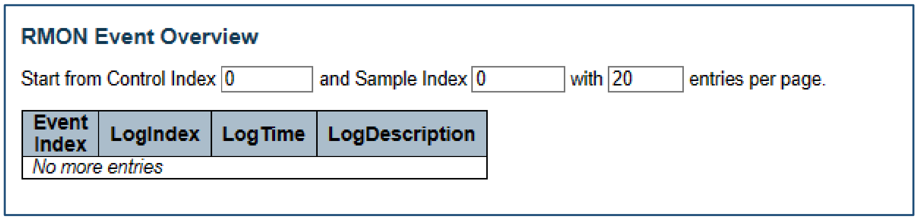


RMON Alarm Overview

Start from Control Index 0 with 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

2.5.3 Alarm Overview



RMON Event Overview

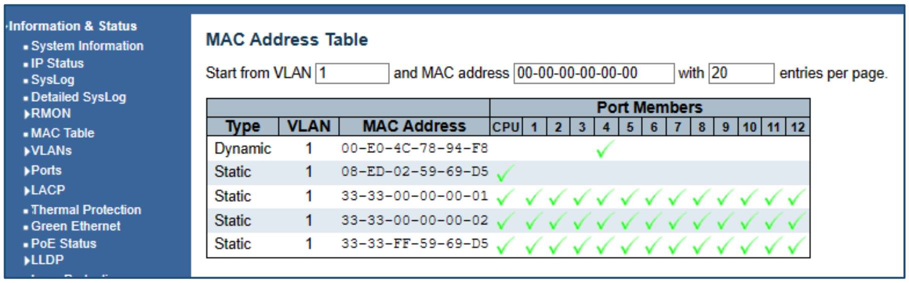
Start from Control Index 0 and Sample Index 0 with 20 entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

2.5.4 ROMN Event Overview

2.6 MAC Table

After click "Information & Status" > "Mac Table", followed screen will appear as:
Clients can go to Section “Advanced Configure” > "MAC Address Table" to do the detailed management.



MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

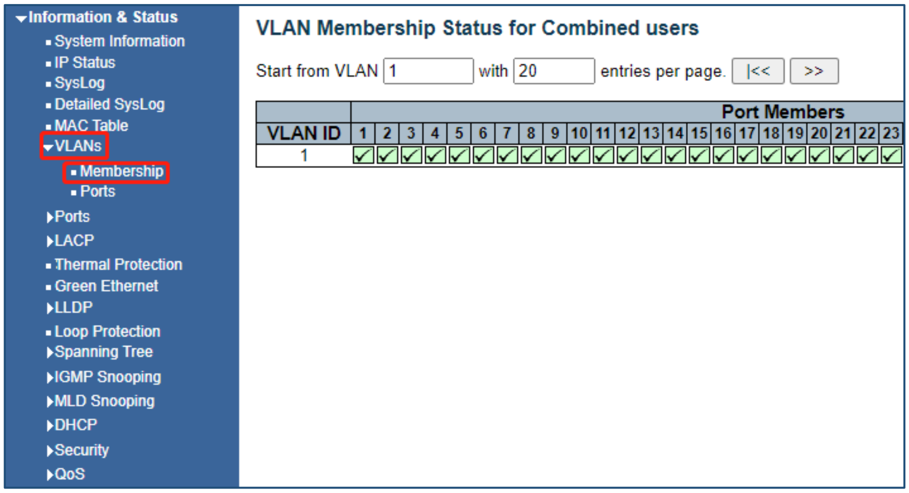
			Port Members												
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12
Dynamic	1	00-E0-4C-78-94-F8					✓								
Static	1	08-ED-02-59-69-D5	✓												
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-59-69-D5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 2-6 Mac Table Screen

2.7 VLANs

After click "Information & Status" > "Vlans", followed screen will appear as:
Clients can go to Section “Advanced Configure” > "Vlan" to do the detailed management.

2.7.1 Membership Screen



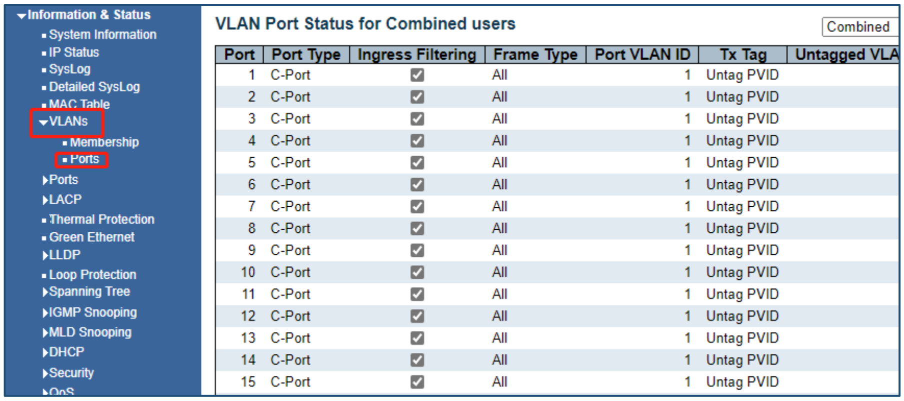
VLAN Membership Status for Combined users

Start from VLAN 1 with 20 entries per page. |<< >>

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

Figure 2-7-1 Membership Screen

2.7.2 Vlan Ports Screen



VLAN Port Status for Combined users

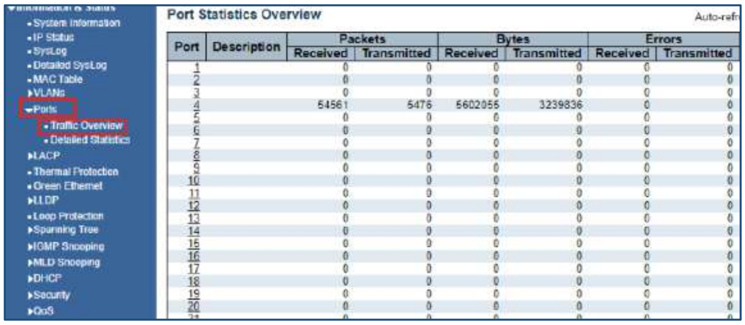
Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLA
1	C-Port	☑	All	1	Untag PVID	
2	C-Port	☑	All	1	Untag PVID	
3	C-Port	☑	All	1	Untag PVID	
4	C-Port	☑	All	1	Untag PVID	
5	C-Port	☑	All	1	Untag PVID	
6	C-Port	☑	All	1	Untag PVID	
7	C-Port	☑	All	1	Untag PVID	
8	C-Port	☑	All	1	Untag PVID	
9	C-Port	☑	All	1	Untag PVID	
10	C-Port	☑	All	1	Untag PVID	
11	C-Port	☑	All	1	Untag PVID	
12	C-Port	☑	All	1	Untag PVID	
13	C-Port	☑	All	1	Untag PVID	
14	C-Port	☑	All	1	Untag PVID	
15	C-Port	☑	All	1	Untag PVID	

Figure 2-7-2 Vlan Ports Screen

2.8 Ports

2.8.1 Traffic Overview Screen

After click "Information & Status" > "Ports", followed screen will appear as:
Clients can go to Section “Port Configure” > "Port Configuration" to do the detailed management.

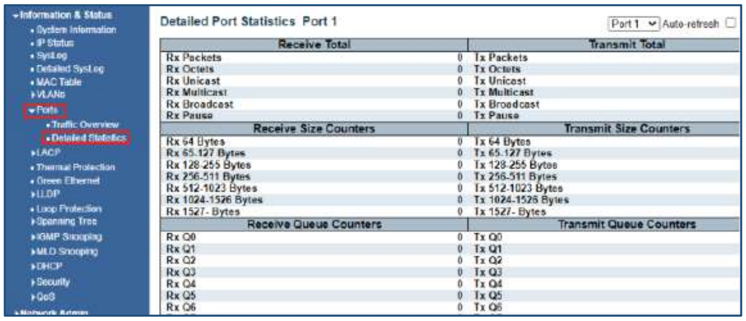


Port Statistics Overview

Port	Description	Packets		Bytes		Errors	
		Received	Transmitted	Received	Transmitted	Received	Transmitted
1		0	0	0	0	0	0
2		0	0	0	0	0	0
3		0	0	0	0	0	0
4		54561	5476	5602055	3239836	0	0
5		0	0	0	0	0	0
6		0	0	0	0	0	0
7		0	0	0	0	0	0
8		0	0	0	0	0	0
9		0	0	0	0	0	0
10		0	0	0	0	0	0
11		0	0	0	0	0	0
12		0	0	0	0	0	0
13		0	0	0	0	0	0
14		0	0	0	0	0	0
15		0	0	0	0	0	0
16		0	0	0	0	0	0
17		0	0	0	0	0	0
18		0	0	0	0	0	0
19		0	0	0	0	0	0
20		0	0	0	0	0	0

Figure 2-8-1 Ports-Traffic Overview Screen

2.8.2 Ports-Detailed Statistics Screen



Detailed Port Statistics Port 1

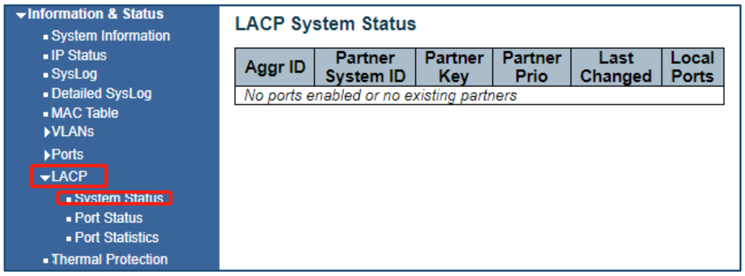
Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	
Rx Octets	0	Tx Octets	
Rx Unicast	0	Tx Unicast	
Rx Multicast	0	Tx Multicast	
Rx Broadcast	0	Tx Broadcast	
Rx Pause	0	Tx Pause	
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	0	Tx 64 Bytes	
Rx 65-127 Bytes	0	Tx 65-127 Bytes	
Rx 128-255 Bytes	0	Tx 128-255 Bytes	
Rx 256-511 Bytes	0	Tx 256-511 Bytes	
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	
Rx 1527- Bytes	0	Tx 1527- Bytes	
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	0	Tx Q0	
Rx Q1	0	Tx Q1	
Rx Q2	0	Tx Q2	
Rx Q3	0	Tx Q3	
Rx Q4	0	Tx Q4	
Rx Q5	0	Tx Q5	
Rx Q6	0	Tx Q6	

Figure 2-8-2 Ports-Detailed Statistics Screen

2.9 LACP

2.9.1 LACP System Status

After click "Information & Status" > "LACP", followed screen will appear as:
Clients can go to Section “Port Configure” > "Link Aggregation" > "LACP Aggregation" to do the detailed management.

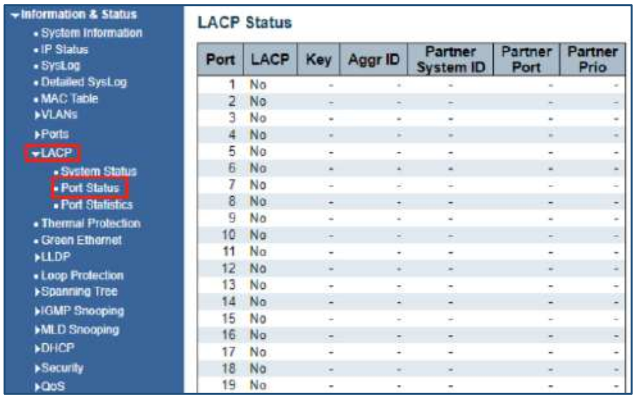


LACP System Status

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

Figure 2-9-1 LACP System Status Screen

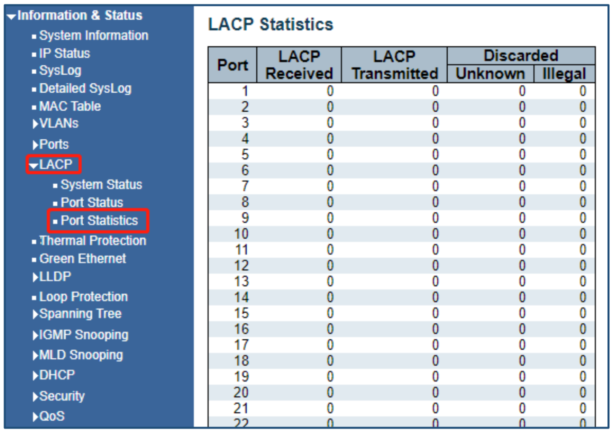
2.9.2 LACP Ports Status Screen



LACP Status

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

Figure 2-9-1 LACP Port Status



LACP Statistics

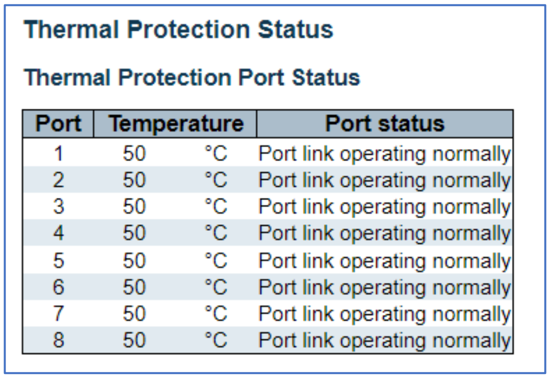
Port	LACP Received	LACP Transmitted	Discarded Unknown	Discarded Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0

Figure 2-9-1 LACP Port Statistics

2.10 Thermal Protection

After click "Information & Status" > "LACP", followed screen will appear as:
Clients can go to Section “Port Configure” > "Thermal Protection Configuration" to do the detailed management.

The programmed limit is 115C. Entering a higher number of results in a warning and will not be accepted.



Thermal Protection Status

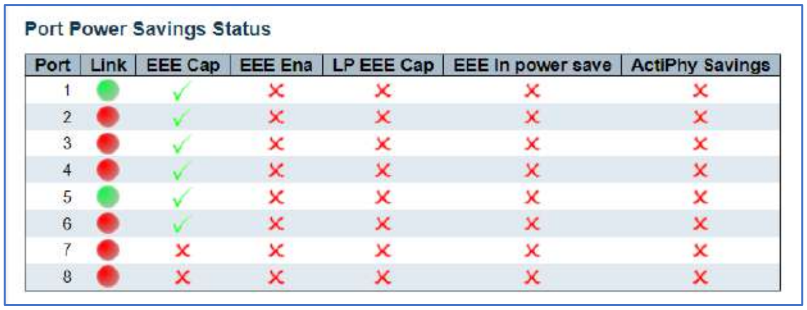
Thermal Protection Port Status

Port	Temperature	Port status
1	50 °C	Port link operating normally
2	50 °C	Port link operating normally
3	50 °C	Port link operating normally
4	50 °C	Port link operating normally
5	50 °C	Port link operating normally
6	50 °C	Port link operating normally
7	50 °C	Port link operating normally
8	50 °C	Port link operating normally

Figure 2-10 Thermal Protection Screen

2.11 Green Ethernet

After click "Information & Status" > "Green Ethernet", followed screen will appear as:
Clients can go to Section “Port Configure” > "Green Ethernet” to do the detailed management.

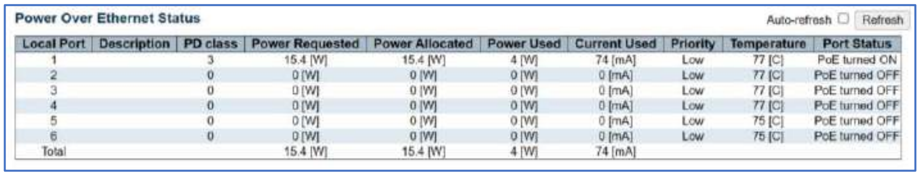


Port Power Savings Status

Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings
1	🟢	✓	✗	✗	✗	✗
2	🔴	✓	✗	✗	✗	✗
3	🔴	✓	✗	✗	✗	✗
4	🔴	✓	✗	✗	✗	✗
5	🟢	✓	✗	✗	✗	✗
6	🔴	✓	✗	✗	✗	✗
7	🔴	✗	✗	✗	✗	✗
8	🔴	✗	✗	✗	✗	✗

Figure 2-11 Green Ethernet Screen

2.11.1 PoE Status Screen



Power Over Ethernet Status

Auto-refresh ☐ Refresh

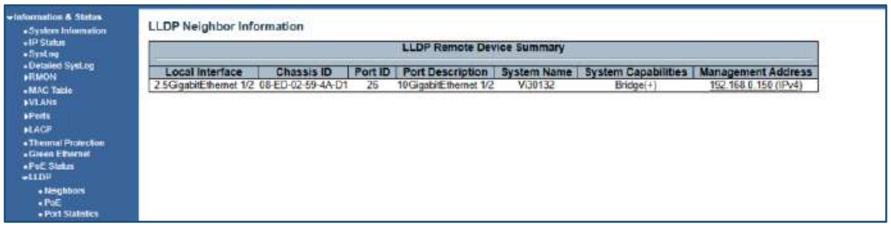
Local Port	Description	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Temperature	Port Status
1		3	15.4 [W]	15.4 [W]	4 [W]	74 [mA]	Low	77 [C]	PoE turned ON
2		0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	77 [C]	PoE turned OFF
3		0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	77 [C]	PoE turned OFF
4		0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	77 [C]	PoE turned OFF
5		0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	75 [C]	PoE turned OFF
6		0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	75 [C]	PoE turned OFF
Total			15.4 [W]	15.4 [W]	4 [W]	74 [mA]			

Figure 2.11.1 PoE Status Screen

2.11 LLDP

After click "Information & Status" > "LLDP", followed screen will appear as:
Clients can go to Section “Advanced Configure” > "LLDP” to do the detailed management.

2.11.1 Neighbor Information



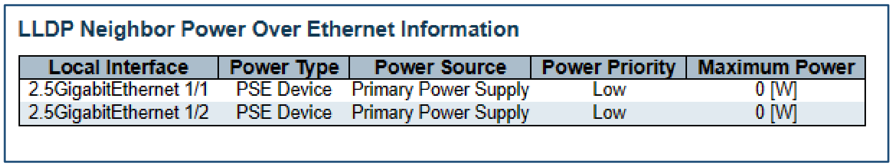
LLDP Neighbor Information

LLDP Remote Device Summary						
Local Interface	**Chassis ID**	**Port ID**	**Port Description**	**System Name**	**System Capabilities**	**Management Address**
2.5GigabitEthernet 1/2	08-ED-02-59-4A-D1	26	10GigabitEthernet 1/2	Vi30132	Bridge(+)	192.168.0.150 (IPv4)

Figure 2.11.1 Neighbor Information

If the network is connected to other devices capable of LLDP detection they will be displayed. To view this point and click to the underlined address under management address.

2.11.2 LLDP-Ports Statistics Screen

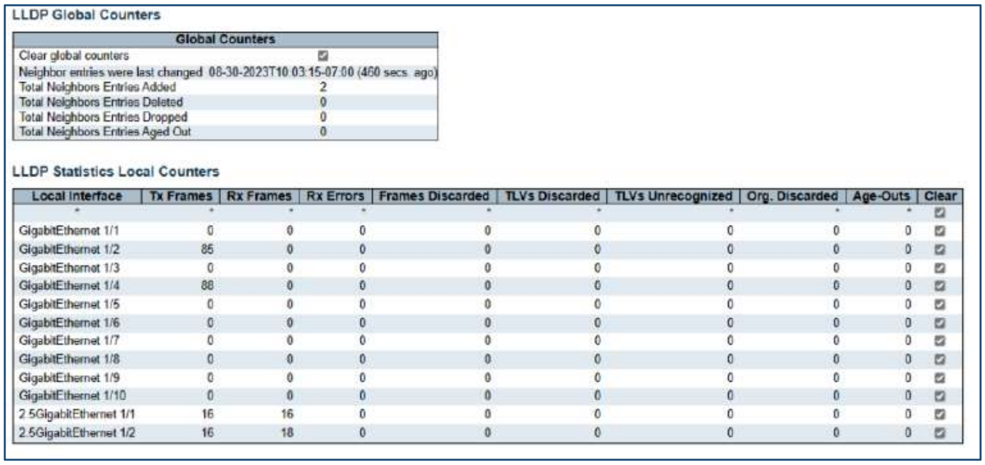


LLDP Neighbor Power Over Ethernet Information

Local Interface	Power Type	Power Source	Power Priority	Maximum Power
2.5GigabitEthernet 1/1	PSE Device	Primary Power Supply	Low	0 [W]
2.5GigabitEthernet 1/2	PSE Device	Primary Power Supply	Low	0 [W]

Figure 2-11-2 LLDP-Ports Statistics Screen

2.11.3 LLDP Global Counters



LLDP Global Counters

Global Counters	
Clear global counters	☑
Neighbor entries were last changed	08-30-2023T10:03:15-07:00 (460 secs. ago)
Total Neighbors Entries Added	2
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

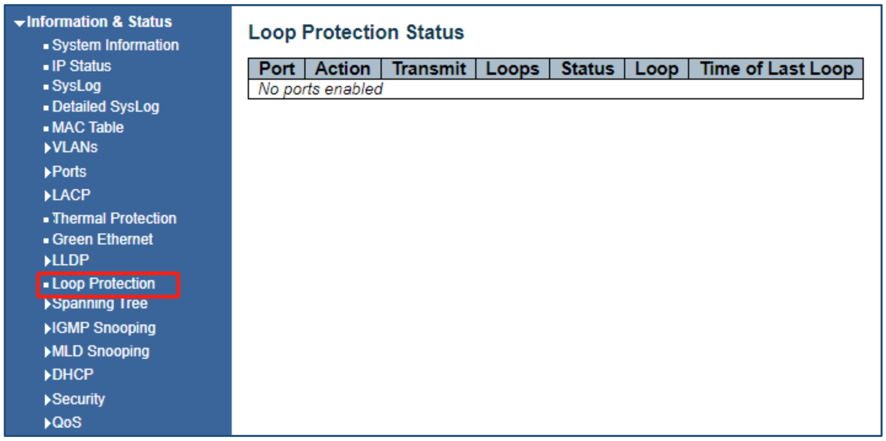
LLDP Statistics Local Counters

Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
*	*	*	*	*	*	*	*	*	☑
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/2	85	0	0	0	0	0	0	0	☑
GigabitEthernet 1/3	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/4	88	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	☑
2.5GigabitEthernet 1/1	16	16	0	0	0	0	0	0	☑
2.5GigabitEthernet 1/2	16	18	0	0	0	0	0	0	☑

Figure 2.11.3 LLDP Global Counters

2.12 Loop Protection

After click "Information & Status" > "Loop Protection", followed screen will appear as:
Clients can go to Section “Advanced Configure” > "Loop Protection" to do the detailed management.



Loop Protection Status

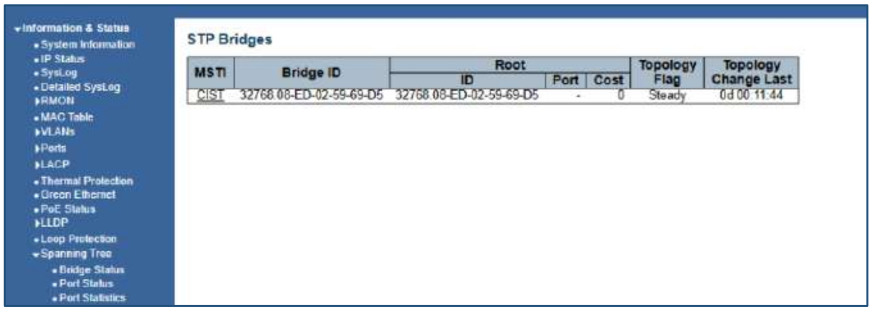
Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

Figure 2-12 Loop Protection Screen

2.13 Spanning Tree

After click "Information & Status" > "Loop Protection", followed screen will appear as:
Clients can go to Section “Advanced Configure” > "STP” to do the detailed management.

2.13.1 Bridge Status

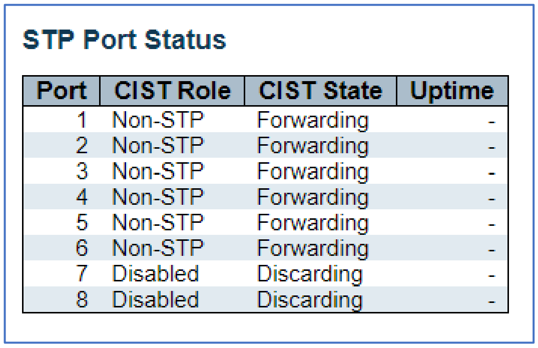


STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.08-ED-02-59-69-D5	32768.08-ED-02-59-69-D5	-	0	Steady	0d 00:11:44

Figure 2-13-1 Spanning Tree Bridge Status Screen

2.13.2 Port Status

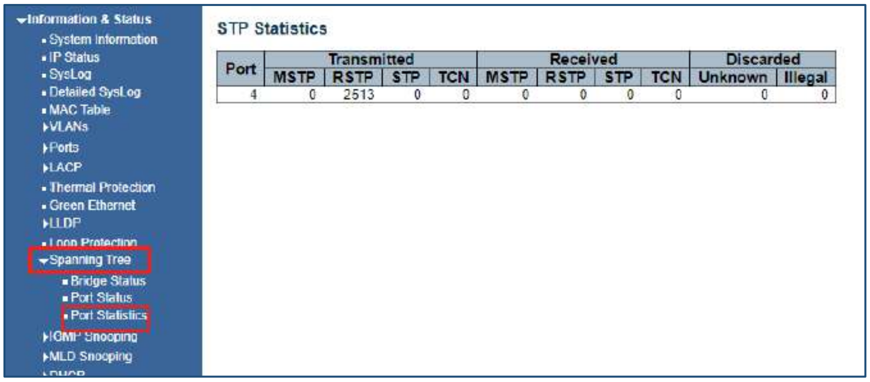


STP Port Status

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-

Figure 2-13-2 Spanning Tree Port Status Screen

2.13.3 Spanning Tree Port Statistics Screen



STP Statistics

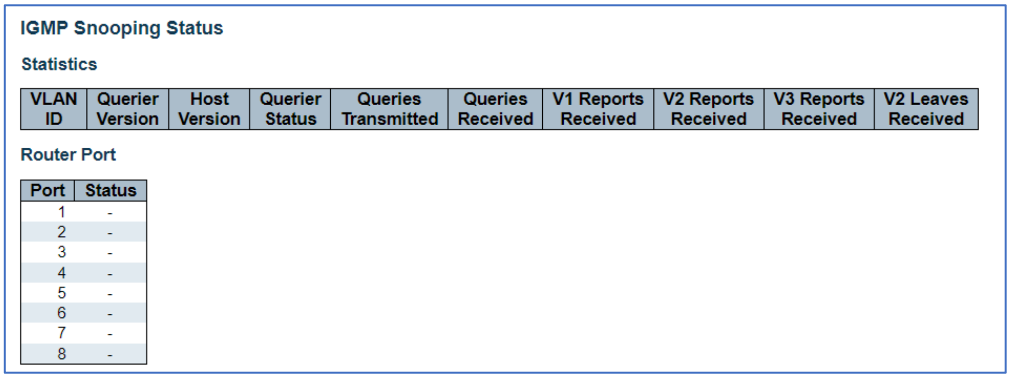
Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
4	0	2513	0	0	0	0	0	0	0	0

Figure 2-13-3 Spanning Tree Port Statistics Screen

2.14 IGMP Snooping

After click "Information & Status" > "IGMP Snooping", followed screen will appear as:
Clients can go to Section “Advanced Configure” > "IGMP Snooping” to do the detailed management.

2.14.1 IGMP Status



IGMP Snooping Status

Statistics

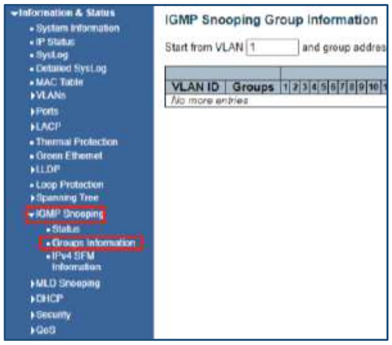
VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

Figure 2-14-1 IGMP Snooping Status Screen

2.14.2 IGMP Group Information

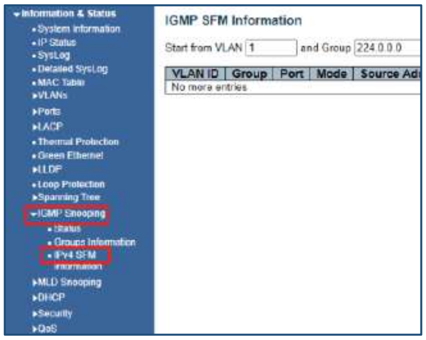


IGMP Snooping Group Information

Start from VLAN 1 and group addres

VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
No more entries											

Figure 2-14-2 IGMP Snooping Group Information Screen



IGMP SFM Information

Start from VLAN 1 and Group 224.0.0.0

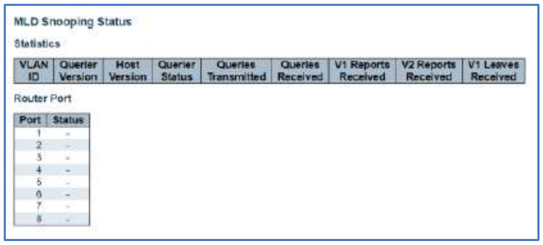
VLAN ID	Group	Port	Mode	Source Ad
No more entries				

Figure 2-14-3 IGMP Snooping IPv4 SFM Information Screen

2.15 MLD Snooping

2.15.1 MLD Status

After click "Information & Status" > "MLD Snooping", followed screen will appear as:
Clients can go to Section “Advanced Configure” > "IPV6 MLD Snooping” to do the detailed management.



MLD Snooping Status

Statistics

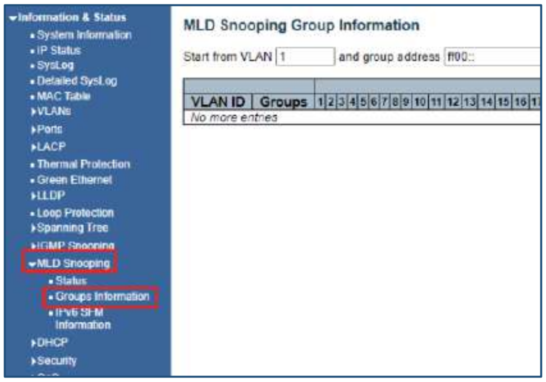
VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

Figure 2-15-1 MLD Snooping Status Screen

2.15.2 MLD Groups Information



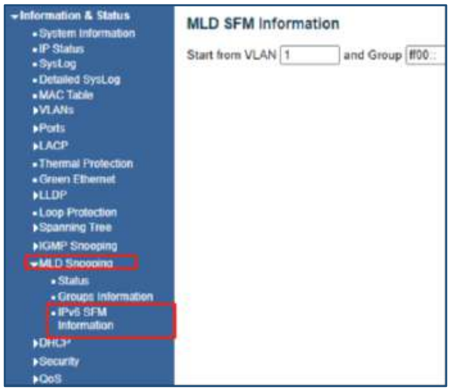
MLD Snooping Group Information

Start from VLAN 1 and group address ff00::

VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	1
No more entries																		

Figure 2-15-2 MLD Snooping Groups Information Screen

2.15.3 MLD IPv6 SFM Information



MLD SFM Information

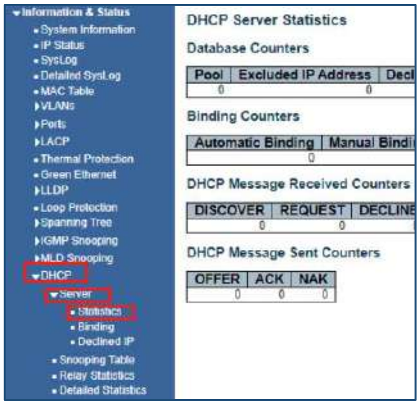
Start from VLAN 1 and Group ff00::

Figure 2-15-3 MLD Snooping IPv6 SFM Information Screen

2.16 DHCP

2.16.1 DHCP Server

After click "Information & Status" > "DHCP", followed screen will appear as: Clients can go to Section “DHCP” to do the detailed management.



DHCP Server Statistics

Database Counters

Pool	Excluded IP Address	Decl
0	0	

Binding Counters

Automatic Binding	Manual Bindi
0	

DHCP Message Received Counters

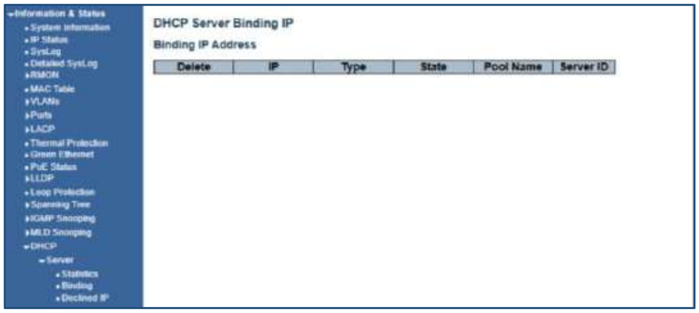
DISCOVER	REQUEST	DECLINE
0	0	

DHCP Message Sent Counters

OFFER	ACK	NAK
0	0	0

Figure 2-16-1 DHCP Server Statistics Screen

2.16.2 DHCP Binding



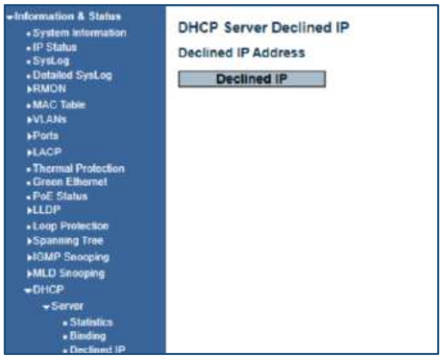
DHCP Server Binding IP

Binding IP Address

Delete	IP	Type	State	Pool Name	Server ID

Figure 2-16-2 DHCP Binding

2.16.3 DHCP Declined IP

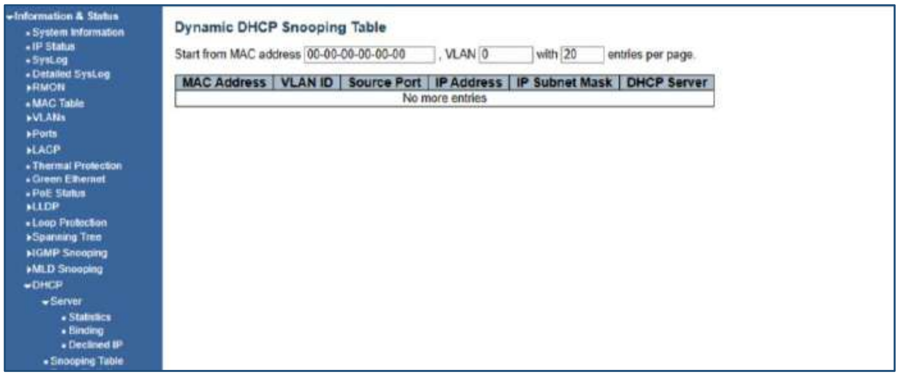


DHCP Server Declined IP

Declined IP Address

Figure 2-16-3 DHCP Declined IP

2.16.4 DHCP Snooping Table



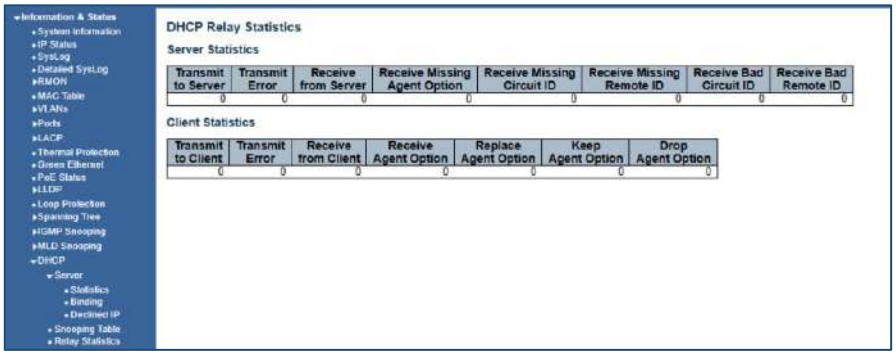
Dynamic DHCP Snooping Table

Start from MAC address 00-00-00-00-00-00 , VLAN 0 with 20 entries per page.

MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server
No more entries					

Figure 2-16-4 Dynamic DHCP Snooping Table

2.16.5 DHCP



DHCP Relay Statistics

Server Statistics

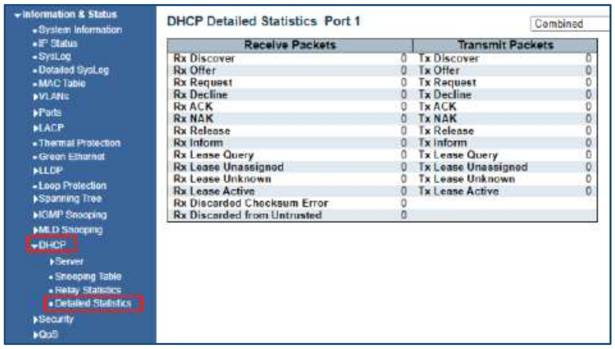
Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

Figure 2-16-5 DHCP Relay Statistics

2.16.6 Detailed Statistics



DHCP Detailed Statistics Port 1

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

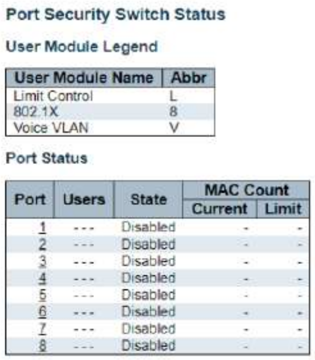
Figure 2-16-6 DHCP Detailed Statistics Screen

2.17 Security

After click "Information & Status" > "Security", followed the screen will appear as:
Clients can go to Section “Security Configure” to do detailed management.

2.17.1 Port Security

2.17.1.1 Port Security Switch



Port Security Switch Status

User Module Legend

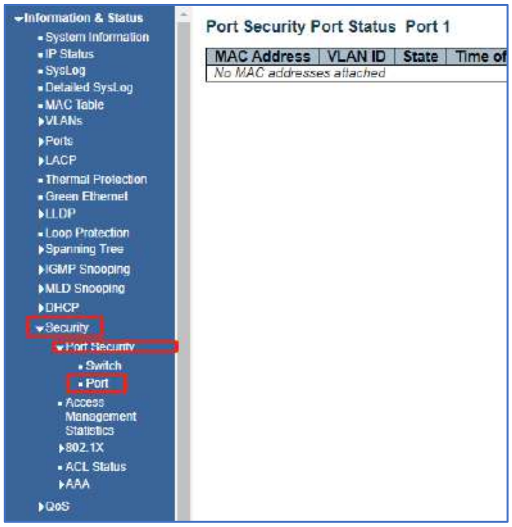
User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	---	Disabled	-	-
5	---	Disabled	-	-
6	---	Disabled	-	-
7	---	Disabled	-	-
8	---	Disabled	-	-

Figure 2-17-1-1 Security - Port Security - Switch Screen

2.17.1.2 Port Security Port

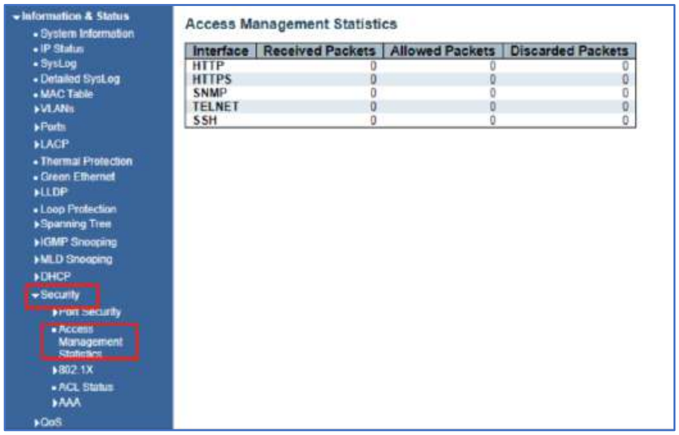


Port Security Port Status Port 1

MAC Address	VLAN ID	State	Time of
No MAC addresses attached			

Figure 2-17-1-2 Security - Port Security - Port Screen

2.17.2 Access Screen



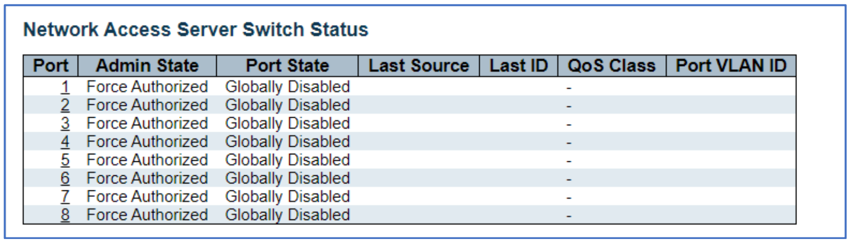
Access Management Statistics

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

Figure 2-17-3 Security - Port Security - Access Screen

2.17.3 Security – 802.1X

2.17.3.1 802.1x Switch Screen

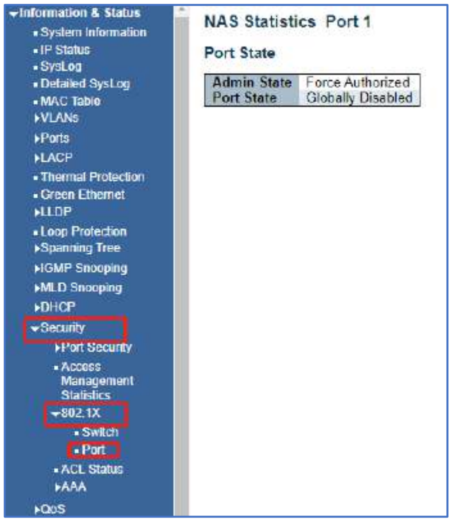


Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	

Figure 2-17-3.1 Security - 802.1X - Switch Screen

2.17.3.2 802.1x Port Screen



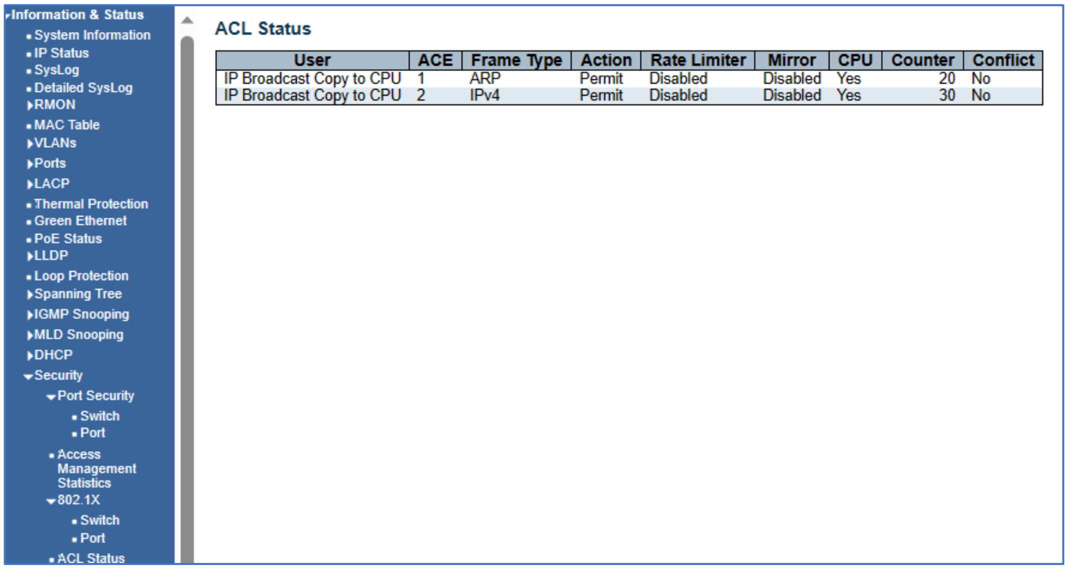
NAS Statistics Port 1

Port State

Admin State	Force Authorized
Port State	Globally Disabled

Figure 2-17-3.2 Security - 802.1X - Port Screen

2.17.4 ACL Status Screen



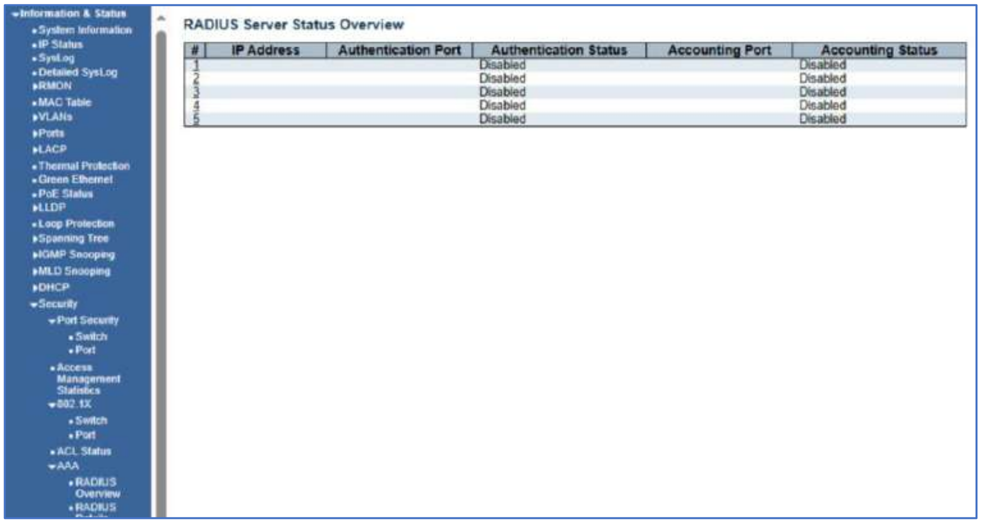
ACL Status

User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
IP Broadcast Copy to CPU	1	ARP	Permit	Disabled	Disabled	Yes	20	No
IP Broadcast Copy to CPU	2	IPv4	Permit	Disabled	Disabled	Yes	30	No

Figure 2-17-6 Security - ACL Status Screen

2.17.5 Security - AAA

2.17.5.1 AAA - Radius Overview Screen

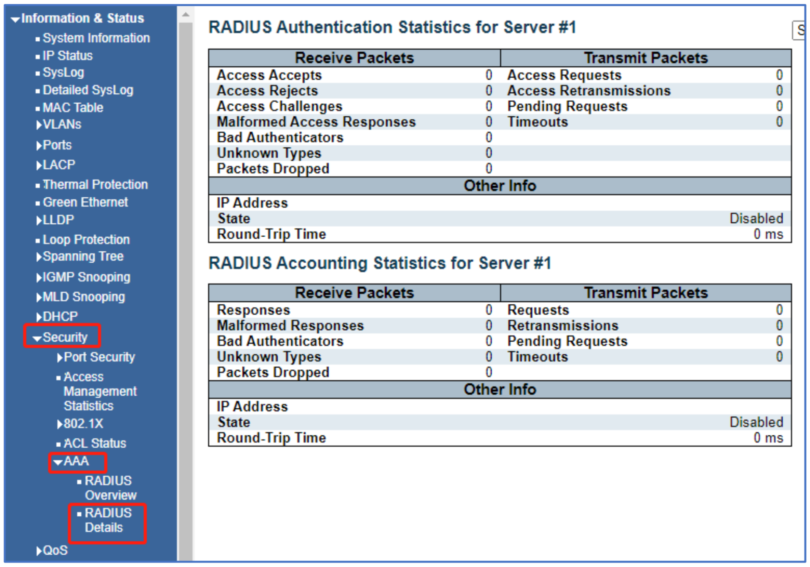


RADIUS Server Status Overview

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1			Disabled		Disabled
2			Disabled		Disabled
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

Figure 2-17-5.1 Security - AAA - RADIUS Overview Screen

2.17.5.2 AAA – Radius Details Screen



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			
State			Disabled
Round-Trip Time			0 ms

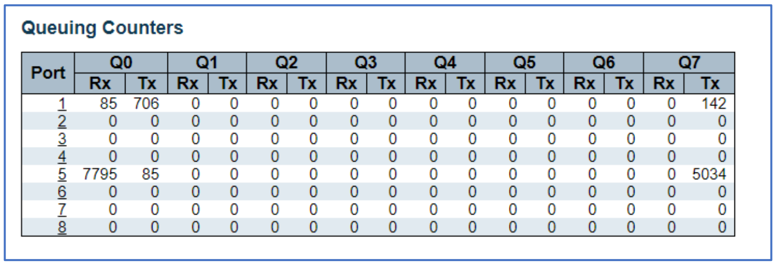
RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			
State			Disabled
Round-Trip Time			0 ms

Figure 2-17-5.2 Security - AAA - RADIUS Details Screen

2.18.1 QOS Statistics

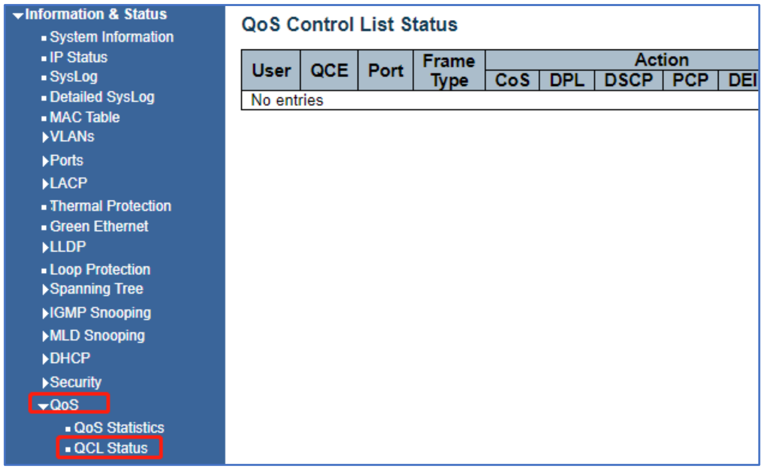
After click "Information & Status" > "Security", followed screen will appear as:
Clients can go to Section Configure” to do the detailed management.



Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	85	706	0	0	0	0	0	0	0	0	0	0	0	0	0	142
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	7795	85	0	0	0	0	0	0	0	0	0	0	0	0	0	5034
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 2-18-1 QOS Statistics Screen



QoS Control List Status

User	QCE	Port	Frame Type	Action				
				CoS	DPL	DSCP	PCP	DEI
No entries								

Figure 2-18-2 QOS Status Screen

Save — When completing a programming function press the “Save” button. This will save the function when you exit the mode or if power is lost.

Reset — Use this in the event you what to change the programming. Note all programming with a mode will be reset and require reprogramming.

Add — Some programming functions can have more than one setting mode. Selecting Add allows for programming additional settings. Remember to use the Save or Rest functions for each setting add

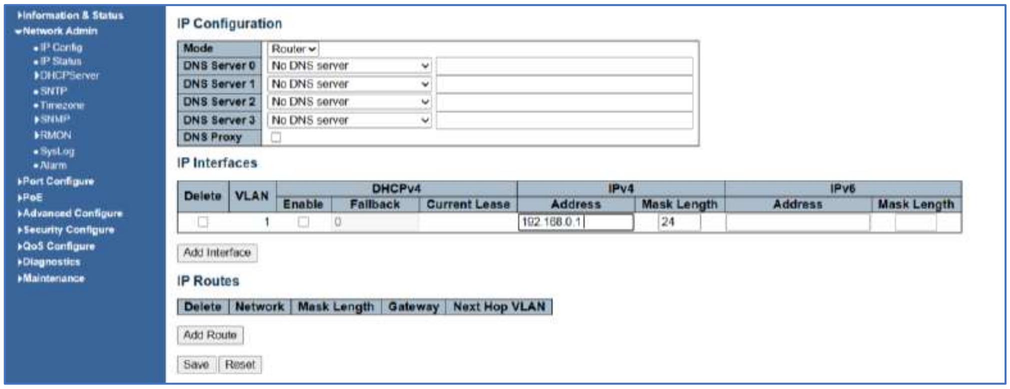
Refresh — Use the Refresh to update the screen.

<> ⌄ — Where active this indicates, the programming selected applies to all ports or actions.

3.1 IP Configuration

3.2 IP Status

Note: IP address of switch is 192.168.0.1 by default, and the default subnet mask is 255.255.255.0(24)
Click "Network Admin" > ''IP Config'', screen will show as:



IP Configuration

Mode	Router	
DNS Server 0	No DNS server	
DNS Server 1	No DNS server	
DNS Server 2	No DNS server	
DNS Server 3	No DNS server	
DNS Proxy	□	

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Address	Mask Length
□	1	□	0		192.168.0.1	24		

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN

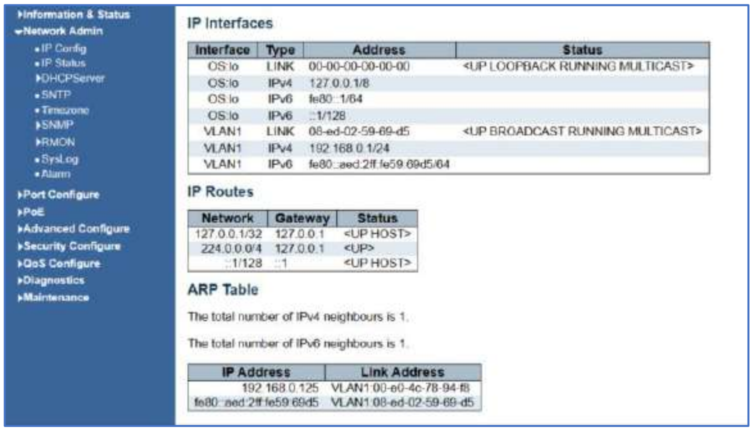
Figure 3-1 IP Configuration Screen

Following is description detail about IP configuration:

Name	Description
VLAN	VLAN for access and management of switch
IPv4 DHCP	- If enable, it means that VLAN port start IPv4 DHCP client, to dynamically get IPv4 addresses of the switch. Otherwise, it will use switch’s static IP configuration. - Fallback (Seconds) means the waiting time for switch to get dynamic IP address via DHCP. The value of "0" here means never over the time. - Current Lease, means the IP address get from DHCP
IPv4	- Address: static IPv4 address entered by user. - Mask Length: static IPv4 subnet mask entered by user.

Click ''Add Interface'' to create a new management for VLAN and IP address. Click ''Save'' to save settings.

3.2 IP Status



IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	08-ed-02-59-69-d5	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.1/24	
VLAN1	IPv6	fe80::aed:2ff:fe59:69d5/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

ARP Table

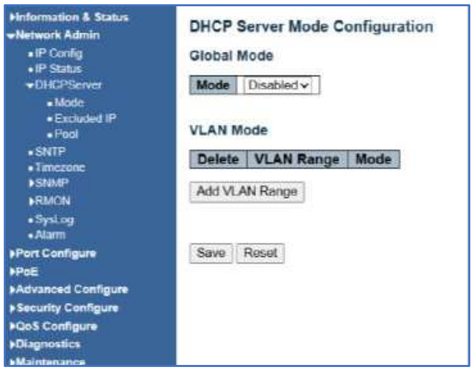
The total number of IPv4 neighbours is 1.

The total number of IPv6 neighbours is 1.

IP Address	Link Address
192.168.0.125	VLAN1:00-e0-4c-78-94-f8
fe80::aed:2ff:fe59:69d5	VLAN1:08-ed-02-59-69-d5

3.2 IP Status

3.3 DHCP Server



DHCP Server Mode Configuration

Global Mode

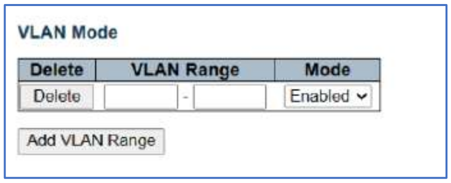
Mode	Disabled

VLAN Mode

Delete	VLAN Range	Mode

3.3.1 DHCP Server Mode Configuration

3.3.1 DHCP Mode

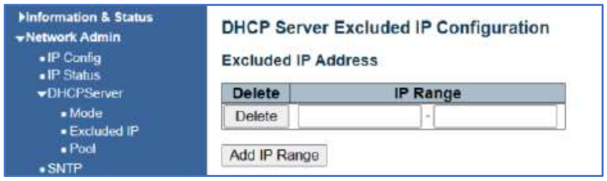


VLAN Mode

Delete	VLAN Range	Mode
Delete	-	Enabled

Name	Description
Enable	Enable or Disable VLAN range For DHCP
VLAN Range	- Range must be greater than 1
Enable Range	Enable all ranges to be used – you can use all programmed ranges
Add VLAN Range	Add additions VLANs- just make certain they are programmed

3.3.2 DHCP Server Excluded IP Configuration



DHCP Server Excluded IP Configuration

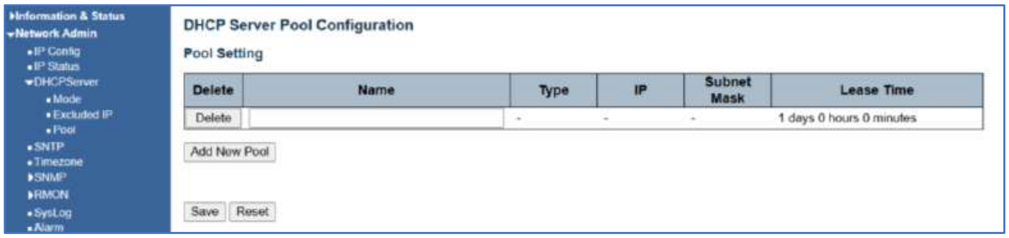
Excluded IP Address

Delete	IP Range
Delete	-

3.3.2 DHCP Server Excluded IP Configuration

Name	Description
Enter IP Range	Enter and IP range which will be allowed for DHCP. The range can consist of 1 more address
Delete	This action deletes the range
Add IP Range	This adds a new IP Range

3.3.3 DHCP Pool



DHCP Server Pool Configuration

Pool Setting

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

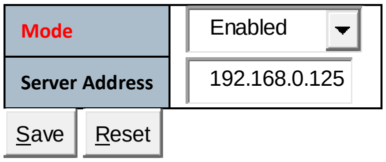
3.3.3 DHCP Sever Pool Configuration

Name	Description
Delete	Will Delete any entries
Name	You can assign a name to pool
Type	**Network:** This defines the IP addresses service by more than one DHCP client. **Host:** This defines the service for a specific DHCP Client as defined by the client address or hardware address. If this is not defined the display will show "-".
IP	**This will display the number of the DHCP pool. If this is not defined the display will show "-".**
Subnet Mask	**This displays the pool subnet mask. If this is not defined the display will show "-".**
Lease time	**The time the pool is active**
Add New Pool	**Use to add additional pools**

3.4 SNTP Configuration

NTP (Network Time Protocol) is a protocol used to synchronize the time of each computer in the network. Its purpose is to synchronize the clock of the computer to the world coordinates UTC, its accuracy can reach 0.1 ms in the LAN and 1-50 MS in most places on the Internet.

The Time Zone function can be use as the NTP reference.
Click "Network Admin" > "SNTP", screen will show as:



Mode	Enabled
Server Address	192.168.0.125

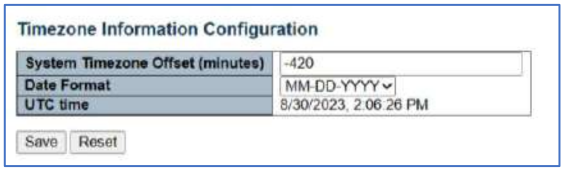
3.4.1 NTP Configuration

Name	Description
Enable	This enables the function
Server Address	Input the address of an NTP server or of the main computer running the VMS or other software

3.4.1 NTP Configuration Screen

3.5 Time Zone Information

Client can use time zone configuration to set system time zone offset (minutes), and Client can synchronize PC Web browser time to the switch local time as well which can be used as the sole reference.
Click "Network Admin" > "System Time", screen will show as:



Timezone Information Configuration

System Timezone Offset (minutes)	-420
Date Format	MM-DD-YYYY
UTC time	8/30/2023, 2:06:26 PM

3.5.1 Time Zone Information Configuration

Name	Description
System Time Zone Offset	Set the time (-) or (+) as determined by your time zone relationship to UTC time. To have the correct time and date displayed in functions such as Syslog- this setting must be correct
Date Format	Select the date format that matches your country
Save	Select Save and confirm the correct time and date form appears

3.5.1 Time zone Information Configuration

3.6 SNMP Configuration

Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

This switch support SNMPv1, v2c. Different versions of SNMP provides different security level for management stations and network devices.

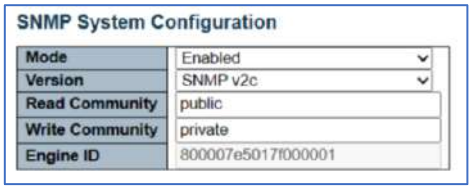
In SNMP's v1 and v2c, it uses the "Community String" for user authentication. That string is like password function. SNMP application of remote user and SNMP of the Switch must use the same community string. SNMP packets of any unauthorized sites will be ignored (discarded).

"Community String" by default for switch's SNMPv1 and v2c access management is:

1. public – allow authentication management station to read MIB objects.

Important Note: In order for your computer to receive SNMP messages it must have the MIB associated with the switch protocol. For a simpler method of messaging use Syslog

3.6.1 SNMP System Configuration



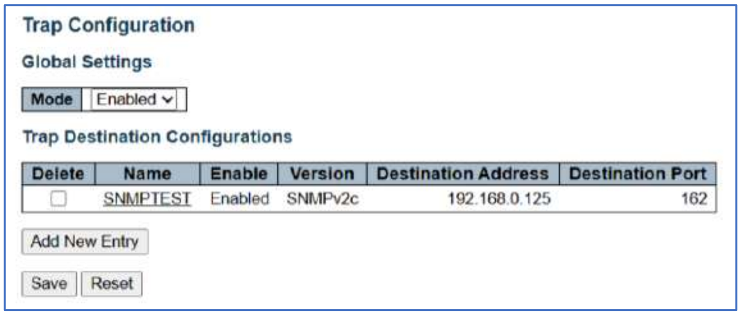
SNMP System Configuration

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

Figure 3.6.1 SNMP System Configuration

Name	Description
Enable/Disable	This enables or disables the SNMP function
Version	Select the version depending on the level of security required
Read Community	Indicates the type of community that will be able to read the SNMP messages – the community will be dependent upon the SNMP Version
Write Community	Indicates the type of community that will the SNMP will able to write to – the community will be dependent upon the SNMP version
Engine ID	This is applied to SNMPv3 – changing this will clear all original users

3.6.2 Trap Configuration



Trap Configuration

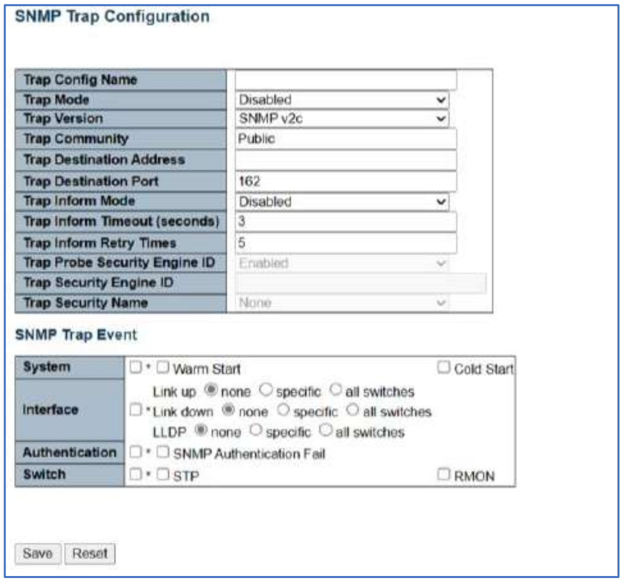
Global Settings

Mode	Enabled

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
□	SNMPTEST	Enabled	SNMPv2c	192.168.0.125	162

3.6.2 Trap Configuration – Global Settings



SNMP Trap Configuration

Trap Config Name	
Trap Mode	Disabled
Trap Version	SNMP v2c
Trap Community	Public
Trap Destination Address	
Trap Destination Port	162
Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled
Trap Security Engine ID	
Trap Security Name	None

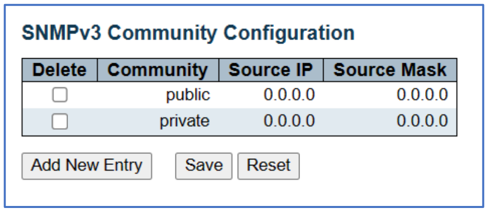
SNMP Trap Event

System	□ * □ Warm Start □ Cold Start
Interface	Link up ● none ○ specific ○ all switches □ * Link down ● none ○ specific ○ all switches LLDP ● none ○ specific ○ all switches
Authentication	□ * □ SNMP Authentication Fail
Switch	□ * □ STP □ RMON

3.6.2 Programming the Trap Configuration – Global Settings

Name	Description
Trap Config Name	Enter a custom name for this trap no spaces
Trap Mode	Select Disable/Enable
Trap Version	Select the version based on security requirements and the ability to clients to receive the selected version
Trap Community	The Community can be public or private
Trap Destination Address	Enter the address of the SNMP Client- note the client must be running "trap" software that can receive the messages – this includes a compatible MIB
Trap Destination Port	SNMP transmission is usually standard on Port 162 – however if you change the port number make certain it is the same for the client
Trap Inform Time out	This is the amount of time the client must acknowledge a message receipt
Trap inform retry times	The number of times a message can be sent prior to determining failure
Trap Probe Security Engine ID	This function is active only with SNMPv3 indicating the trap probe security ID. Enable/Disable
Trap Security Engine ID	This function is active only with SNMPv3- one the Engine ID is enable this will indicate if it was found
Trap Security Name	This informs the SNMP name using USM (User Security Model) defining the procedures used for SNMP message security level
Save	After save is selected screen will return to the Trap Destination Configuration for verification of your settings

3.6.3 Community Configuration



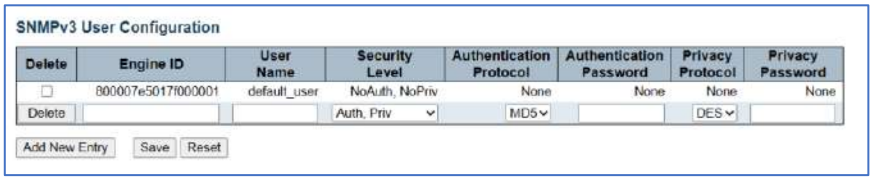
SNMPv3 Community Configuration

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

6.6.3 SNMPv3 Community Configuration

Name	Description
Public Community	This setting is used for SNMPv3: Enter the source address for the SNMP source. Enter the Source Mask address for the SNMP Mask Select Delete to Delete the information
Private Community	This setting is used for SNMPv3: Enter the source address for the SNMP source. Enter the Source Mask address for the SNMP Mask Select Delete to Delete the information
Add New Entry	Select to add a new set and note the ASCII characters must be different and range from 33-126

3.6.4 User Configuration



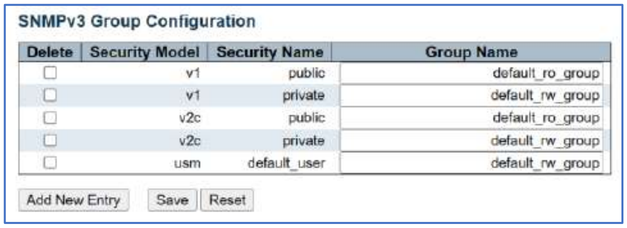
SNMPv3 User Configuration

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

3.6.4 SNMP User Configuration: (the following applies only to SNMPv3)

Name	Description
Delete	This selection the settings to delete
Engine ID	The octet string in hexadecimal form that identities the Engine the octet belongs to
Username	This names the entry; the string is 1-32 in ASCII characters from 33-126
Security Level	Programs the security mode No Authorization or Authorization with privacy or no privacy
Authentication Protocol	This set Authentication. It can only set if the system level is not already determined
Authentication Password	This setting is only value if MD5 authentication is active
Privacy Protocol	This selects as none, or DES (Data Encryption Standard) or AES (Advanced Encryption Standard) – both are used to secure authentication from client and servers.
Privacy Password	This sets a user password for SNMPv3

3.6.5 Group Configuration



SNMPv3 Group Configuration

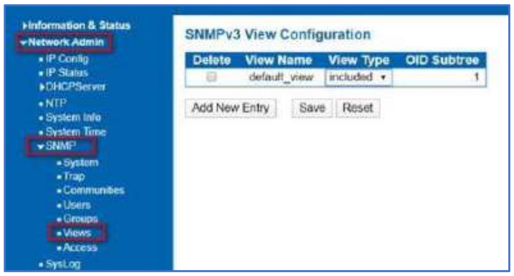
Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
□	usm	default_user	default_rw_group

3.6.5 SNMPv3 Group Configuration

Name	Description
Delete	This selection the settings to delete - selection will delete and individual group
Security Model	This defines the SNMP type the programming will be defined for
Security Name	The name given to the security model the allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126
Group Name	The given to the group. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126

3.6.6 View Configuration

Users can set SNMPv3 Group function. Click "Network Admin" > "SNMP" > "Views”, then this screen will show as:



SNMPv3 View Configuration

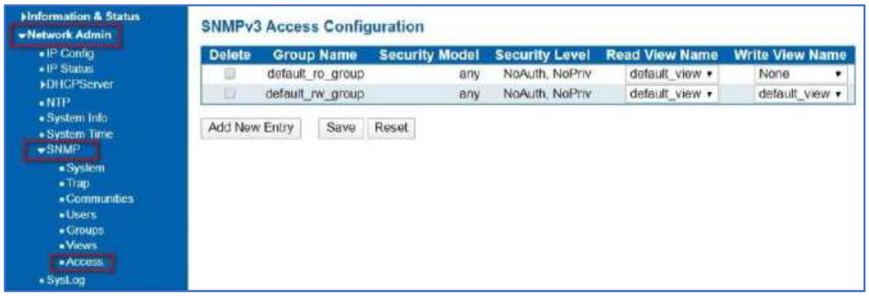
Delete	View Name	View Type	OID Subtree
□	default_view	included ▾	1

3.6.6 View Configuration

Name	Description
Delete	This selection the settings to delete - selection will delete and individual group
View Name	This names the view the entry belongs to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
View type	The choice is Included- with the ability the view subtree is include or Excluded- note if you exclude you have an alternative programmed
OID	This is the Object Identifier to identify the address of the connected device. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*).

Then this screen will show as:

3.6.7 SNMPv3 Access Configuration



SNMPv3 Access Configuration

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

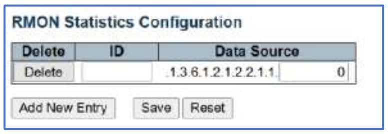
3.6.7 Access Configuration

Name	Description
Delete	This selection the settings to delete - selection will delete and individual group
Group Name	Identifies the group name the entry will be tied to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Model	Indicates the model the entry belongs to. It any Any, v1, v2c or USM which is a USER based Security model
Security Level	This is defined as the authorization level, No Authorization- nor privacy/Authorization with no privacy/Authorization with privacy
Read View Name	This defines the reading of the name of the MIB which is used. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Write View Name	This is the MIB and can be used to request a new value. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

3.7 RMON

RMON stands for Remote Monitoring helping with network operations through the use of connected devices labeled as monitors or probes – it is an extension of SNMP.

3.7.1 RMON Statistics



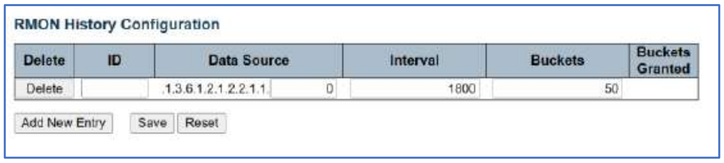
RMON Statistics Configuration

Delete	ID	Data Source	
Delete		.1.3.6.1.2.1.2.2.1.1	0

3.7.1 Statistics

Name	Description
Delete	This selection the settings to delete - selection will delete and individual group
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switching 3 port 5, the value is 2000005.

3.7.2 RMON History Configuration



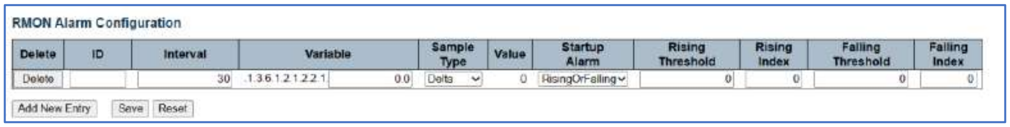
RMON History Configuration

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

3.7.2 history Configuration

Name	Description
Delete	This selection the settings to delete - selection will delete and individual group
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005
Interval	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds
Buckets	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50
Buckets Granted	The number of data shall be saved in the RMON

3.7.3 RMON Alarm Configuration



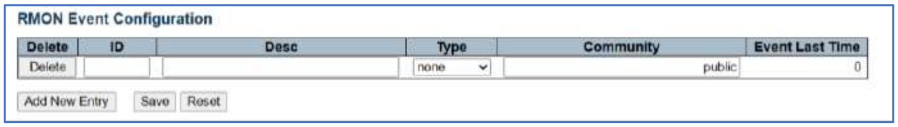
RMON Alarm Configuration

Delete	ID	Interval	Variable		Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
Delete		30	.1.3.6.1.2.1.2.2.1	0.0	Delta	0	RisingOrFalling	0	0	0	0

3.7.3 Alarm Configuration

Name	Description
Delete	This selection the settings to delete - selection will delete and individual group
ID	Indicates the index of the entry. The range is from 1 to 65535.
Interval	indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from greater than 1
Variable	Input the variable to be sampled
Sample Type	Select the variable and calculating the variable that will compared against the Threshold: Absolute= directly get the sample. Delta= Calculate the differences between samples- this is the default
Value	Static value of the last sampling period
Startup Alarm	Assigns the method used to select the variable and calculate that value against the selected types
Rising Threshold	Rising threshold value (-2147483648-2147483647)
Rising Index	Rising event index (1-65535).
Railing Threshold	Number indicated as the top value
Falling index	Falling event index Falling event index (1-65535).

3.7.4 RMON Event Configuration



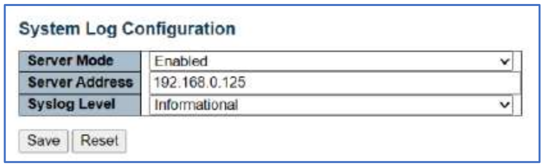
RMON Event Configuration

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

3.7.4 Event Configuration

Name	Description
Delete	This selection the settings to delete - selection will delete and individual group at the next save
ID	Indicates the index of the entry. The range is from 1 to 65535.
Description	Indicates this event, the string length is from 0 to 127, default is a null string.
Type	This indicates the type of event that will included in the SNMP log
Community	Specify the community when trap is sent, the string length is from 0 to 127, default is "public".
Event Last Time	Indicates the value of sysUpTime at the time this event entry last generated an event.

3.8 System Log Configuration



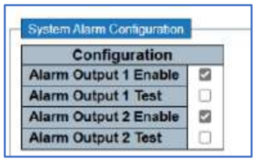
System Log Configuration

Server Mode	Enabled
Server Address	192.168.0.125
Syslog Level	Informational

3.8 System Log Configuration

Name	Description
Server Mode	Disable/Enable: When enabled Syslog information will be transmitted to the assigned address
Server Address	Entry the server address that will receive syslog information
Syslog Level	Select the Level that will be transmitted: informational/ Notice/Warning/Error- note only if the selected error occurs will it be transmitted

3.8.1 Alarm Configuration

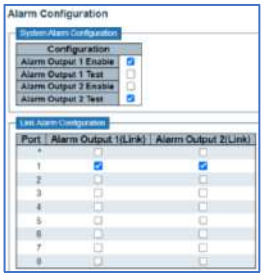


System Alarm Configuration

Configuration	
Alarm Output 1 Enable	☑
Alarm Output 1 Test	□
Alarm Output 2 Enable	☑
Alarm Output 2 Test	□

3.8.1 System Alarm Configuration

Name	Description
Alarm Output Enable 1,2	Check the box will enable the physical alarm outputs in the event a programmed alarm condition occurs – If an alarm is active – it will also be shown on the front panel LED. To extinguish an active alarm condition, uncheck the box
Alarm output test 1, 2	Check the box to test the alarm- the front panel LEDs will be active as will the will physical alarm output. Uncheck to extinguish the test



Alarm Configuration

System Alarm Configuration

Configuration	
Alarm Output 1 Enable	☑
Alarm Output 1 Test	□
Alarm Output 2 Enable	□
Alarm Output 2 Test	☑

Link Alarm Configuration

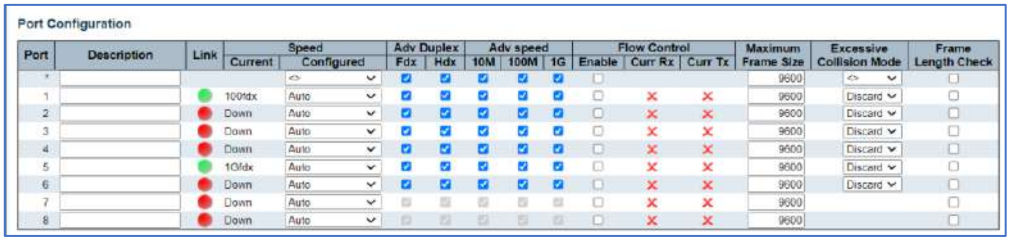
Port	Alarm Output 1(Link)	Alarm Output 2(Link)
*	□	□
1	☑	☑
2	□	□
3	□	□
4	□	□
5	□	□
6	□	□
7	□	□
8	□	□

3.8.1 System Alarm Configuration

Name	Description
Alarm Output Link 1,2	Select the appropriate link output associated with the port number. Only a selected port will be active if an alarm occurs at that port

Chapter 4: Port Configuration

4.1 Ports



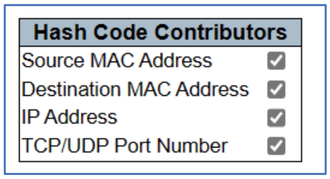
Port Configuration

Port	Description	Link	Speed		Adv Duplex		Adv speed			Flow Control			Maximum Frame Size	Excessive Collision Mode	Frame Length Check
			Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx			
*				<>	☑	☑	☑	☑	☑	☐			9600	<>	☐
1		🟢	100fdx	Auto	☑	☑	☑	☑	☑	☐	✗	✗	9600	Discard	☐
2		🔴	Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	9600	Discard	☐
3		🔴	Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	9600	Discard	☐
4		🔴	Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	9600	Discard	☐
5		🟢	1Gfdx	Auto	☑	☑	☑	☑	☑	☐	✗	✗	9600	Discard	☐
6		🔴	Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	9600	Discard	☐
7		🔴	Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	9600		☐
8		🔴	Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	9600		☐

Name	Description
Description	Enter the name for the port
Link	Indicates link status- Red = Down, Green= Up
Configured	Disable or set port speed. Auto or specific value. For Fiber ports 11 and 12 set the specific speed as per the SFP used – note ports 11 and 12 will indicate speed based on inserted SPF and the connection speed if not connected it will only display deflect 100Mbps-1G
Adv Duplex	Select either Full or Half Duplex both can be active
Adv Speed	All boxes must be checked that allow for connections at the selected speed each port can operate at all speeds- note this setting applies only to the UTP ports
Flow Control	This regulates the data speed between two connected devices. If not in sync it can halt transmission. As video cameras are UDP and most other devices are direct connections it usually is not used.
Maximum Frame size	Standard data switches limit port speeds of 100Mbps to 1518bytes (non-jumbo frames). This setting allows for Jumbo frames at any wire port speed
Excessive Collision Mode	This is determined by the number of collisions usually 16 when attempting to transmit a single frame
Frame Length check	This checks for the frames that lengths are greater than 1500 bytes and shorter than 64 bytes It should not be used for Video applications

4.2 Aggregation

This is the function of combining ports to increase total bandwidth.



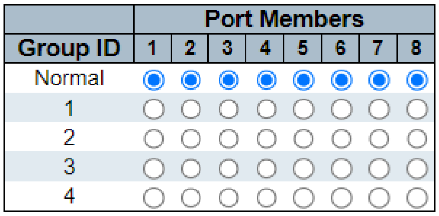
Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	☑
IP Address	☑
TCP/UDP Port Number	☑

4.2 Aggregation

4.2.1 Hash Code Contributors

Name	Description
Hash Code Contributors	The Code that is used to define the Aggregation is select with a check mark, all of them can be selected

4.2.2 Aggregation- Port Members



	Port Members							
Group ID	1	2	3	4	5	6	7	8
Normal	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○

4.2.2 Port Members

Name	Description
Group ID	Normal= no aggregation.
Port Members	Numbers 1-6= Select the ports to aggregate and note that all selected ports must be full duplex and must be operating at the same speed. Different ports should be used for different groups and not mixed

Link Aggregation Control Protocol is the component that combines multiple Ethernet links into a single link

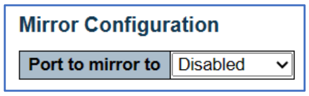
4.2.3 Aggregation- LACP Port configuration

Name	Description
Port	Defines the Port number
LACP Enable	Enables the LACP function
Key	This value defines the aggregation port speed. The range is 1-65535. Auto Setting= 10Mb = 1, 100Mb = 2, 1Gb = 3 Specific=sets a specific port speed (generally not used) – this will release the box to fill in the value Note: All ports in the same aggregated group must have the same port speed
Role	Active= LACP packets will be transmitted each second Passive= LACP packets will be transmitted when received from the connected device
Timeout	Fast= LACP packets are transmitted each second Slow= devices wait 30 seconds prior to transmitting LACP packets
Prior	This function assigns the port priority (1-65535) and determines which ports will be active in the aggregation process based on transmission and port capacity. Those ports outside the ability to transmit will be assigned as back up – the lower number assigned that higher the priority

4.3 Mirroring

Mirroring copies packet transmission from one port or VLAN to another.

4.3.1 Mirroring Configuration



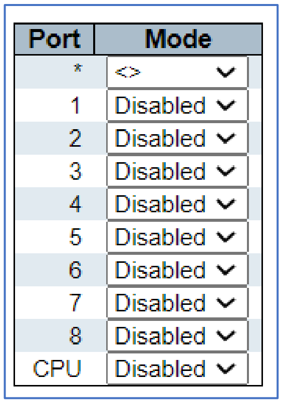
Mirror Configuration

Port to mirror to: Disabled

4.3.1 Mirroring Configuration

Name	Description
Port to Mirror	Select Disable or Enable

4.3.2 Mirror Port Configuration



Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
CPU	Disabled

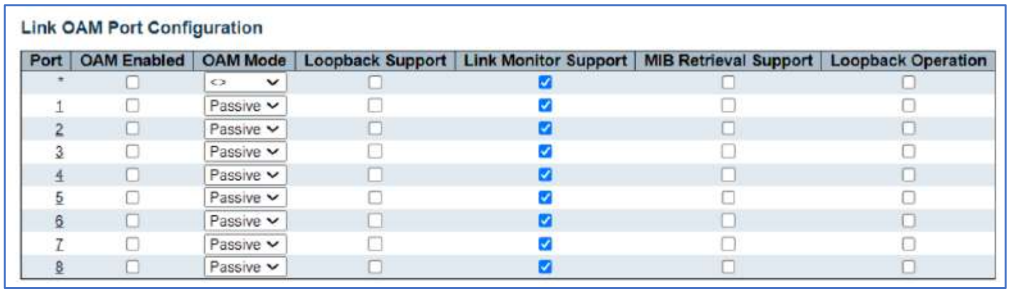
4.3.2 Mirror Port Configuration

Name	Description
Port	Indicates the port number
Mode	Rx= only packets received on these ports are transmitted Tx = only packets received on these ports are transmitted Disable= no packets are transmitted Enable = Received and Transmitted packets are mirrored

4.4 Link OAM

Operations, Administration, and Maintenance (OAM) monitors link operations and enables network connections in the event of a failure.

4.4.1 Link OAM Port Configuration – Port Setting



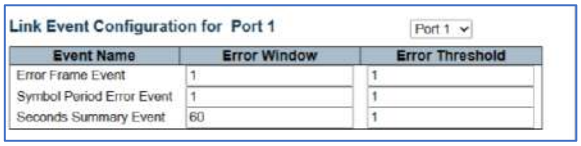
Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	□	<>	□	☑	□	□
1	□	Passive	□	☑	□	□
2	□	Passive	□	☑	□	□
3	□	Passive	□	☑	□	□
4	□	Passive	□	☑	□	□
5	□	Passive	□	☑	□	□
6	□	Passive	□	☑	□	□
7	□	Passive	□	☑	□	□
8	□	Passive	□	☑	□	□

4.4.1 Link OAM Port Configuration – Port Setting

Name	Description
Port	Indicates the port number
OAM Enable	Enables the port for the programming that follows
OAM Mode	Active Mode=system automatically looks at the exchange of information expecting responses- all connections must be active. Passive Mode= status is not done and must be conducted by an external source.
Loopback support	When active the system monitors localized faults and link performance
Link Monitor Support	When active the port supports event notification including diagnostic information.
MIB Retrieval Support	If the required MIB is included the system will poll the links for its contents
Loopback Operations	If enabled the port will conduct a loopback operation

4.4.2 Link OAM- Link Event Port Settings



Link Event Configuration for Port 1

Port 1

Event Name	Error Window	Error Threshold
Error Frame Event	1	1
Symbol Period Error Event	1	1
Seconds Summary Event	60	1

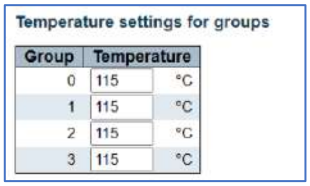
4.4.2 Link OAM- Link Event Port Settings

Name	Description
Port	Use the drop-down menu to select the port
Event Name	The Event name is fixed. **Error Frame Event** = counts the number of error fames (example defined errors such as CRC) during over a specified time period- the setting is in seconds 1-60 Symbol Period Error Event = counts the number of symbol errors (undefined errors) during over a specific time period – the setting is in seconds 1-60 **Seconds Summary Event** -Indicates if the number of errors is greater than the specified number
Error Threshold	Represents the time period in 1 second for link events. The setting range is 0 (default) to 4294967295. Note the Summary Event limit is 42949

As wiring resistance increases port temperature increases. Operator can set limits to reflect any increase as a warning or at level near the failure port.

4.5 Thermal Protection

4.5.1 Temperature setting for Groups.



Temperature settings for groups

Group	Temperature	
0	115	°C
1	115	°C
2	115	°C
3	115	°C

4.5.1 Temperature setting for groups – the setting applies to each group.

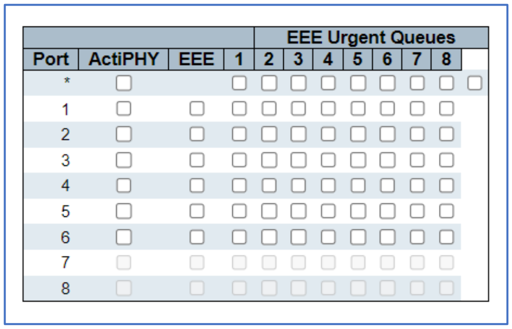
Name	Description
Group	Notes each of the 4 groups
Temperature	Settings range from 0-115C over 115C will trigger a pop up warning Look for the actual operating temperature in Information and Status setting as a reference

Green Ethernet monitors the port for activity. If no activity is senses, it reduces power. It is not generally not recommended for security networking applications as powering down can disable PoE disabling the connected device. This setting does not apply to fiber connections.

4.6 Green Ethernet

Name	Description
Drop Down Select	Notes the individual that the setting will apply to: Latency= time duration between sensing power Power= power level drops

4.6.1 Green Ethernet – Port Configuration



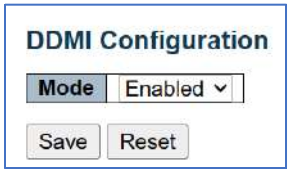
			EEE Urgent Queues								
Port	ActiPHY	EEE	1	2	3	4	5	6	7	8	
*	□		□	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□	□	□	
2	□	□	□	□	□	□	□	□	□	□	
3	□	□	□	□	□	□	□	□	□	□	
4	□	□	□	□	□	□	□	□	□	□	
5	□	□	□	□	□	□	□	□	□	□	
6	□	□	□	□	□	□	□	□	□	□	
7	□	□	□	□	□	□	□	□	□	□	
8	□	□	□	□	□	□	□	□	□	□	

4.6.1 Green Ethernet, Port Configuration.

Name	Description
Port	Indicates port number where settings are applied
ActiPHY	When active the power of a port will be lower (disabled) if no connection is detected.
EEE	Energy Efficient Ethernet detects the amount of transmission and depending on the Power Latency setting will determine if the port is idle and power is reduced.
EEE Urgent Queues	The setting 1-8 will indicate how quickly individual frames are detected. If not set the system will wait for a burst of frames

4.7 DDMI Configuration

DDMI stands for Digital Dynamic Management Interface. In order to operate the SFP you use must include DDMI firmware (all Vigitron SFPs do) and the network switch you use must be able to read DDMI (Vigitron enterprise switches do)

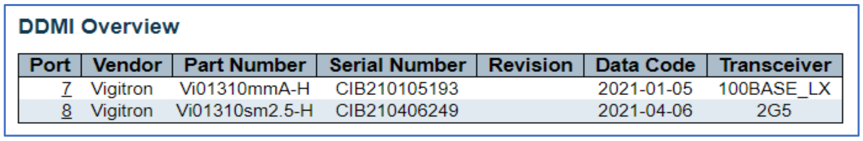


DDMI Configuration

Mode	Enabled

Name	Description
Enable/Disable	Enables/Disable DDMI reading. If disabled SFP DDMI will not operate

4.7.1 DDMI Overview

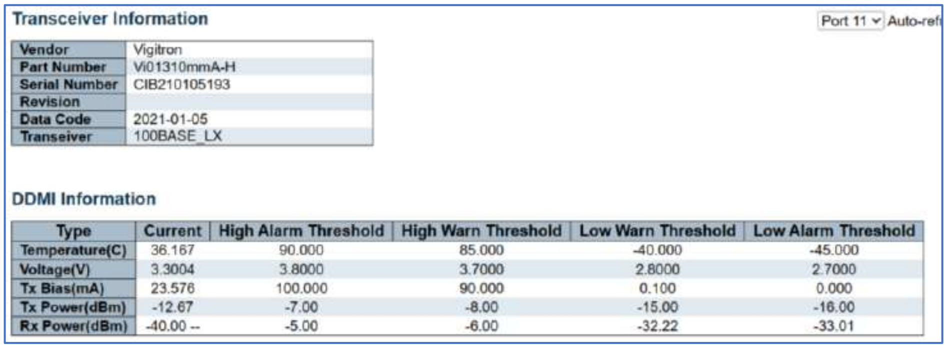


DDMI Overview

Port	Vendor	Part Number	Serial Number	Revision	Data Code	Transceiver
7	Vigitron	Vi01310mmA-H	CIB210105193		2021-01-05	100BASE_LX
8	Vigitron	Vi01310sm2.5-H	CIB210406249		2021-04-06	2G5

4.7.1 DDMI Overview.

Name	Description
DDMI Overview	Select Network Admin>DDM>DDM Overview



Transceiver Information

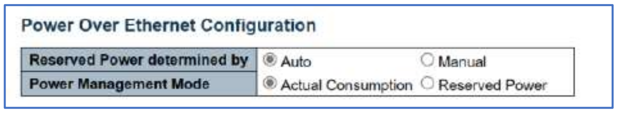
Vendor	Vigitron
Part Number	Vi01310mmA-H
Serial Number	CIB210105193
Revision	
Data Code	2021-01-05
Transeiver	100BASE_LX

DDMI Information

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	36.167	90.000	85.000	-40.000	-45.000
Voltage(V)	3.3004	3.8000	3.7000	2.8000	2.7000
Tx Bias(mA)	23.576	100.000	90.000	0.100	0.000
Tx Power(dBm)	-12.67	-7.00	-8.00	-15.00	-16.00
Rx Power(dBm)	-40.00 --	-5.00	-6.00	-32.22	-33.01

4.7.2 Power Over Ethernet Configuration

This operation sets the power available per port.



Power Over Ethernet Configuration

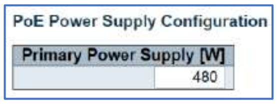
Reserved Power determined by	● Auto	○ Manual
Power Management Mode	● Actual Consumption	○ Reserved Power

4.7.2 Power Over Ethernet Configuration.

Name	Description
Reserved Power Determined by	Auto: = automatic sensing of the connected device
	Manual- The value entered
Power Management Mode	Actual Consumption= the total power consumed Reserve power= the amount of power remaining after the amount of power used is determined

Chapter 5: PoE

5 PoE Power Supply Configuration

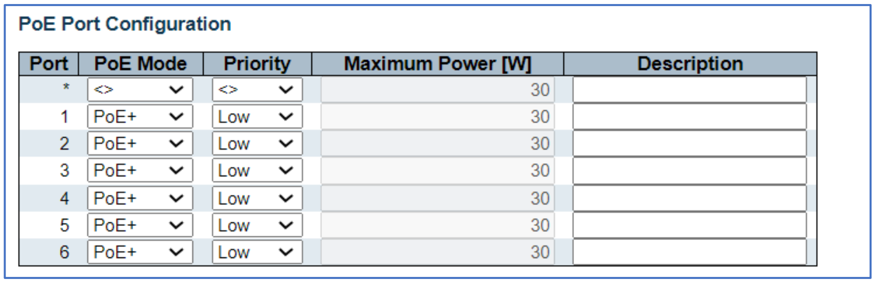


PoE Power Supply Configuration

Primary Power Supply [W]
480

Name	Description
Primary Power Supply(W)	Enter the value of the power supply- this is a manual entry and determines the rest of the settings.

5.1 PoE Port Configuration Setting



PoE Port Configuration

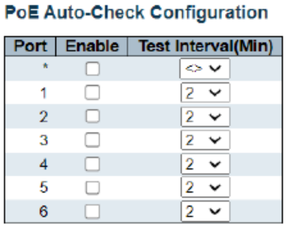
Port	PoE Mode	Priority	Maximum Power [W]	Description
*	<>	<>	30	
1	PoE+	Low	30	
2	PoE+	Low	30	
3	PoE+	Low	30	
4	PoE+	Low	30	
5	PoE+	Low	30	
6	PoE+	Low	30	

5.1. PoE Port Configuration.

Name	Description
Port	Identifies the port number
PoE Mode	There are 4 settings: Disabled= No PoE is provided to the port PoE= Provides power to 15.4W=802.3af PoE+ Provides power to 30W=802.3at PoE++ Provides power to 90W 802.3bt Manual Provides the ability to enter a specific PoE amount and power most no standard PoE modes
Priority	Low= Lowest PoE priority. PoE will be provide only after all other mode requirements are met High= Power is provided over Low Critical= PoE is provided to these ports first
Maximum Power	Set a maximum level equal or greater than the value required by the connect device. If you are using the Manual mode with devices requiring more than 30W – set the level to 90W – only the amount of power needed by the connected device will be used regardless of the setting
Description	Enter any information regarding the connected device

5.2 PoE Auto Check

Auto checking monitors the connection link. In the event a link is lost it will automatically attempt to apply PoE and reconnect. If the attempt fails 3 times the link will be dropped



PoE Auto-Check Configuration

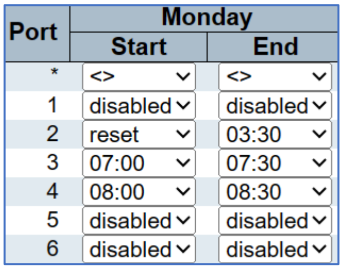
Port	Enable	Test Interval(Min)
*	□	<>
1	□	2
2	□	2
3	□	2
4	□	2
5	□	2
6	□	2

5.2. PoE Auto Check.

Name	Description
Port	Identifies the port
Enable	Enables the auto-checking feature for the port
Test Interval	All PoE devices have different times to recognize PoE and power up. The range is 2-10 seconds and must be set to allow the connected device to properly power up

5.3 PoE Scheduling

This setting will turn PoE on and off at the scheduled times. The Start time indicates when PoE is turned ON, the end time is when PoE is turned OFF. To operate this the TimeZone function must be programmed. In the following example only, Monday is shown- all days are available in the actual programming.



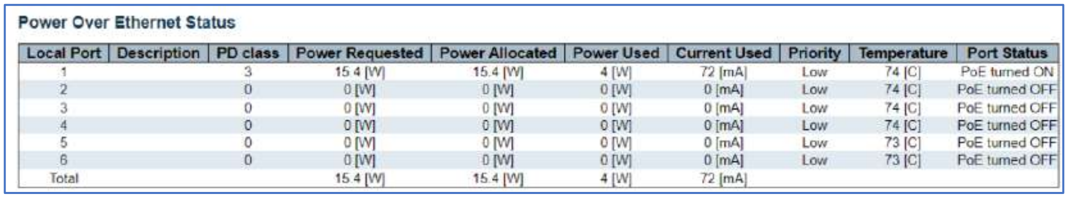
Port	Monday	
	Start	End
*	<>	<>
1	disabled	disabled
2	reset	03:30
3	07:00	07:30
4	08:00	08:30
5	disabled	disabled
6	disabled	disabled

5.3. PoE Scheduling.

Name	Description
Port	Identifies the port number
Day	Day is displayed and programming for that day follows
Start	Disable=no time is programmed – function is turned off Reset = PoE will reset that at the time indicated in the End Colum Time program= start time for PoE is turned ON
End	Disable=no time programmed – function is turned off Reset= the time programmed in this column indicates when PoE is reset Time program= End time when PoE is turned Off

5.4 Power Over Ethernet Status

Power over Ethernet Status is a checking function based on the previous programming and is used to confirm if the connected device is properly powered based on proper programming.



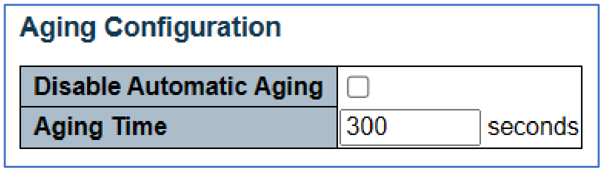
Power Over Ethernet Status

Local Port	Description	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Temperature	Port Status
1		3	15.4 [W]	15.4 [W]	4 [W]	72 [mA]	Low	74 [C]	PoE turned ON
2		0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	74 [C]	PoE turned OFF
3		0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	74 [C]	PoE turned OFF
4		0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	74 [C]	PoE turned OFF
5		0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	73 [C]	PoE turned OFF
6		0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	73 [C]	PoE turned OFF
Total			15.4 [W]	15.4 [W]	4 [W]	72 [mA]			

5.3. PoE Over Ethernet Status.

Name	Description
Port	Identifies the port number
Description	Shows the name as manually entered
PD Class	Shows the PD class of the connected device
Power Requested	Shows the PoE power as requested by the connected device
Power allocated	Show the power allocated by the connected device. This value should be equal or greater than the power allocated
Power Used	Reflects the actual power used. PoE devices may have different power usage at different time depending on their activity
Current used	Reflects the actual current used.
Priority	Based on the programming
Temperature	Shows the actual temperature of the port which is used to determine shorts or high resistance- if the temperature is close to the limit of 115C please check your system
Port Status	This is the final check that confirms if the Port PoE power is actually powering the connected device.

6 MAC Table Aging Configuration



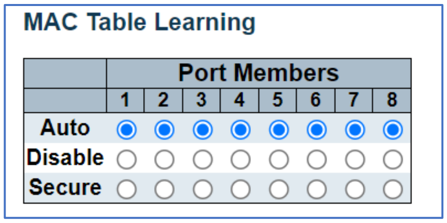
Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

6 MAC Table Aging Configuration

Name	Description
Disable Automatic Aging	Setting Check box on
Aging Time	Duration 10-1000000 seconds defines when Dynamic entries are removed from the MAC table

6.1 MAC Table Learning



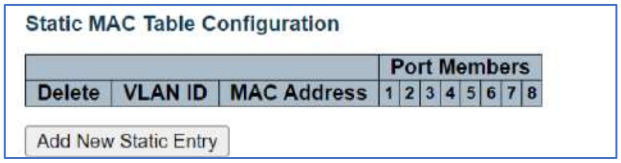
MAC Table Learning

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

6.1 MAC Table Learning

Name	Description
Auto	Automatically learns when a frame with unknow SMAC (Simple Medium Access Control) is received – only active in star configurations
Disable	No port learning is done
Secure	Only Static MAC entries are learned others are dropped

6.1.1 MAC Table Configuration



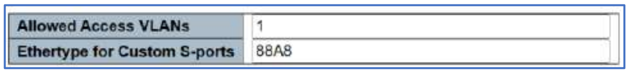
Static MAC Table Configuration

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

6.1.1 MAC Table Configuration.

Name	Description
Delete	Check to active Delete – information will be deleted
VLAN ID	Enter the number of the VLAN
MAC Address	Enter the MAC address of the VLAN – this will be entry point
Port Members	Check the port members to be included

6.2 Global VLAN Configuration

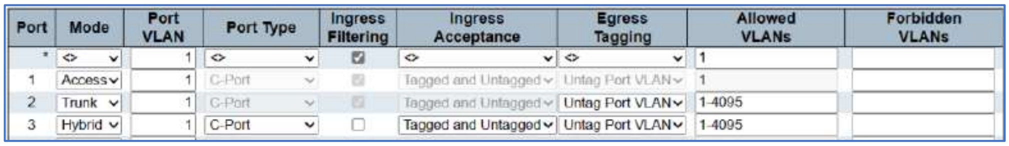


Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

6.2 Global VLAN Configuration.

Name	Description
Allowed Access VLANs	Input the VLAN number. Default is 1. You can enter multiple numbers separated by commons.
Ether type for Custom S-Ports	Set S-Port identification for all ports that are S-Port

6.2.1 Port VLAN Configuration

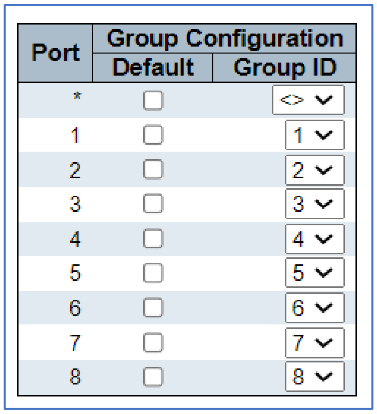


Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
2	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Hybrid	1	C-Port	□	Tagged and Untagged	Untag Port VLAN	1-4095	

6.2.1 Port VLAN Configuration.

Name	Description
Port	Defines the port number
Mode	Defines the Mode. There are 3 choices: **Access** is the universal choice. The default VLAN is 1. Both Tagged and Untagged frames can be transmitted. **Trunk** ports can be members of multiple VLANs and tagging is allowed. **Hybrid** is like Trunk but allows for customization of tags so frames within the VLAN can be controlled independently.
Port VLAN	Defines the number of VLAN as programmed
Port Type	Type will classify a priority to the transmission. **C-Port** can be considered as universal default allowing the frame to assigned to VLAN port. **S-Port**- provides tagging on Ingress and only those frames will be accepted. **S-Custom- Port**: This will treat C-Port in the same manner as S-Ports
Ingress Filtering	Check this to allow for changing Ingress filtering, If Access and Trunk ports are active other frames will be rejected – including frames not members of any assigned VLANs
Ingress Acceptance	This is only active using a Hybrid setting and allows for both tagged and untagged ports
Ingress Tagging	Active under Trunk and Hybrid: Untag Port VLAN separates untagged and other tag frames
Allowed VLANS	Defines the number of VLANs 1-4095 the setting is assigned to
Forbidden VLANs	Blocks an individual port from being a member of a VLAN- recommended for use if dynamic settings are used

6.3 VLAN Translation

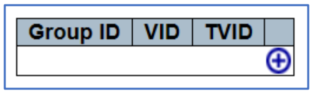


Port	Group Configuration	
	Default	Group ID
*	□	<>
1	□	1
2	□	2
3	□	3
4	□	4
5	□	5
6	□	6
7	□	7
8	□	8

6.3 Port VLAN Translation.

Name	Description
Port	Defines the port number
Default	Defines the switch port for the default VLAN Translation Group
Group ID	The number of Groups is equal to the number of ports. These will assign a VLAN to an individual group. Multiple ports can be configured to the same group

6.3.1 VLAN Translation Mapping Table



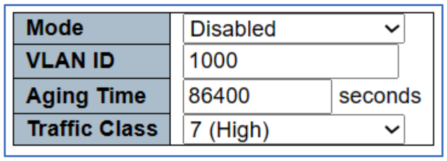
Group ID	VID	TVID
		⊕

6.3.1 VLAN Translation Mapping Table

Name	Description
Group ID	This is the Group created in the previous setting
VID	This is source VLAN ID (1-4095) created in the previous setting
TVID	Notes the VLAN ID in which the ingress frame to translated to- based on the previous settings
⊕	Use the + to add new setting

This setting is used for Voice communications. If need it is suggested that Voice and Data traffic (which includes voice) be segregated to different VLANs.

6.4 Voice VLAN Configuration

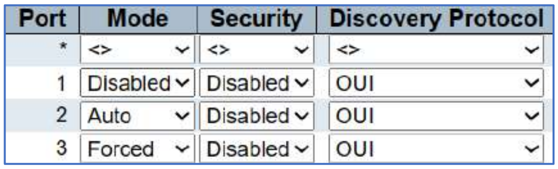


Mode	Disabled
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High)

6.4 Voice VLAN Configuration

Name	Description
Mode	Select disable/enable
VLAN ID	The VLAN mode that is assigned (1-4095) Do not mix VLAN assigned to other processes
Aging Time (sec)	Input value 10 -10000000 seconds and is equal to the allowed range when the security or auto detect is enabled
Traffic Class	All VLAN traffic assigned with the same class will be applied

6.4.1 Voice VLAN Port Configuration



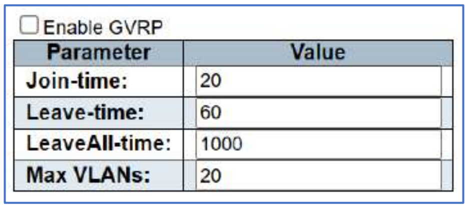
Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Auto	Disabled	OUI
3	Forced	Disabled	OUI

6.4.1 Voice VLAN Configuration

Name	Description
Port	Fixed Port Number
Mode	Disabled: Settings are disabled. Auto: Enables auto detection if a VoIP phone is connected to a specific port. Forced: Forces joining regardless of connected device
Security	Modes are Enable/Disable: Blocks all non-phone MAC addresses for 10 seconds
Discovery Protocol	Choices are OUI: requires device OUI address. LLDP: Detection by LLDP. Both; Either OUI and LLDP.

6.5 GVRP Configuration

Effects dynamic VLAN management by eliminating unnecessary broadcast and unicast traffic using 802.aQ traffic links.



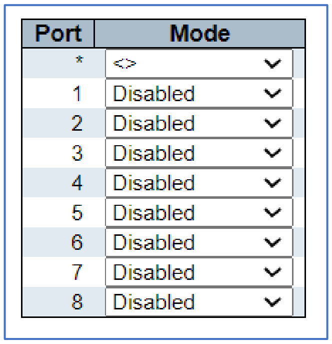
☐ Enable GVRP

Parameter	Value
Join-time:	20
Leave-time:	60
LeaveAll-time:	1000
Max VLANs:	20

6.5 GVRP Configuration

Name	Description
Enable	If checked the settings are Enabled
Join-time	Is programmed in a range of 1-20cs (hundreds of a second) the default value is 20cs - defines the time during joining can occur
Leave-time	Is programmed in a range of 60-300cs (hundreds of a second) Defines when the function is off – applies to a specific VLAN – default is 60cs
LeaveAll-time	Is programmed in a range of 1000-5000cs (hundreds of a second) defines when total VLANs function is off – defaults is 1000cs
Max VLANs	Defines the maximum number of VLANs supported – default is 20 – note the number can only be changed when the setting is off.

6.5.1 GVRP Port Configuration



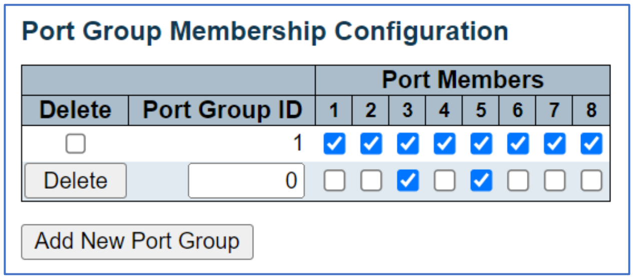
Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

6.5 GVRP Configuration

Name	Description
Port Number	The port number is fixed
Mode	Disable: The function on that port is disabled. GVRP: The selected port for GVRP is enabled 3.1.20.0

Port Group Membership Configuration
The following setting applies to Private VLAN (PVLAN). In this setting be aware that by Default all VLAN, and PVLAN are VLAN 1.

6.6 Port Isolation



Port Group Membership Configuration

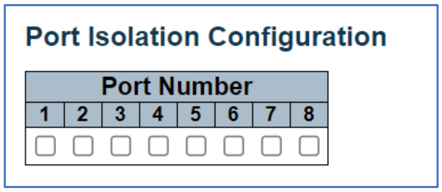
		Port Members							
Delete	Port Group ID	1	2	3	4	5	6	7	8
☐	1	☑	☑	☑	☑	☑	☑	☑	☑
Delete	0	☐	☐	☑	☐	☑	☐	☐	☐

Add New Port Group

6.6 Port Isolation

Name	Description
Delete	Checking this will delete the entry after Save is selected
Port Group ID	Select the number of PVLAN you want to program
Port Members	Check the ports you want to Include in the PVLAN, unchecked ports are excluded
Add New Port Group	Select this to add a PVLAN

6.6.1 Port Isolation Configuration



Port Isolation Configuration

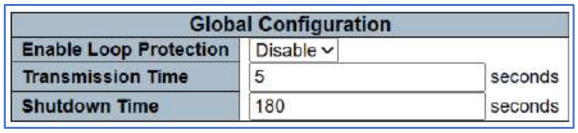
Port Number							
1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□

6.6.1 Port Isolation Configuration

Name	Description
Port Number	When check the port is isolated from VLAN and PVLAN- Port Isolation is defaulted on all ports

6.7 Loop Protection

This feature prevents duplicate data paths from repeating the information and degrading performance.

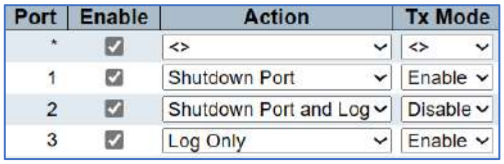


Global Configuration		
Enable Loop Protection	Disable	
Transmission Time	5	seconds
Shutdown Time	180	seconds

6.7 Loop Protection

Name	Description
Enable Loop Protection	Enables or disable applying Loop Protection to all ports
Transmission Time	Defines the interval between each loop protection sending applied to the data being send. Values at 1-10 second and default is 5 seconds
Shutdown time	Determines the duration a port will be disabled after a loop is detected and shut down. Values are 0 – 604800 seconds- default is 180 seconds

6.7.1 Loop Protection Configuration – Port Configuration

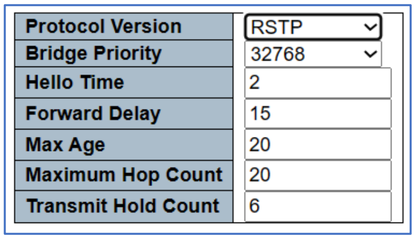


Port	Enable	Action	Tx Mode
*	☑	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port and Log	Disable
3	☑	Log Only	Enable

6.7.1 Port Configuration

Name	Description
Port	Select the fixed port number
Enable	Check the box to enable the port
Action	Defines the action to be taken when a loop is detected. **Shutdown Port**- Port is shutdown. **Shutdown port and Log**- Port is shut down and log is created. **Log only**- Port remains active but log is generated
Tx mode	Enable/Disable- when enabled setting will actively look for data to determine if loop is valid. If disable system will be passive

6.8 Spanning Tree

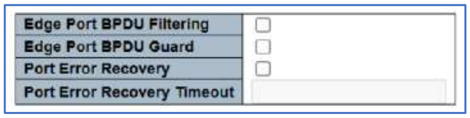


Protocol Version	RSTP
Bridge Priority	32768
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

6.8 Spanning Tree

Name	Description
Protocol Version	The choices are : **STP** (Spanning Tree Protocol) prevents loops when bridging LANS. **RSTP** – Rapid STP) updated version of STP increasing speed. **MSTP** (Multiple STP) used when multiple Spanning Trees are involved
Bridge Priority	This number assigns a bridge priority. The lower the number the higher the priority
Hello Time,	This is the time between BPDUs (Bridge protocol data units) to detect loops. The setting is 1-10 seconds. **The default is 2 seconds, and it recommended the default not be changed**
Forward Delay	This controls the port forwarding within STP operations. Settings are 4 to 30 seconds.
Max Age	This applies to the Root Bridge. Valid times of 6 to 40 seconds. Note the Max age setting must be at least set with (delay time -1)*2 to be valid
Maximum Hop Count	This applies to MSTI (Multiple Spanning Tree Protocol) and defines the remaining hops as to how many bridges a root bridge can distribute with the set time. The range is 6 to 40 hopes
Transmit Hold Count	The number of BPDUs a bridge can send per second. If the setting is exceeded the next BPDU will be delayed. Setting is 1 to 10 BPDU's per second

6.8.1 STP Bridge Configuration – Advance Settings



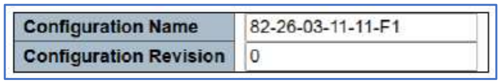
Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

6.8.1 STP Bridge Configuration – Advance Settings

Name	Description
Edge Port BPDU Filtering	The port must be first configured as an edge port. An edge port is only connected to a user application such a server or computer and not a LAN. This will prevent these ports from causing Loop problems. Check the box to be active to allow reception of BPDUs
Edge Port BPDU Guard	Check this box to disable the reception of BPDUs
Port Error Recover	Controls the recovery of a port after it is error disabled. If this setting is not used and the port is disabled, you must use the STP setting to enable.
Port Error Recovery Time out	The time before a port that has been disabled can be re-enabled. Valid settings are between 30 – 86400 seconds

MSTI (Multiple Spanning Tree Protocol) provides connection assignments to both simple and full connection to VLANs in a local area bridge network using BPDUs for exchanging information.

6.8.2 MSTI Configuration Identification

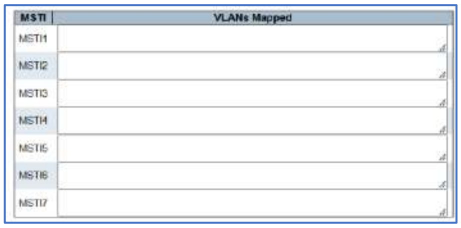


Configuration Name	82-26-03-11-11-F1
Configuration Revision	0

6.8.2 MSTI Configuration Identification

Name	Description
Configuration Name	This is the name given to identify the VLAN to the MSTI mapping. The name is limited to 32 characters
Configuration Revision	The number assigned as the revision to the MSTI configuration named above – the numbers range from 0 to 65535

6.8.2 MSTI Mapping



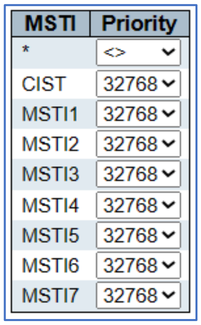
MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

6.8.2 MSTI Mapping

Name	Description
MSTI	This is fixed (Note CIST cannot be mapped and receives VLANS that are not mapped
VLAN Mapped	VLANs can be indicated with two digits between 1-4094 or within a range of two-digit number. Note only one VLAN can be mapped to one MSTI

This works with the STP MSTI priority.

6.8.3 MSTI Configuration



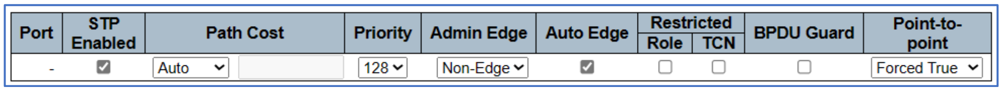
MSTI	Priority
*	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

6.8.3 MSTI Configuration

Name	Description
MSTI	Fixed number
Priority	Indicates the priority – the lower the number the higher the pri

Common Internal Spanning Tree is a part of MSTP (multiple spanning Tree protocol) used for identifying administers and the root bridge for each spanning tree – it is not applied to a specific MSTI.

6.8.4 CIST Aggregated Port Configuration

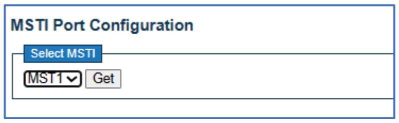


Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Forced True

6.8.4 CIST Aggregated Port Configuration

Name	Description
Port	Switch Port
STP Enabled	Check the box to enable Spanning Tree for the port
Path cost	Controls the port path **Auto**: determines path cost by the port link speed. **Specific:** Using a user defined value- lower paths as forwarded over high paths – the value range is 1 – 200000000.
Priority	Controls port priority and is related to the Path cost – the value is 0-240
Admin Edge	Controls whether the operEdge flag is set or cleared- the setting is Non-Edge or Edge:
Auto Edge	Activate with check mark. Enables bridge to automatically port edge detection. Operates by detecting BPDU (loop detection) received on the port
Restricted – Role	Restricts the port from being selected as the root for either CIST or MSTI
Restricted- TCN	Restricts the port from transmitting topology changes to other ports
BPDU	If active the port will be disabled if BPDUs are received
Point to Point	Controls if the port connection will be point to point instead of shared. The setting are: **Auto:** - will automatically be active; **Force True**: The connection is made regardless of traffic. **Forced False:** The connection will not be made regardless of valid traffic

6.8.5 MSTI Port Configuration



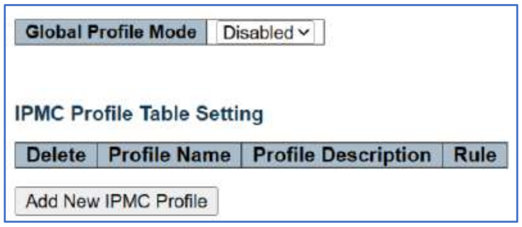
6.8.5 MSTI Port Configuration

Name	Description
MSTI Select	Select is 1-7 used to select the STP MSTI port configurations. Note MSTI is a virtual port which contains the MSTI port settings for physical or aggregated ports
GET	When active it retrieves the MSTI settings

6.9 IPMC

IPMC provides management and monitoring for the switch's CPU operating systems. This interfaces with a connected computer in a on or off condition and report on these conditions.

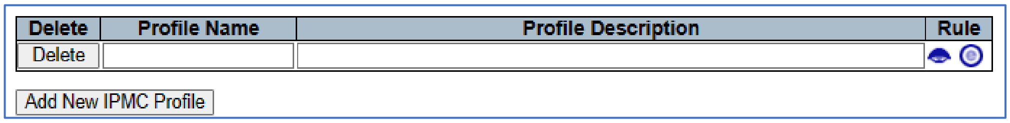
6.9.1 IPMC Profile Configuration



6.9.1 IPMC Profile Configuration

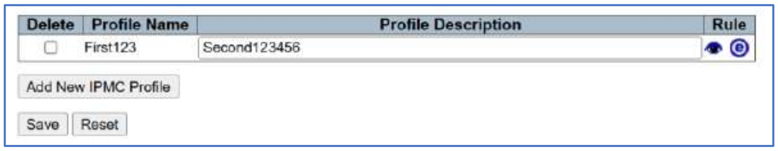
Name	Description
Disable/ Enable	Use the drop down to enable or disable mode
Add new IPMC Profile	Select to add new profile

6.9.2 IPMC Profile Table Setting



96.9.2 IPMC Profile Table Setting

Name	Description
Delete	Select to delete the specific entry
Profile Name	Name used to identify the profile table. Maximum of 16 Alph and numbers – name must include at least one alph.
Profile Description	Is a more detailed description. It can be up to 64 alph and numbers no blank spaces are allow but "-"can be used to separate a sentence
Rule	After the Profile name and Description are entered – the following buttons will be active: 👁: List the rules associated with the designated profile. ⓔ: Adjust the rules associated with the designated profile.

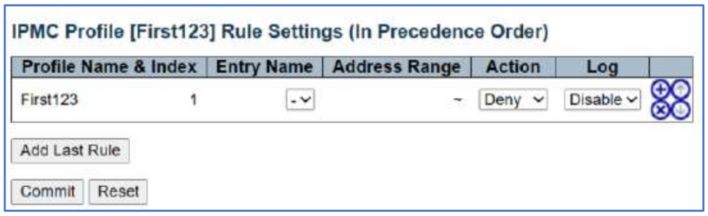


Delete	Profile Name	Profile Description	Rule
□	First123	Second123456	ⓔ

Add New IPMC Profile

Save | Reset

Selecting ⓔ will show the setting:



IPMC Profile [First123] Rule Settings (In Precedence Order)

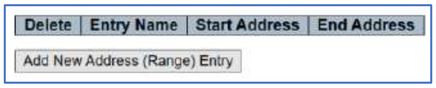
Profile Name & Index	Entry Name	Address Range	Action	Log	
First123 1	-	~	Deny	Disable	⊕ ↑ ⊗ ↓

Add Last Rule

Commit | Reset

Name	Description
Profile Name and Index	The name previous given- this name cannot be edited
Entry Name	The name that will be associated with the profile
Address Range	The address range used for the rule and will be filled in based on the name entered
Action	Action to be taken when the address of the received framed that matches the address of the rule. **Permit:** Group address matches the range specified in the rule will be learned. **Deny**: Group address matches the range specified in the rule will be dropped.
Log	Controls what is logged: **Enable**: Corresponding information of the group address, that matches the range specified in the rule, will be logged. **Disable**: Corresponding information of the group address, that matches the range specified in the rule, will not be logged
Radio Buttons	Used to Manage the rules. ⊕: Insert a new rule before the current entry of rule. ⊗: Delete the current entry of rule. ↑: Moves the current entry of rule up in the list. ↓: Moves the current entry of rule down in the list.

6.9.3 IPMC Profile Address Configuration

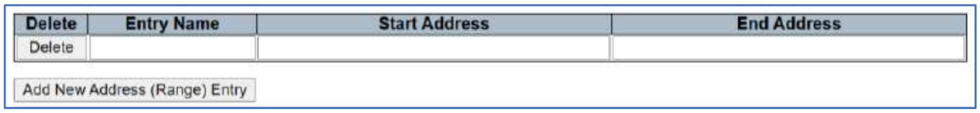


Delete	Entry Name	Start Address	End Address

Add New Address (Range) Entry

6.9.3 IPMC Profile Address Configuration

Name	Description
Add New Address Entry	Click to add new address



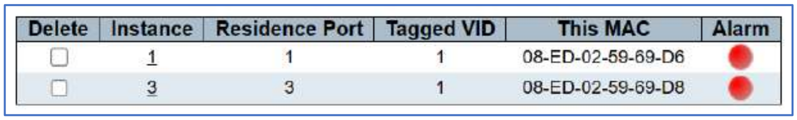
Delete	Entry Name	Start Address	End Address
Delete			

Name	Description
Delete	Delete information for that entry
Entry Name	The name used to index the address entry table. The name is 16 alph and numbers with at least one alpha
Start Address	The starting address for the group addresses. It can either be IPv4 or IPv6
End Address	The ending address for the group
Add New Address	Add new entries

6.10 MEP - Maintenance Entity Point

MEP defines the point at which the network sends and receives messages in order to confirm connectivity to a network.

6.10.1 MEP Programming

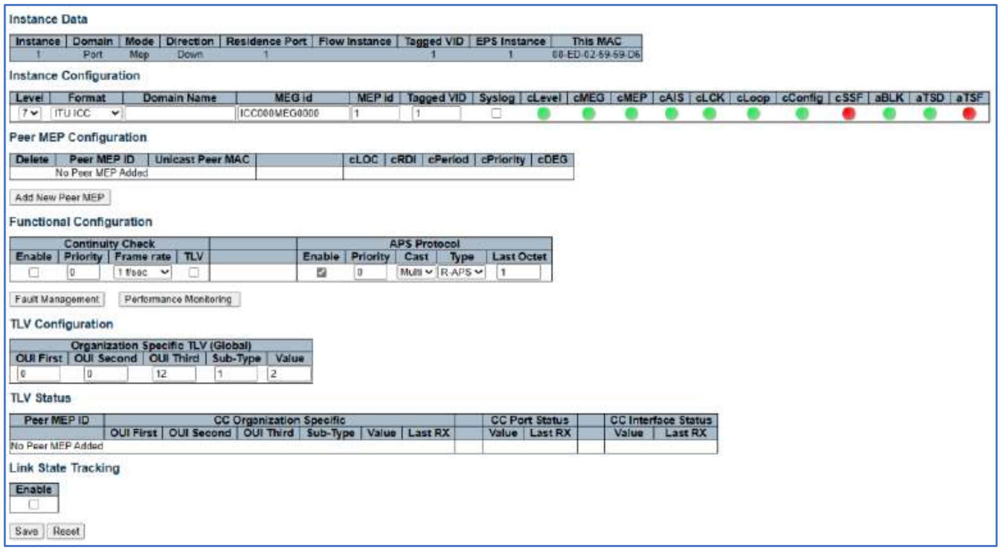


Delete	Instance	Residence Port	Tagged VID	This MAC	Alarm
□	1	1	1	08-ED-02-59-69-D6	●
□	3	3	1	08-ED-02-59-69-D8	●

6.10.1 MEP Programming

Name	Description
Delete	For deleting the input
Instance	The ID of the MEP for entering the configuration range which is 1-100
Residence Port	Names the port
Tagged VID	Indicates if the port is tagged- entering 0=no tagging
MAC Address	Information only indicates MAC and is only active when unicasting is active
Alarm	Red indicates Alarm activity
Add New MEP	To add a new MEP entry

Select the Instance to display the following.
The following results and programming are dependent upon the previous programming.



Instance Data

Instance	Domain	Mode	Direction	Residence Port	Flow Instance	Tagged VID	EPS Instance	This MAC
1	Port	Mep	Down	1		1	1	08-ED-02-59-69-D6

Instance Configuration

Level	Format	Domain Name	MEG id	MEP id	Tagged VID	Syslog	cLevel	cMEG	cMEP	cAIS	cLCK	cLoop	cConfig	cSSF	aBLK	aTSD	aTSF
7	ITU ICC		ICC000MEG0000	1	1	□	●	●	●	●	●	●	●	●	●	●	●

Peer MEP Configuration

Delete	Peer MEP ID	Unicast Peer MAC		cLOC	cRDI	cPeriod	cPriority	cDEG
	No Peer MEP Added							

Functional Configuration

Continuity Check					APS Protocol				
Enable	Priority	Frame rate	TLV		Enable	Priority	Cast	Type	Last Octet
□	0	1 f/sec	□		☑	0	Multi	R-APS	1

TLV Configuration

Organization Specific TLV (Global)				
OUI First	OUI Second	OUI Third	Sub-Type	Value
0	0	12	1	2

TLV Status

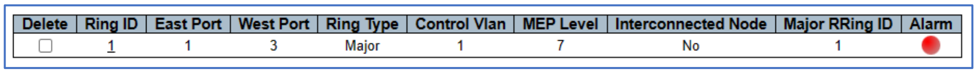
Peer MEP ID	CC Organization Specific						CC Port Status			CC Interface Status	
	OUI First	OUI Second	OUI Third	Sub-Type	Value	Last RX	Value	Last RX		Value	Last RX
No Peer MEP Added											

Link State Tracking

Enable
□

6.11 ERPS - Ethernet Rapid Ring Protection Switching

Ethernet Rapid Ring Protection Switching is a group of connections allowing the movement of data through the loop. In the event a node is lost, the ring will find the best path to communicate with as many nodes as possible.



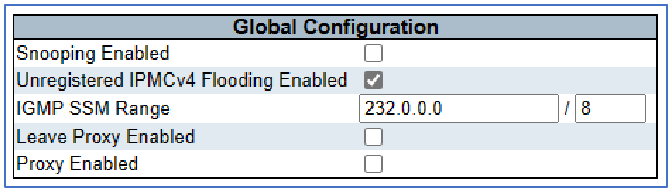
Delete	Ring ID	East Port	West Port	Ring Type	Control Vlan	MEP Level	Interconnected Node	Major RRing ID	Alarm
□	1	1	3	Major	1	7	No	1	●

6.11 ERPS - Ethernet Rapid Ring Protection Switching

Name	Description
Delete	Marking this will delete the input on the next save
Ring ID	The number ID of the ring which can be 1-64
East Port	The port communicating the MEP for the ring
West Port	The port communicating the MEP for the ring
Ring Type	This is defined as Major: = the main ring and Sub= which is the ring within the Main rign.
Control VLAN	Assigns the VLAN number to the ring
MEP Level	The MEP level associated with the interconnected sub ring
Interconnected Node	This defines the nodes that are part of the ring with specific ports that communicate to the ring – indicated this will direct the ring must communicate with this node
Major RRing ID	This defines the major communicates used for updating
Alarm	Indicates if an alarm has occurred on the ring

6.12 IGMP Snooping

IGMP Snooping (Internet Group Management Protocol)
IGMP is the key to multicasting and monitors traffic controlling IP multicasts between a host and other devices on the network. The process helps to restrict bandwidth by restricting traffic to only those devices on the network that are programmed to receive the transmissions from the host.

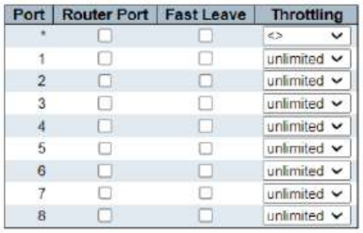


Global Configuration	
Snooping Enabled	□
Unregistered IPMCv4 Flooding Enabled	☑
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	□
Proxy Enabled	□

6.12 IGMP Snooping Configuration

Name	Description
Snooping Enabled	Check to enable Snooping
Unregistered IPMCv4 Flooding Enabled	Check to enable= provides flood control when IGMP is enabled
IGMP SSM Range	SSM=Source Specific Multicast= programs IGMP within a specific range based on valid IPv4 multicast addresses – the prefix address range is based on 232. X . X .X - = 232.0.0.0/8 is generally a default setting
Leave Proxy Enabled	Active with check box = enacts IGMP leave when a data message without sending any indication of last message transmit
Proxy Enabled	Active with check box= this feature directs traffic to specific multicast groups. Proxy acts as an intermediary for multicasting between network segments

6.12.1 IGMP Port Related Configuration

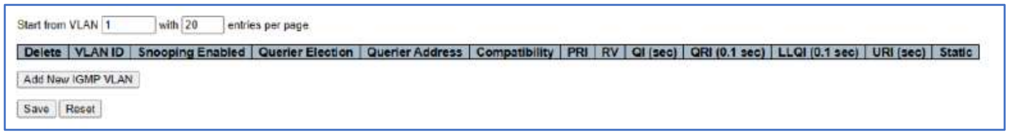


Port	Router Port	Fast Leave	Throttling
*	□	□	<>
1	□	□	unlimited
2	□	□	unlimited
3	□	□	unlimited
4	□	□	unlimited
5	□	□	unlimited
6	□	□	unlimited
7	□	□	unlimited
8	□	□	unlimited

6.12.1 IGMP Port Related Configuration

Name	Description
Port	Fixed port number
Router Port	The selected switch port that directs data to the assigned Layer 3 multicast network devices or Query devices which has priority
Fast Leave	If a stop forwarding message transmission will stop – the setting are unlimited to 10.
Throttling	This allows or limits the number of multicast groups the switch can belong to

6.12.2 IGMP Snooping VLAN Configuration

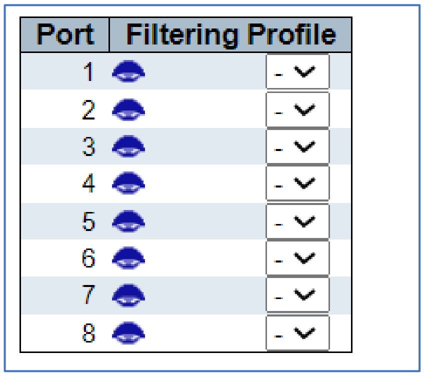


Start from VLAN 1 with 20 entries per page

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)	Static

6.12.2 IGMP Snooping VLAN Configuration

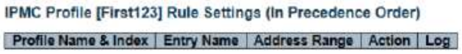
Name	Description
Delete	Deletes line entered information
VLAN ID	The VLAN ID entry point as previous defined
Snooping Enabled	Enables individual VLAN snooping with a maximum of 32 VLANS
Querier Election	Will querier those connects with querier enabled- must be disabled for non querier devices
Querier Address	Using IPv4 defines the querier address – if not set the system will use the first available IPv4 address
Compatibility	This is based on compatibility between the hosts and routers and is dependent on the IGMP version The allowed selection is **IGMP-Auto**, **Forced IGMPv1**, **Forced IGMPv2**, **Forced IGMPv3**, default compatibility value is IGMP-Auto. It is recommended the setting remain on IGMP-auto
PRI	Is Priority of Interface which controls the frame priority level as generated by the system. The setting ranges from 0 -7.
RV	Is Robustness Variable = which determines the expected packet loss. Setting can range between 1- 255 with a default setting of 2.
Q1 (SEC)	This is Query Interval and is used with Querier functions. It determines the interval between queries with a setting range of 1 – 32744 seconds and a default setting of 125 second
QRI (0.1SEC)	This determines the response time based on the Q1 setting range it is set in 10ths of seconds with a default of 10 seconds
LLQ1 (0.1sec)	Last member query interval= is the reporting time of the last IGMP member and base on the Q1 setting as programmed in 10ths of second default is 1 second
URI (sec)	Unsolicited Report Interval – is the time between repetitions of a host's initial report of membership in a group the range is the same as Q1
Static	Setting is disabled = system is free run. Enabled = system refers to settings



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

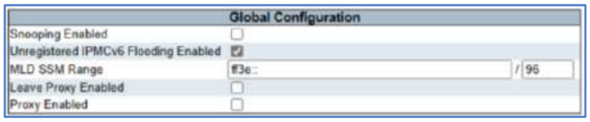
6.12.3 IGMP Snooping Port Filter Profile Configuration

6.12.3 IGMP Snooping Port Filter Profile Configuration

Name	Description
Port	Fixed port number
Filtering Profile	This selects the IPMC Profile for the port
Profile Management Button	Opens the rules for the port profile. To see the First123 rule settings you have to save the setting and then select the eye icon. It will display the rules as follows. They are fixed by previous settings.
IPMC Profile (First 123) Rule Settings	 IPMC Profile [First123] Rule Settings (In Precedence Order) Profile Name & Index | Entry Name | Address Range | Action | Log

6.13 MLD Snooping

IPv6 is a different addressing sequence from IPv4. For the following to be active even if programmed, the a device connected to a specific port must have an IPv6 address. MLD is Multicast Listener Discovery is used for connecting to and listing for IPv6 devices on a network.

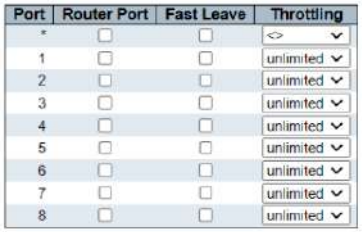


Global Configuration	
Snooping Enabled	☐
Unregistered IPMCv6 Flooding Enabled	☑
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	☐
Proxy Enabled	☐

6.13 1MLD Snooping Configuration

6.13.1 MLD Snooping Port Related Configuration

Name	Description
Snooping Enabled	If checked Snooping is Enabled. Action of the following settings require that Snooping is Enabled
Unregistered IPMCv6 Flooding Enabled	IPMCv6 can be registered or unregistered if check the setting will respond to unregistered traffic and could result in flooding
MLD SSM Range	SSM is Source Specific Multicast. The source must be SSM aware for both hosts and routers within the address range – the IPv6 address needs a prefix length from 8-128.
Leave Proxy Enabled	This avoids forwarding unnecessary messages to the router reducing traffic
Proxy Enabled	Then active traffic will only be forwarded to the proxy router

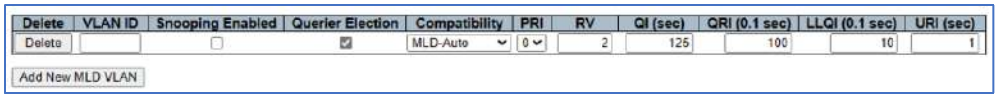


Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☐	☐	unlimited
7	☐	☐	unlimited
8	☐	☐	unlimited

6.13.1 MLD Snooping Port Related Configuration

Name	Description
Port	Port number is fixed
Router Port	Check box will indicate the port is connected to a router
Fast Leave	If checked the port will stop forwarding data if a leave message is received and will not send a query message
Throttling	This will limit the number of groups to be sent. The range is unlimited to a limit of 10

6.13.2 MLD Snooping VLAN Configuration



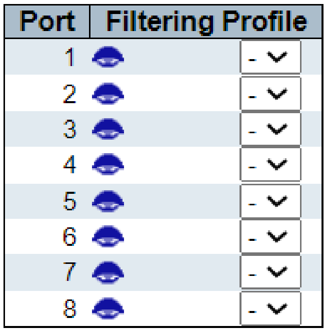
Delete	VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Delete		□	☑	MLD-Auto	0	2	125	100	10	1

Add New MLD VLAN

6.13.2 MLD Snooping VLAN Configuration

Name	Description
Delete	Deletes the entry
VLAN ID	Input the previously programmer VLAN ID number
Snooping Enabled	Enables snooping on the selected VLAN. The total number of VLANs is 32
Querier Election	When enabled a querier can be contained with snooping when disabled non queriers will be included
Compatibility	Sets the compatibility with hosts and routers which depend on the MLD version. The allowed selection is **MLD-Auto**, **Forced MLDv1**, **Forced MLDv2**, default compatibility value is MLD-Auto.
PRI	Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is **0** (best effort) to **7** (highest), default interface priority value is 0.
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is **1** to **255**, default robustness variable value is 2.
QI (sec)	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is **1** to **31744** seconds; default query interval is 125 seconds.
QRI (0.1sec)	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is **0** to **31744** in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds).
LLQI (0.1sec)	Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is **0** to **31744** in tenths of seconds; default last listener query interval is 10 in tenths of seconds (1 second).
URI (sec)	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is **0** to **31744** seconds; default unsolicited report interval is 1 second.
Add new MLD VLAN	Select to create a new entry

6.13.3 MLD Snooping Port Filtering Profile Configuration

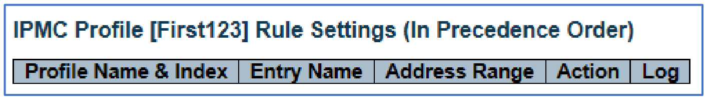


Port	Filtering Profile
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

6.13.3 MLD Snooping Port Filtering Profile Configuration

Name	Description
Port	Fix port number
Filtering Profile	Selects the IPMC profile as previously programmed
Eye Icon	You must select a filtering profile prior to selecting the icon

6.13.4 IPMC Profile



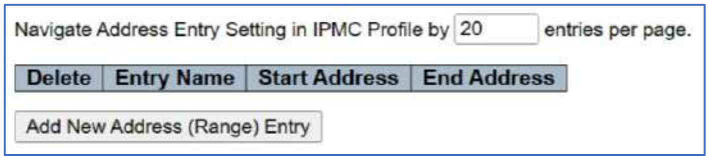
IPMC Profile [First123] Rule Settings (In Precedence Order)

Profile Name & Index	Entry Name	Address Range	Action	Log

6.13.4 IMPC Profile

The above will appear with information previous entered.

6.13.5 PMC Profile Address Configuration



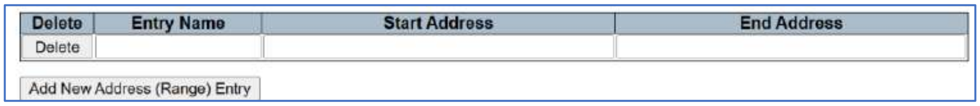
Navigate Address Entry Setting in IPMC Profile by 20 entries per page.

Delete	Entry Name	Start Address	End Address

6.13.5 PMC Profile Address Configuration

Name	Description
Number of Entries per Page	Enter the number of Entries you want to display per page
Add New Addressed	Selects to enter a new address

6.13.6 IPMC Profile Address Configuration



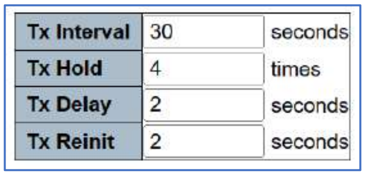
Delete	Entry Name	Start Address	End Address
Delete			

6.13.6 IPMC Profile Address Configuration

Name	Description
Delete	Select followed by save to delete the entry
Enter a name	Name can be a maximum of 16 Alpha/numeric with at least one alpha
Start Address	Enter the starting IPv4 or IPv6 multicast group address
End Address	Enter the ending IPv4/IPv6 Alpha/numeric group address

6.14 LLDP Parameters

LLP Link Layer Discovery Protocol allows all network components with LLDP ability to communicate with each other advertising their major status.

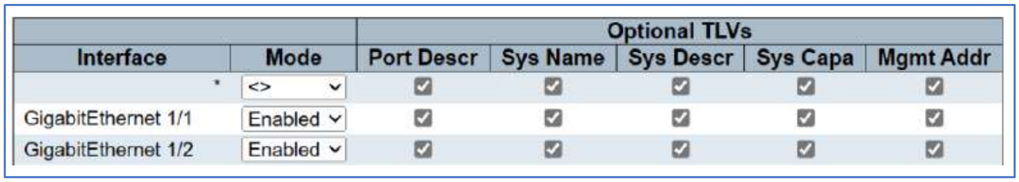


Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

6.14 LLDP Parameters

Name	Description
Tx Interval	The interval between LLDP transmitted frames. Valid values are 5-32768 seconds
Tx Hold	Determines how long the LLDP transmitted frames will be valid. Values are expressed in times and then multiplied by the interval
Tx Delay	If a new IP address or any configuration is entered this will be the time prior to transmitting between frames. Values are 1-8192 seconds
Tx Reinit	This determines the time a message is transmitted to all network points with an interface within the network is shut down and a new LLDP is started

6.14.1 LLDP Interface Configuration



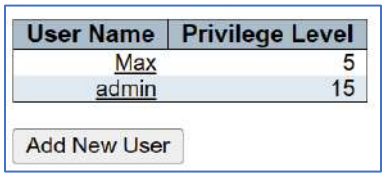
		Optional TLVs				
Interface	Mode	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Enabled	☑	☑	☑	☑	☑
GigabitEthernet 1/2	Enabled	☑	☑	☑	☑	☑

6.14.1 LLDP Interface Configuration

Name	Description
Interface	Fixed Port number
Mode	There are four states. **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.
Port Description	When checked the description is included in the LLDP information
Sys Name	When checked the System name is included in the LLDP information
Sys Capability	When checked the System Capability is included in the LLDP information
Mgmt Address	When checked the management address is included in the LLDP information

Chapter 7: Security Configure

7.1 Users Configuration

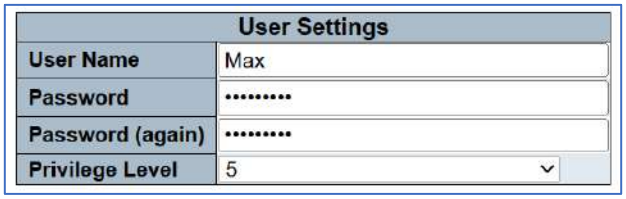


User Name	Privilege Level
Max	5
admin	15

7.1 Users Configuration

Name	Description
Username	Displays the number of assigned users and their associated Privilege Levels
Add New User	Select to add a new user

7.1.1 Changing user setting.



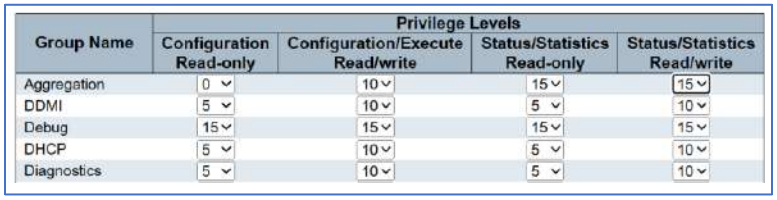
User Settings	
User Name	Max
Password	•••••••••
Password (again)	•••••••••
Privilege Level	5

7.1.1 Changing user setting

Name	Description
Username	Add or change username: Valid is 1-31 characters
Password	Add or change password associated with username
Password	Re-enter password to verify
Privilege Level	You can assign 1 -15 different permission levels which define the permission given to the user

Each operation can be assigned a specific privilege level for each programmable function for each of 4 functions.

7.2 Privilege Level Configuration



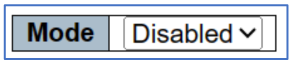
Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	0	10	15	15
DDMI	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
Diagnostics	5	10	5	10

7.2 Privilege Level Configuration

Name	Description
Group	Fixed defines the switch functions
Configuration Read only	Level defines user can read but not program function
Configuration/Execute Read/write	Level defines user can read and program function
Status/Statistics Read only	Level defines user can only read Statistics
Status/Statistics Read/Write	Level defines user can both read and write to Statistics
Set level	Level will determine permission given to that function

7.3 SSH Configuration

SSH is a Secured Shell allowing data to be exchanged over a secured channel with encrypted communications.



Mode	Disabled

7.3 SSH Configuration

Name	Description
Mode	Disable/Enable

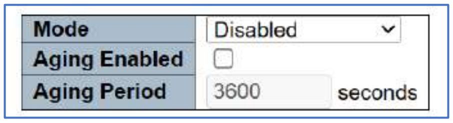
7.4 HTTPS Configuration

HTTPS stands for Hypertext Transfer, Protocol over Secure Socket Layer. It secures communication between two points using port 443 instead of port 80 which is used for open network communications.

Name	Description
Mode	Disable/Enable
Automatic Redirect	When active if the mode is enabled an HTTP connection will be automatically directed to a HTTPS connection.
Certification Maintain	The operation of certificate maintenance. Possible operations are: **None**: No operation. **Delete**: Delete the current certificate. **Upload**: Upload a certificate PEM file. Possible methods are **Web Browser** or **URL**. **Generate**: Generate a new self-signed RSA certificate.
Certification Status	Display the status of certificate on the switch. Possible statuses are: **Switch secure HTTP certificate is presented**. **Switch secure HTTP certificate is not presented**. **Switch secure HTTP certificate is generating ...**

7.5 Port Security Limit Control Configuration

This setting defines the number of users that can access a port.

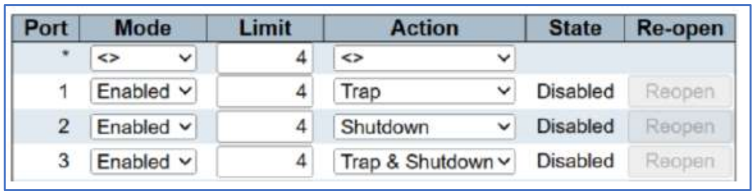


Mode	Disabled
Aging Enabled	☐
Aging Period	3600 seconds

7.5 Port Security Limit - System Configuration

Name	Description
Mode	Is a Global setting. If disabled alternative settings can be use
Aging Enabled	If checked the MAC addresses will be subject to the Aging period as defined by the Aging period
Aging Period	The duration can be 10-10,000,000 seconds. This setting use if a host switch is connected to another switch or port on which Limit Control is enable. If the source host is log outed or powered down – the end host will still be using its resources. At the end of the period the switches on the network will evaluate valid connections and free up any connection that is not for forwarding.

7.5.1 Port Limit Port Configuration



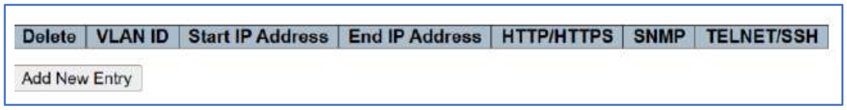
Port	Mode	Limit	Action	State	Re-open
*	<>	4	<>		
1	Enabled	4	Trap	Disabled	Reopen
2	Enabled	4	Shutdown	Disabled	Reopen
3	Enabled	4	Trap & Shutdown	Disabled	Reopen

7.5.1 Port Limit Port Configuration

Name	Description
Port	Port Number is fixed
Mode	Enable/Disable
Limit	Maximum number of MAC addresses that can be secured to the port. The maximum number is 1024
Action	**None:** Do not allow more than Limit MAC Addresses on the but it sensed take no further action. Trap If the Limit plus 1 MAC is sensed send a SNMP **Trap** -Note is aging is disabled on one SNMP trap will be sent, if enable SNMP trap will be sent each time the limit is exceeded by 1. **Shutdown:** If limit is exceeded by 1 the port will be shut down. **Trap and Shutdown:** This combination of the two if the Limit is exceeded by 1
State	This shows the current state of the port: The state takes one of four values: **Disabled**: Limit Control is either globally disabled or disabled on the port. **Ready**: The limit is not yet reached. This can be shown for all actions. **Limit Reached**: Indicates that the limit is reached on this port. This state can only be shown if Action is set to **None** or **Trap**. **Shutdown**: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to **Shutdown** or **Trap & Shutdown**.
Re-open	If the port is shutdown if can be re-opened by using this button

7.6 Access Management

Determines and regulates data and can prevent data transferred as per programming.



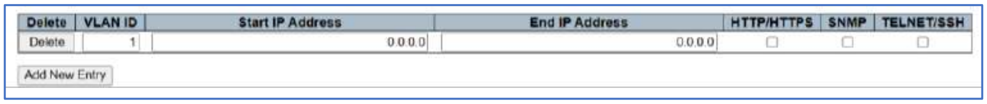
Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH

Add New Entry

7.6 Access Management

Name	Description
Enable/Disable	Enable or disable function
Add New Entry	Select to add a new entry

7.6.1 Program Access Management Configuration



Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	1	0.0.0.0	0.0.0.0	□	□	□

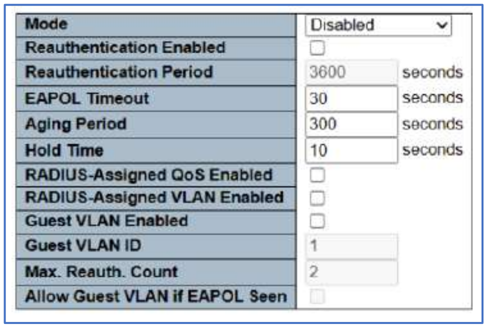
Add New Entry

7.6.1 Program Access Management Configuration

Name	Description
Delete	Delete the entry followed by save
VLAN ID	Enter the VLAN Number ID that allows to the settings
Start IP address	Enter the starting IP address for the start of access management
End IP Address	Enter the end IP address for the end of the access management
HTTP/HTTPS	Allows the host (switch) to access other switches using the HTTP/HTTPS interface if the IP address matches the input range of IP addresses entered
SNMP	If active the host switch can access the other switches using the SNMP interface if the IP address range is matched
Telnet/SSH	If active the host switch can access other switches using the Telnet or SSH interface if the IP address range is matched

7.7 802.1X - Network Access System Configuration

This setting sets up a gateway between the switch and the wider network using authentication information usually in the form of a username and password when a Radius server is used. A Radius server is a client-based protocol allowing remote access switches/servers to communicate with a central server/switch.



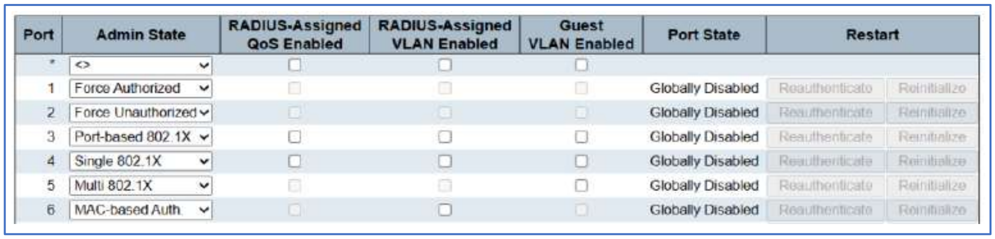
Mode	Disabled
Reauthentication Enabled	□
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	□
RADIUS-Assigned VLAN Enabled	□
Guest VLAN Enabled	□
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	□

7.7 802.1x - Network Access System Configuration

Name	Description
Mode	Mode is enabled/disabled
Reauthentication Enabled	If active authentication will occur based on the reauthentication period
Reauthentication Period	The reauthentication period. The duration is 1 to 3600 second
EAPOL Timeout	Determines the time for EAPOL Identification frames – An EAPOL frame is requested to disconnect- it does not affect MAC based ports
Aging Period	This setting applies modes relating to 802.1X for port security based on MAC addresses
Hold Time	If access is denied the hold time will reject frames during this period
RADIUS Assigned QoS enabled	Uses QoS settings for traffic control coming from authorized sources
RADIUS Assigned VLAN Enabled	Uses VLAN enabled for traffic control coming from authorized sources
Guest VLAN Enabled	Used for VLANs with limited network access when active ports that mirror settings can be used into the area and used depending on the value of Guest VLAN ID
Guest VLAN ID	The values are 1-4095
Max Reauth Count	The number of times a EAPOL can be made the value is 1-255
Allow Guest VLAN If EAPOL	Determines the status of a valid EAPOL frame to allow entry to the Guest VLAN

This setting applies to individual ports.

7.7.1 Network Access System Configuration- Port Configuration



Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	□	□	□			
1	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
2	Force Unauthorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
3	Port-based 802.1X	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
4	Single 802.1X	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
5	Multi 802.1X	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
6	MAC-based Auth.	□	□	□	Globally Disabled	Reauthenticate	Reinitialize

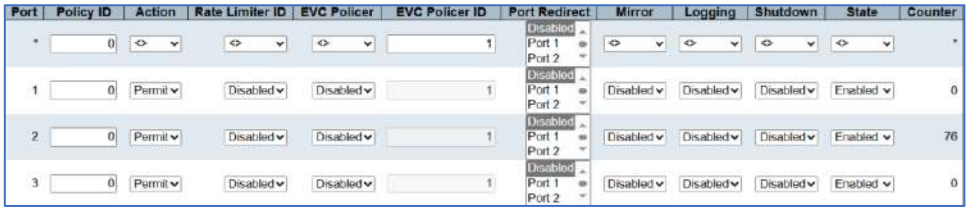
7.7.1 Network Access System Configuration- Port Configuration

Name	Description
Port	Number of the logical port
Admin State	If the NAS is globally enabled the individual port's authentication mode. The modes are **Force Authorized** – switch will send on EAPOL Success frame when port becomes active and can be accessed without authorization **Force Unauthorized**- when port becomes active switch will send EAPOL and if it is a failure frame access will be denied. **Port Based 802.1X** access is based on a 802.1x communications. **Single 802.1x** – upon receiving one authenticated communication the port will be opened to network traffic. **Multi 802.1.x** - Multiple authenticated communications can be received at the one port **MAC Based Auth.** -authentication is based on MAC addresses
Radius – Assigned QoS Enabled	Assigns incoming traffic to RADIUS Based on QoS
RADIUS Assigned VLAN Enabled	Assigns incoming traffic to VLAN RADIUS enabled
Guest VLAN Enabled	When active individual ports can be move into the Guest VLAN – this is based on transmitting EAPOL
Port State	The following programmable states are: **Globally Disabled:** NAS is globally disabled. **Link Down:** NAS is globally enabled, but there is no link on the port. **Authorized:** The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. **Unauthorized:** The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. **X Auth/Y Unauth:** The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
Restart	There are two programmable states: **Reauthenticate:** Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. **Reinitialize:** Forces a reinitialization of the clients on the port and thereby a reauthentication immediately.

7.8 ACL.

7.8.1 ACL Port

Access Control List which controls network traffic but only allowing those programmed with ACL permission (rules) to be included.

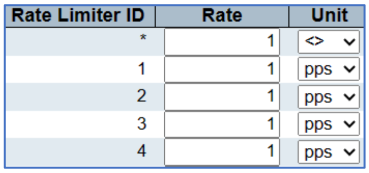


Port	Policy ID	Action	Rate Limiter ID	EVC Policer	EVC Policer ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	1	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	76
3	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

7.8 ACL Ports

Name	Description
Port	The fixed port number
Policy ID	Selects the policy applied to the port. Values at 0-255 with the default at 0
Action	The selection is to Permit or Deny- default is Deny
Rate Limiter ID	Programs either disable (default) or values 1-16 determines the sampling rate
EVC Policer	EVC (Ethernet Virtual Circuit) defines a logical network connection but is not dedicated transporting Ethernet frames – both the EVC Policer and ACL cannot be active together
EVC Policer ID	Selects the EVC ID applied to the port disabled (default) or values 1-256
Port Redirect	Selects the port where frames are redirected or disabled (default).
Mirror	Activates if the port is mirrored with the function. **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is "Disabled".
Logging	Activates Logging function: **Enabled**: Frames received on the port are stored in the System Log. **Disabled**: Frames received on the port are not logged. The default value is "Disabled". Note: The logging feature only works when the packet length **is less than 1518(without VLAN tags)** and the System Log memory size and logging rate is limited.
Shutdown	Will shut down the port: **Enabled**: If a frame is received on the port, the port will be disabled. **Disabled**: Port shut down is disabled. The default value is "Disabled". Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).
State	Determines if ports are closed or reopened: **Enabled**: To reopen ports by changing the volatile port configuration of the ACL user module. **Disabled**: To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".
Counter	Counts the frames that match ACL/ACE

7.8.2 ACL Rate Limit Configuration



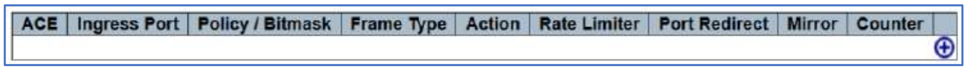
Rate Limiter ID	Rate	Unit
*	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps

7.8.2 ACL Rate Limit Configuration

Name	Description
Rate Limiter ID	Fixed Notes the Rate Limiter ID
Rate	The programmable rate is 0-3276700 and notes pps or 0-1000000 in kbps
Unit	Can be programmed as pps or kbps

7.8.3 Access Control List Configuration

This displays information only as programmed and current status. Modification program is done by selecting ⊕ The maximum number of ACE which consist of the ACL is 256. Start programming with the lowest number.

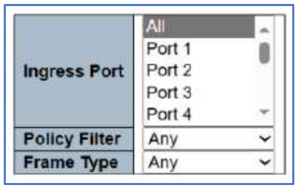


ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
									⊕

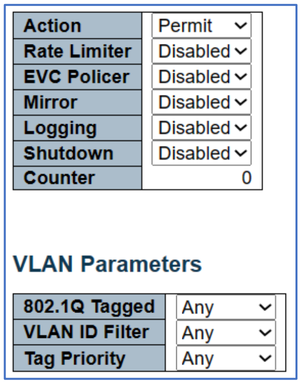
7.8.3 Access Control List Configuration

Name	Description
ACE	Indicates the ACE ID
Ingress Port	The selections are: **All**: The ACE will match all ingress port. **Port**: The ACE will match a specific ingress port.
Policy/Bitmask	Notes the policy number and bitmask of the ACE
Frame/Type	This defines the frame type what is allowed; **Any**: The ACE will match any frame type. **EType**: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. **ARP**: The ACE will match ARP/RARP frames. **IPv4**: The ACE will match all IPv4 frames. **IPv4/ICMP**: The ACE will match IPv4 frames with ICMP protocol. **IPv4/UDP**: The ACE will match IPv4 frames with UDP protocol. **IPv4/TCP**: The ACE will match IPv4 frames with TCP protocol. **IPv4/Other**: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. **IPv6**: The ACE will match all IPv6 standard frames.
Action	Action on forwarding the ACE: **Permit**: Frames matching the ACE may be forwarded and learned. **Deny**: Frames matching the ACE are dropped. **Filter**: Frames matching the ACE are filtered.
Rate Limiter	Selection is (Disabled)-default. Or range 1-16 assigned to the number of the ACE
Port Redirect	Selection is Disabled or specified with a port number
Mirror	Selects the port where ACE frames are mirrored. **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored.
Counter	Counts the number of times the ACE is hit by a frame
⊕	Select this to modify the Ace

7.8.4 Access Configuration



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



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

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

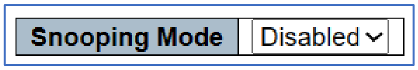
7.8.4 Access Configuration

Name	Description
Ingress Port	Select the specific port all ALL- applies to all ports
Policy Filter	Specifies the policy number applied to ACE **Any**: No policy filter is specified. (policy filter status is "don't-care".) **Specific**: If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.
Frame Type	**Any**: Any frame can match this ACE. **Ethernet Type**: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) and the value should not be equal to 0x800(IPv4), 0x806(ARP) or 0x86DD(IPv6). **ARP**: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type. **IPv4**: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type. **IPv6**: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.
Action	Indicates the action to be taken when a packet is recognized by the ACE **Permit**: The frame that hits this ACE is granted permission for the ACE operation. **Deny**: The frame that hits this ACE is dropped. **Filter**: Frames matching the ACE are filtered.
Rate Limiter	Determines limit of base units. Range is Disabled (default) and 1-16
EVC Policer	Select if the EVC Policer is enabled or disabled- cannot be used with ACL rate limiter is active
Mirror	Determines mirror operation of port for packets matching ACE – selection is enabled or disabled.
Logging	Selection is Enable/Disable for logging matching ACE frames – only works with frame values under 1518bytes
Shutdown	If active the port will shut down if the packet matches ACE. If disabled, the packet will be allowed to pass – note shutdown only works a packet values under 1518bytes
Counter	Counts number of ACE packets
VLAN Parameters	The following settings applied to the VLANs
802.1Q Tagged	The action applies to tagged frames under 802.1Q **Any**: Any value is allowed ("don't-care"). **Enabled**: Tagged frame only. **Disabled**: Untagged frame only. The default value is "Any".
VLAN ID Filter	The selection is: **Any**: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) **Specific**: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.
Tag Priority	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is **0** to **7** or range **0-1**, **2-3**, **4-5**, **6-7**, **0-3** and **4-7**. The value **Any** means that no tag priority is specified (tag priority is "don't-care".

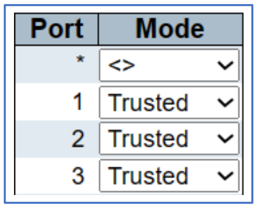
7.9 DHCP

Dynamic Host Configuration Protocol is used to automatically assign IP addresses usually from a DHCP server in order that all address operate on network. It is recommended the use of DHCP be considered with great care as it will not allow for direct access for connected devices unless you know the addresses assigned by the DNCP server.

7.9.1 DHCP Snooping Configuration – (Snooping Setting)



Snooping Mode	Disabled

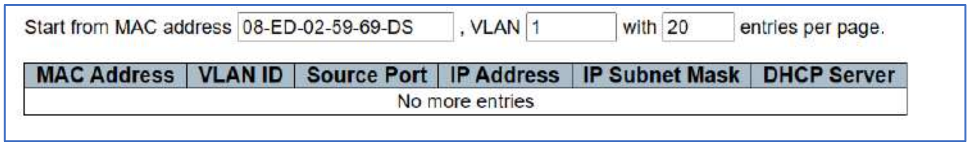


Port	Mode
*	<>
1	Trusted
2	Trusted
3	Trusted

7.9.1 DHCP Snooping Configuration – (Snooping Setting)

Name	Description
Snooping Mode	Enable or Disable Snoop Mode
Port	Port number is fixed
Mode	Indicates the DHCP snooping port mode. Possible port modes are: **Trusted**: Configures the port as trusted source of the DHCP messages. **Untrusted**: Configures the port as untrusted source of the DHCP messages.

7.9.2 Snooping Table- Dynamic DHCP Snooping Table



Start from MAC address 08-ED-02-59-69-DS , VLAN 1 with 20 entries per page.

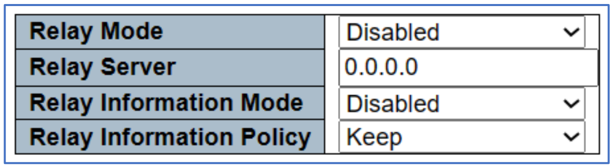
MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server
No more entries					

7.9.1 Snooping Table- Dynamic DHCP Snooping Table

Name	Description
Start MAC Address	The starting MAC address
VLAN Entries	Input the stating VLAN
Entries per page	The number of entries per page
Topic Headers	The topic headers from MAC Address to DHCP shows the information depending on the received information

7.9.3 DHCP Relay Configuration

Relay process is used to forward DHCP agents between clients and servers that are not on the same subnet. The interface address is stored in the DHCP GIADDR (Gateway Address) and determines the subnet value. To correctly operate the VLAN address and PVID (Port VLAN ID) must be correct.

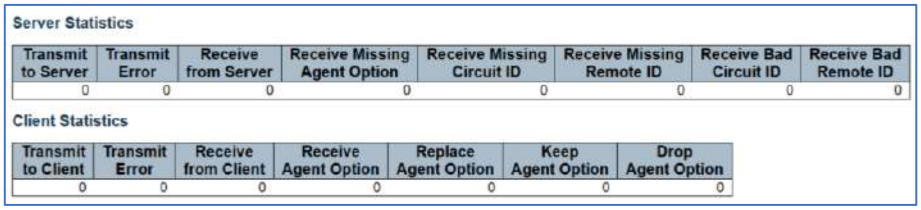


Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Keep

7.9.3 DHCP Relay Configuration

Name	Description
Relay Mode	Enabled: DHCP messages are forwarded and transfers between
Relay Server	This is the relay server's IP address
Relay Information Mode	This is the Relay information mode and conforms to Option 82- the number is constructed as follows: 0006 (VLAN ID 6) 02 (SW ID) 09 (Port Number) **Enable:** this information is transmitted when DHCP is enabled. **Disabled:** Information is not transmitted
Relay Information Policy	**Replace**: Replace the original relay information when a DHCP message that already contains it is received. **Keep**: Keep the original relay information when a DHCP message that already contains it is received. **Drop**: Drop the package when a DHCP message that already contains relay information is received.

7.9.4 DHCP Relay Statistics



Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

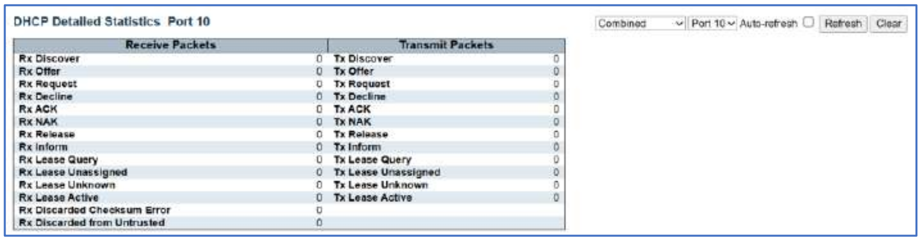
Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

7.9.4 DHCP Relay Statistics

Name	Description
Server/Client Statistics	Based on the previously entered information this will display the resulting information

7.9.4 DHCP Detailed Statistics (Per Port)



DHCP Detailed Statistics Port 10

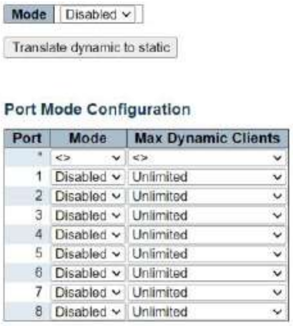
Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

7.9.4 DHCP Detailed Statistics (Per Port)

Name	Description
Per Port DHCP Detailed Statistics	Displays detailed information per port

7.10 IP Source Guard

IP Source Guard restricts IP traffic for untrusted Layer 2 port by filtering packet transmission depending on DHCP snooping binding database or manually configured IP source bindings when enabled all transmission except for DHCP packets with an assigned source IP address will be blocked.



Mode: Disabled

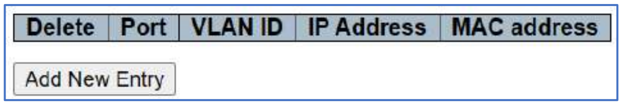
Port Mode Configuration

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

7.9.4 DHCP Detailed Statistics (Per Port)

Name	Description
Mode	Enable/Disable Mode. When enabled ACEs will be lost
Translate dynamic to static	Translates Dynamic entries to static which are required for operation
Port	Port Number is fixed
Mode	Per Port mode is enabled or disabled
Max Dynamic Clients	Defines the maximum number of clients that can be learned on a single port the values are 0,1,2, unlimited. If 0 is selected the only IP packets that will be forwarded are those that match the static entry on that port

7.10.1 IP Source Guard Static IP Guard Table



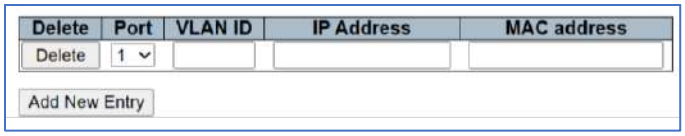
Delete	Port	VLAN ID	IP Address	MAC address

Add New Entry

7.10.1 IP Source Guard Static IP Guard Table

Name	Description
Add New Entry	Select to add a new entry

7.10.2 IP Guard Table

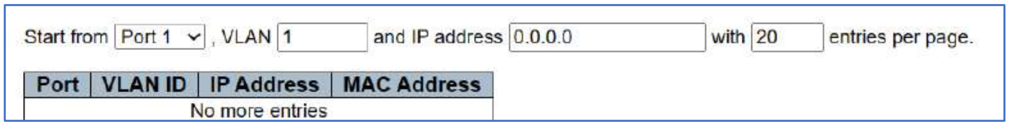


Delete	Port	VLAN ID	IP Address	MAC address
Delete	1			

Add New Entry

Name	Description
Delete	Select to Delete entry
Port	Select the Port Number
VLAN ID	The VLAN ID (must be connected to the Port contained within the VLAN)
IP Address	This is the source IP address contained within the VLAN ID
MAC Address	The MAC address of the connected device
Add New Entry	Select new Entry to add

7.10.3 IP Source Guard Dynamic IP Guard Table



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

Port	VLAN ID	IP Address	MAC Address
No more entries			

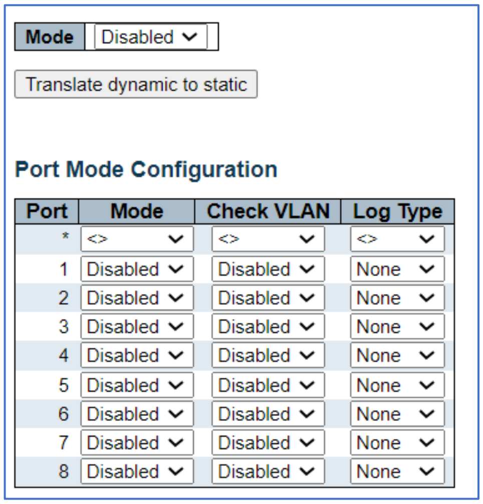
7.10.3 IP Source Guard Dynamic IP Guard Table

Name	Description
Start from Port	Select the port number as the starting point
VLAN	Select the VLAN ID
IP address	Enter the IP address (must be contained in the VLAN)
Port	Displays Port Number
VLAN ID	Displays VLAN ID
IP Address	Displays IP Address
MAC Address	Displays MAC Address

7.11 ARP Inspection

Address Resolution Protocol used to connect changing IP address to a MAC address contained in a local area network (LAN) – it is usually restricted to IPv4 addresses.

7.11.1 ARP Port Inspection Configuration



Mode: Disabled

Translate dynamic to static

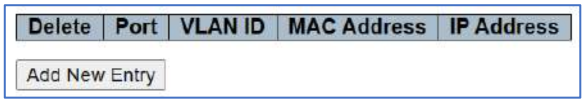
Port Mode Configuration

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

Name	Description
Mode	Select Disable/Enable
Translate dynamic to static	Dynamic input will be translated into static
Port	Fix mode of port
Mode	Enabled: ARP is active. Disable/Enable: When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:
Check VLAN	**Enabled**: Enable check VLAN operation. **Disabled**: Disable check VLAN operation. Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting.
Log Type	**None**: Log nothing. **Deny**: Log denied entries. **Permit**: Log permitted entries. **ALL**: Log all entries.

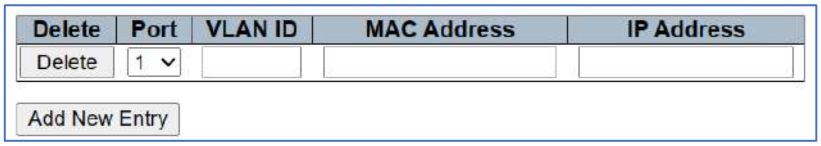
Static ARP Inspection Table

7.11.2 ARP Inspection Table



Delete	Port	VLAN ID	MAC Address	IP Address

Add New Entry



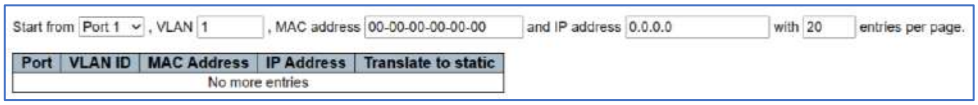
Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1			

Add New Entry

7.11.3 ARP Inspection Table

Name	Description
Add New Entry	Click to make new entry
Delete	Delete entered information
Port	Select port number
VLAN ID	Input the VLAN ID number
MAC Address	Enter MAC address for the ARP packet request
IP Address	Enter IP address for the ARP packet request

7.11.3 Dynamic ARP Inspection Table



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

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

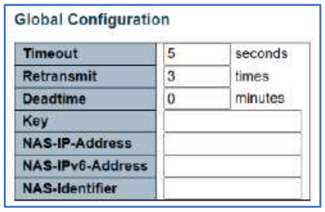
7.11.3 Dynamic ARP Inspection Table

Name	Description
Start from Port	Selects Port number for entry display
VLAN ID	Input VLAN ID permitting ARP traffic
MAC Address	Input associated MAC address
IP Address	Input IP address associated with the entry
Number of entries per page	Input number of pages you want to display per page

7.12 AAA

7.12.1 AAA- REDIUS Server Configuration

Authentication, Authorization and Accounting tracks user activities for IP based networks controlling access to network resources. The process verifies user identity, what that user can do and information on what that user has done. It is used for network security.

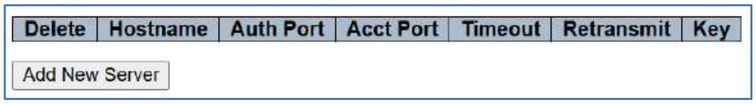


Global Configuration

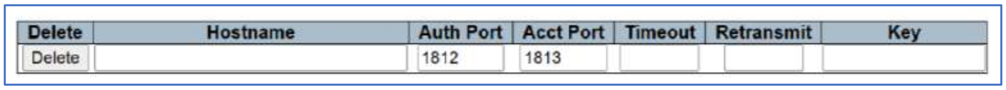
Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

7.12.1 AAA- REDIUS Server Configuration

Name	Description
Timeout	Number of seconds from 1-1000 to receive a reply from a RADIUS server prior to issuing a new transmission
Retransmit	The number of times from 1 to 1000 a RADIUS request is re-transmitted to a server if no responses are received
Deadtime	The time from 0 to 1440 during which the system will not send new requests to a server
Key	A nonpublic word up to 63 characters which is share between the switch and RADIUS server
NAS-IP-Address	The IPv4 address used for the RADIUS to request packets – if blank the IP address of the outgoing interface is used
NAS IPv6 Address	The IPv6 address used for the RADIUS to request packets – if blank the IP address of the outgoing interface is used
NAS – Identifier	The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet



Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key

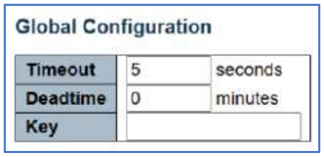


Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Delete		1812	1813			

Name	Description
Add New Server	Click to add new server
Delete	Delete entered information
Hostname	Use IP address or Hostname of the RADIUS server
Auth Port	This is a UDP port on the RADIUS server for authentication 0= disabled
Acct Port	This is a UDP port on the RADIUS server for accounting. 0=disabled
Timeout	This setting overrides the global timeout value. If left blank the global timeout will be used
Retransmit	This setting overrides the global retransmit time. If left blank the global retransmit time will be used
Key	This overrides the global key. If left blank the global key will be used

7.12.2 AAA- TACACS+ Server Configuration

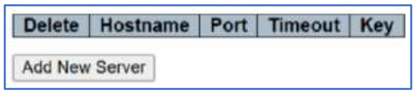
Terminal Access Controller Access Control System provides centralize authentication, authorization, and accounting (in the form of AAA, services for switch data transmission to connected devices such as routers, firewalls, and other switches



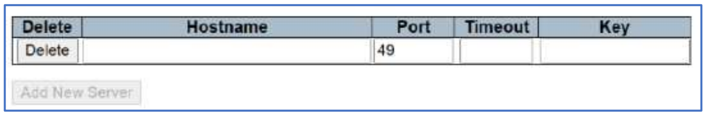
Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key		

Name	Description
Timeout	Input the number of seconds 1 to 1000 to wait for a reply from a TACACS+ server. If a response is not received in the specified time the server is considered as of line.
Deadtime	This is the time from 0-1440 minutes when the switch will not send new requests to a failed request.
Key	A private name shared between TACACS+ server and switch



Delete	Hostname	Port	Timeout	Key



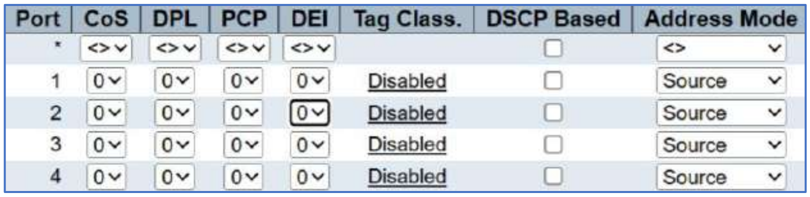
Delete	Hostname	Port	Timeout	Key
Delete		49		

Name	Description
Add New Server	Select to add new server information
Delete	To delete server information
Hostname	Enter IP address or hostname for TACACS+ server
Port	The TCP port of the TACACS+ server for authentication
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key

Chapter 8: QoS Configure

8.1 Qos Ingress Port Classification

Quality of service measures and helps to control network traffic to assure performance by assigning priority based on assigned performance.

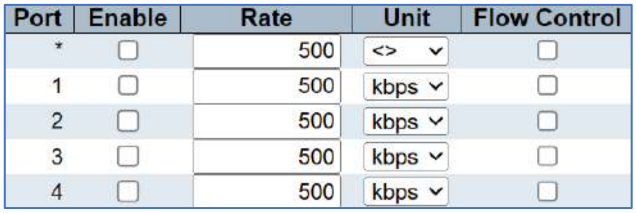


Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<>	<>	<>	<>		□	<>
1	0	0	0	0	Disabled	□	Source
2	0	0	0	0	Disabled	□	Source
3	0	0	0	0	Disabled	□	Source
4	0	0	0	0	Disabled	□	Source

8.1 Qos Ingress Port Classification

Name	Description
Port	Fixed- the logical port number
CoS	Class of Service – provides priority of selected traffic. Range is 0-7 with 0 having the lowest priority 7 the highest
DPL	Drop Precedence Level – monitors traffic to prevent information from being routed outside the network – the port must be VLAN aware, tagged and tag class- if QCL is set that setting will over rule DPL
PCP	Port Control Protocol-allows the host switch to forward data from another device using Network Address Translation (information from a router) or packet filtering. – The port must be VLAN aware with the packet tagged. Range is 0-7 with 0 having the lowest priority 7 the highest
DEI	Drop Eligible Indicator is contained within a VLAN tag- indicator the priority if a frame needs to be dropped
Tag Class	Selection is Enable: Use mapped version of PCP and DEI for tagged frames. Disable: Use default CoS and DPL for tagged frames- note this function is functional for Tagged packets on unaware ports.
DSCP Based	Differential Services Code Point classifies network traffic based on a header inserted in the Ingress packets it establishes route and priority.
Address Mode	Defines the address depending in the IP/MAC address mode: Source: Enable SMAC/SIP matching. Destination: Enable DMAC/DIP matching.

8.2 Qos Ingress Port Policers

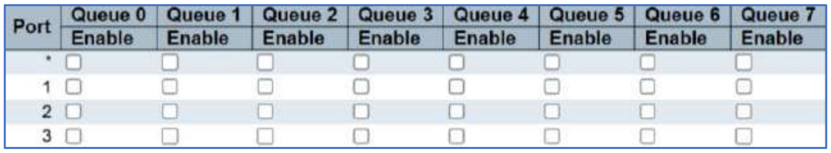


Port	Enable	Rate	Unit	Flow Control
*	□	500	<>	□
1	□	500	kbps	□
2	□	500	kbps	□
3	□	500	kbps	□
4	□	500	kbps	□

8.2 Qos Ingress Port Policers

Name	Description
Port	The logical port number fixed
Enable	Enables/Disables the port policer for the port
Rate	Defines the rate applied to the port. Programming is 100-3276700 when the Unit selected id kbps or bps. Or 1-3276 when the Unit is defined as Mbps or Kfps.
Unit	Defines the unit as Kbps, bps Mbps or Kbps and determines the rate definition
Flow Control	When active pause frames will be sent instead of being discarding

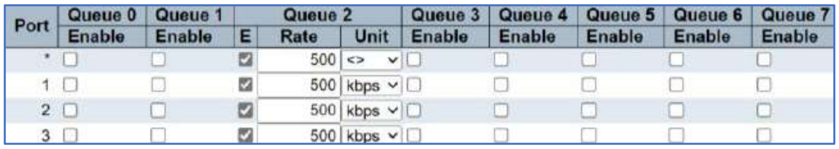
8.3 Qos Ingress Queue Policers



Port	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□

8.3 Qos Ingress Queue Policers

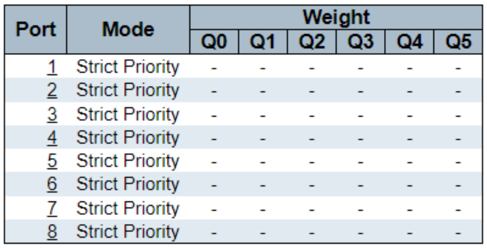
Name	Description
Port Number	The logical port number – the number is fixed
Enable Queue	Will Enable or Disable the port – Select this to move to the submenu



Port	Queue 0	Queue 1	Queue 2			Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable
*	□	□	☑	500	<>	□	□	□	□	□
1	□	□	☑	500	kbps	□	□	□	□	□
2	□	□	☑	500	kbps	□	□	□	□	□
3	□	□	☑	500	kbps	□	□	□	□	□

Name	Description
Port	Logical fixed port number
Enable/Disable	Enable or disable for the specific indicated Queue as previous selected. When you enable a specific queue, the other selections will follow
Rate	Controls the rate for the queue policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This setting only applies to the selected Queue
Unit	Controls the unit of measure for the queue policer rate as kbps or Mbps. This setting only applies to the selected Queue

8.4 QoS Egress Port Schedulers

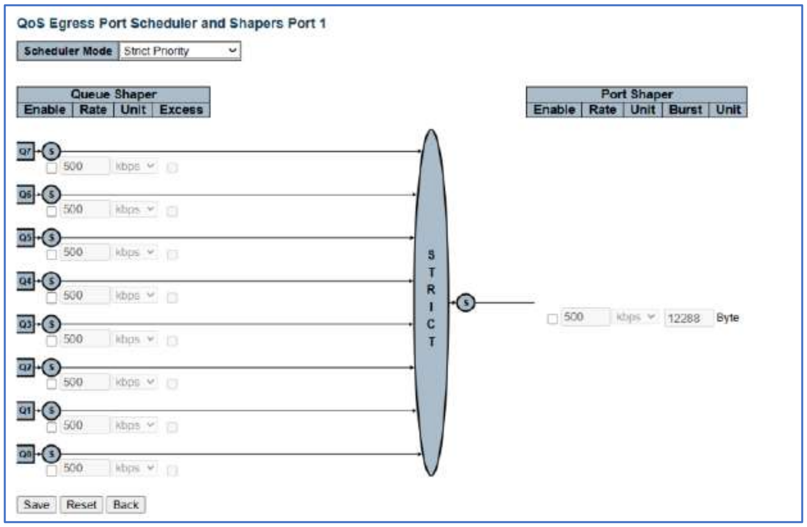


Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-

8.4 QoS Egress Port Schedulers

Name	Description
Port	Fixed logical port number
Mode	Show Scheduling mode-select the port number for further programming
Weight	Show Weight programmed Q0-Q5 -select the port number for further programming

When the individual port is select the further programming for that port will appear

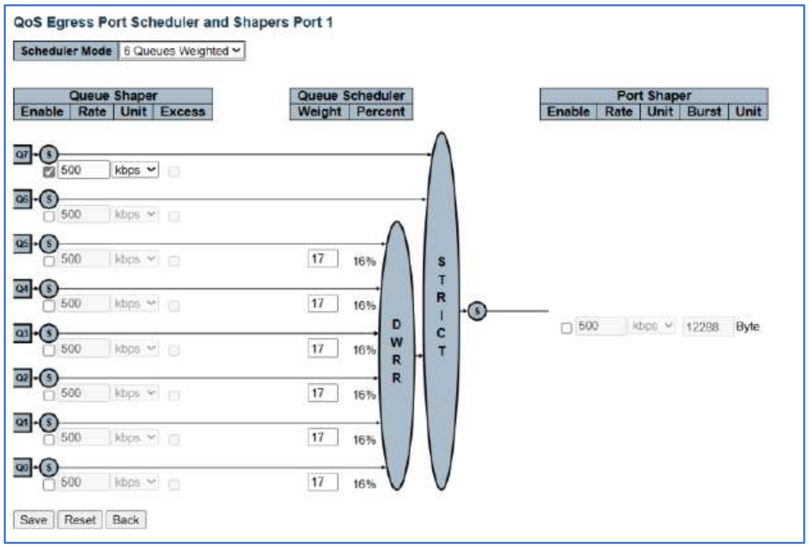


QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

Queue Shaper			
Enable	Rate	Unit	Excess
Q7 ☐	500	kbps	☐
Q6 ☐	500	kbps	☐
Q5 ☐	500	kbps	☐
Q4 ☐	500	kbps	☐
Q3 ☐	500	kbps	☐
Q7 ☐	500	kbps	☐
Q1 ☐	500	kbps	☐
Q0 ☐	500	kbps	☐

Port Shaper				
Enable	Rate	Unit	Burst	Unit
☐	500	kbps	12288	Byte



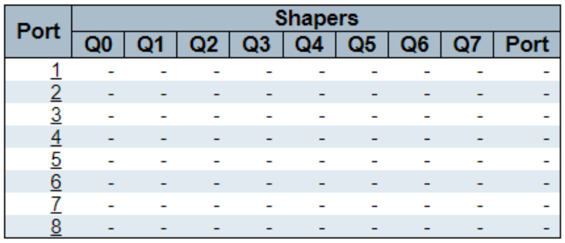
QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: 6 Queues Weighted

Queue Shaper				Queue Scheduler	
Enable	Rate	Unit	Excess	Weight	Percent
Q7 ☑	500	kbps	☐		
Q6 ☐	500	kbps	☐		
Q5 ☐	500	kbps	☐	17	16%
Q4 ☐	500	kbps	☐	17	16%
Q3 ☐	500	kbps	☐	17	16%
Q2 ☐	500	kbps	☐	17	16%
Q1 ☐	500	kbps	☐	17	16%
Q0 ☐	500	kbps	☐	17	16%

Port Shaper				
Enable	Rate	Unit	Burst	Unit
☐	500	kbps	12288	Byte

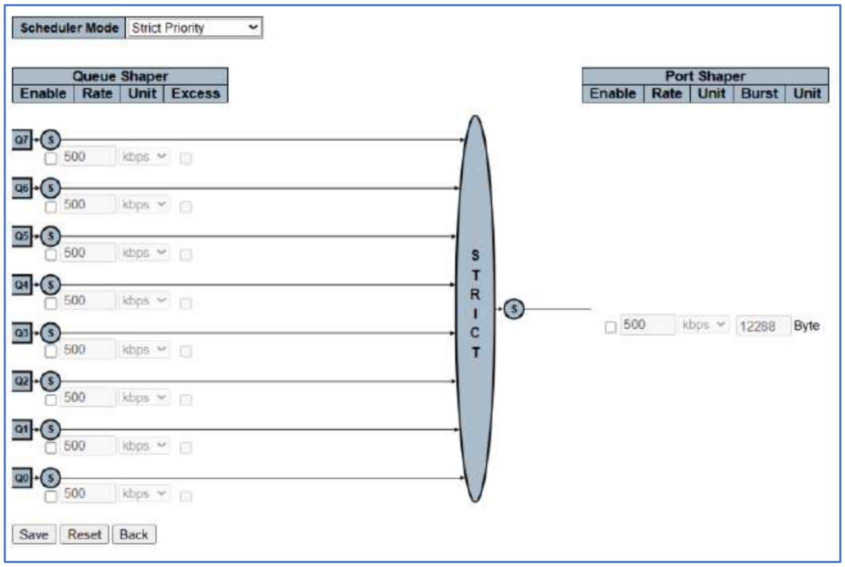
8.5 QoS Egress Port Shapers



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

8.5 QoS Egress Port Shapers

Name	Description
Port	Fixed logical port number – select the port number

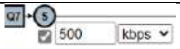


Scheduler Mode: Strict Priority

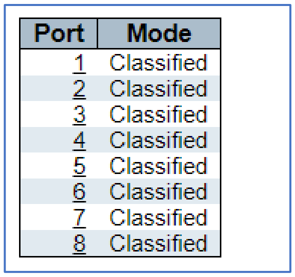
Queue Shaper			
Enable	Rate	Unit	Excess
Q7 ☐	500	kbps	☐
Q6 ☐	500	kbps	☐
Q5 ☐	500	kbps	☐
Q4 ☐	500	kbps	☐
Q3 ☐	500	kbps	☐
Q2 ☐	500	kbps	☐
Q1 ☐	500	kbps	☐
Q0 ☐	500	kbps	☐

Port Shaper				
Enable	Rate	Unit	Burst	Unit
☐	500	kbps	12288	Byte

The above setting follows that of the Port schedular.

Name	Description
Scheduler	Choices are: Strict Priority: Applies to an individual Queue. 6 Queues Weighted: Divides 6 queues which make up DWRR – Deficit Weighted Round Robin and is based on a even division – This is defined by Weight and Percentage
Select the queue	Check the box under the queue  Q7 ☑ 500 kbps
Rate	Input the rate:This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper.
Unit	Indicate Unit as kbps or Mbps
Burst/Unit	Indicates the number of bytes in the selected mode

8.6 QoS Tag Remarking

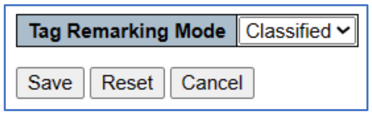


Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified

8.6 QoS Tag Remarking

Name	Description
Port	Logical Port number Click on the port number
Mode	Depending on programming: **Classified**: Use classified PCP/DEI values. **Default**: Use default PCP/DEI values. **Mapped**: Use mapped versions of QoS class and DP level.

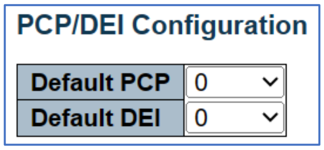
8.7 Port DSCP



Tag Remarking Mode: Classified

Name	Description
Tag Remarking Mode	**Classified**: Use classified PCP/DEI values. **Default**: Use default PCP/DEI values. **Mapped**: Use mapped versions of QoS class and DP level
Select Port	**Select the port to proceed to the next programming screen**

8.8 DSCP- Based Qos



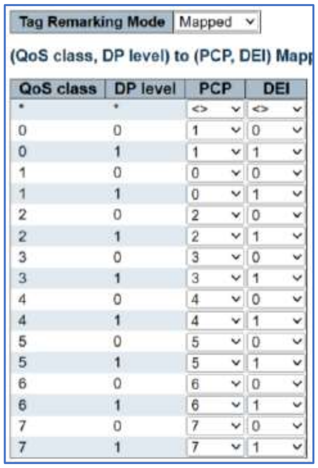
PCP/DEI Configuration

Default PCP	0
Default DEI	0

Name	Description
Default PCP	Program 0-7 for Port Control Protocol to control incoming packets are translated and forwarded
Default DEI	Program 0-7

8.9 DSCP - Translation

The following controls the QoS, DEP levels to PCP, DEI Mapping



Tag Remarking Mode: Mapped

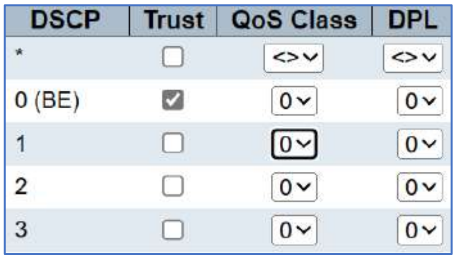
(QoS class, DP level) to (PCP, DEI) Mapp

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

Name	Description
QoS Class	Previously programmed
DP Level	Previously programmed
PCP	Assign new level 0-7
DEI	Assign New level 0-1

8.10 DSCP – Classification

This programs the QoS DSCP based Ingress Classifications

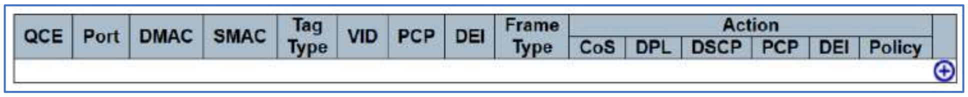


DSCP	Trust	QoS Class	DPL
*	□	<>	<>
0 (BE)	☑	0	0
1	□	0	0
2	□	0	0
3	□	0	0

8.10 QoS DSCP - Classification

Name	Description
DSCP	Sets the DSCP values which are 1-64
Trust	If selected controls if a specific DSCP value is trusted. If selected and trusted the DSCP values will be mapped to the specific QoS class and Drop Precedence Level (DPL). If a frame is untrusted, it will be treated as a non- IP Frame
QoS Class	Can be programmed from a value of 0-7 as previously programmed
DPL	Can be programmed from a value of 0-1 as previously programmed

8.11 QoS Control List Configuration

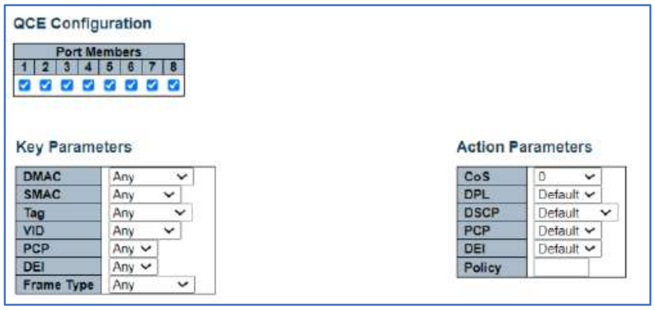


QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action					
									CoS	DPL	DSCP	PCP	DEI	Policy

8.11 QoS Control List Configuration

The Control List Configuration (QCL) consists of QCEs (QoS Control Entry) which is defined by Ethernet Type, VLAN, UDP/TCP port, DSCP, TOS and Tag Priority – all of which are previous defined.

⊕ Selecting the + will open the programming for each item.



QCE Configuration

Port Members							
1	2	3	4	5	6	7	8
☑	☑	☑	☑	☑	☑	☑	☑

Key Parameters

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

Action Parameters

CoS	0
DPL	Default
DSCP	Default
PCP	Default
DEI	Default
Policy	

QCE Configuration

Name	Description
Port Members	Check the box that the following ports. If no ports are checked all ports will be included by default

Key Parameters

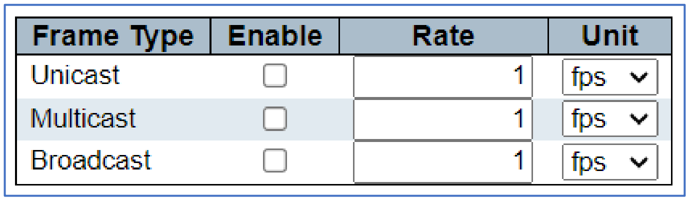
Name	Description
DMAC	Destination MAC Address- the settings are Unicast, Multicast,. Broadcast or Any.
SMAC	Source MAC address- will refer to a specific MAC address or Any
Tag	Value of the programmed Tag in the Tag settings:
VID	Defines the value assign to a specific VLAN ID 1-4095 or Any which will include any programmer VLAN address
PCP	Defines the value of the PCP. Programming can an individual number, programmed as a range of number, or Any
DEI	The Value of 0-1 or Any
Frame Type	This defines the frame type that will be allowed: Known defined types are Any, Ethertype, IPv4, IPv6. Others are; SNAP-this is an EtherType defined in Hex 0x0000xFFFF or Any
LLC	Logical Link Control for internal interfaces between MAC sublayers and network layers. The selections are: **DSAP Address** Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'. **SSAP Address** Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'. **Control** Valid Control field can vary from 0x00 to 0xFF or 'Any'.
SNAP	Is an EherType – Valid PID expressed as 0x0000-0xFFFF or 'Any'.

Action Parameters

Name	Description
CoS	Defines Class of Service as 0-7 or default
DPL	Defines Drop Precedence Level as 0-1 or default
DSCP	Defines DSCP as per a specific setting or Default
PCP	PCP set as 0-7 or Default- Note requires DEI setting
DEI	Set as 0-1 or Default- Note requires PCP setting
Policy	Sets ACL policy as 0-255 if field is left empty it is considering as Default and QCE settings are no longer applied

8.12 Global Storm Policer Configuration

A network storm occurs when more data is transmission that is able to be handled by the switch programming due to continuous multicast or broadcast traffic.



Frame Type	Enable	Rate	Unit
Unicast	☐	1	fps
Multicast	☐	1	fps
Broadcast	☐	1	fps

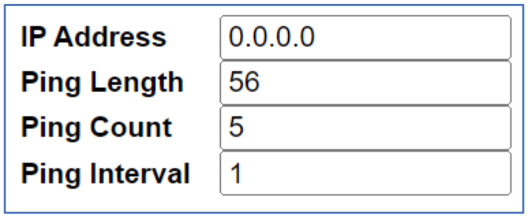
8.12 Global Storm Policer Configuration

Name	Description
Frame Type	Check the frame type. One or all can be checked. Checks are enabled, unchecked disabled
Enable	Rate is dependent on Unit definition; Value is 1-1024000 if Unit is set to fps and 1-1024 when set to kfps
Rate	See Enable for settings
Units	Defines the type in fps or kfps

Chapter 9: Diagnostics

9.1 ICMP Ping

ICMP is for Internet Control, Message Protocol and is used to test Internet connections.

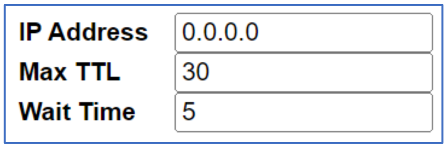


IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

9.1 ICMP Ping

Name	Description
IP Address	Input the IP address of the device you want to ping making certain it on the same network
Length	This is the packet size. Valid entry is 2 to 1452 bytes which are non-Jumbo frames
Ping Count	The number of times the ping is issued
Ping Interval	The duration in seconds between pings
Valid Display	A valid return will show the following information. PING server 192.168.0.150, 56 bytes of data. 64 bytes from 192.168.0.150: icmp_seq=0, time=160ms 64 bytes from 192.168.0.150: icmp_seq=1, time=0ms 64 bytes from 192.168.0.150: icmp_seq=2, time=0ms 64 bytes from 192.168.0.150: icmp_seq=3, time=0ms 64 bytes from 192.168.0.150: icmp_seq=4, time=0ms Sent 5 packets, received 5 OK, 0 bad Note the number of packets sent as per the programmed number, the number Ok and the number Bad

9.2 Traceroute



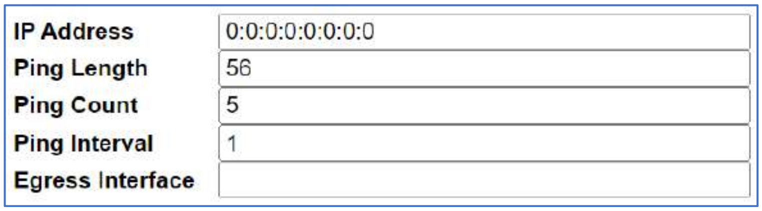
IP Address	0.0.0.0
Max TTL	30
Wait Time	5

9.2 Traceroute

Name	Description
IP Address	Input the connected device IP address. Make certain it is on the same network
Max TTL	Time to Life limits the duration data is transmitted to the defined IP address- once the time is exceeded the data is dropped indication the duration the data was valid
Wait Time	The time in seconds to determine the transmission
Valid Display	The following display shows the destination address, the number of hops (the number of devices the data will pass through between the source and destination- will not equal the physical device number). The first hop is zero. The higher the number the more time the trip takes. Traceroute to 192.168.0.150 (192.168.0.150), 30 hops max, 56 byte packets 1 192.168.0.150 106.103 ms 90.003 ms 11.589 ms Traceroute complete

9.3 ICMPv6 Ping

IPv6 is a different series of IP address and not compatible with IPv4. IPv6 contains more information than IPv4.

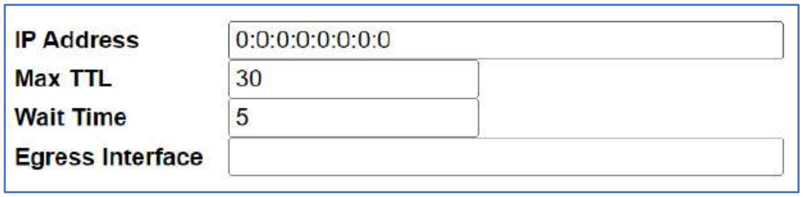


IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1
Egress Interface	

9.3 ICMPv6 Ping

Name	Description
IP Address	Destination IP address of the connected device
Ping Length	The packet size from 2 to 1452
Ping Count	The number ping generated
Ping Interval	Duration between pings
Egress Interface	This indicates the VLAN ID for the egress that transmits the ICMP. The valid range is 1- 4094 (the number of VLANs) If not programmed the function will determine the best match however for a local link or multicast the address should be included.
Valid display	PING6 server ff02::2, 56 bytes of data. 64 bytes from fe80::219:5bff: fe2f:b47: icmp_seq=0, time=10ms Sent 1 packets, received 11 OK, 0 bad

9.4 Traceroute6



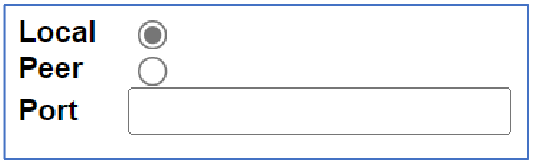
IP Address	0:0:0:0:0:0:0:0
Max TTL	30
Wait Time	5
Egress Interface	

9.4 Traceroute6

Name	Description
IP Address	The destination IP address
Max TTL	The number of hops noting the time and number of devices the data passed through. This will not be equal to the physical device's connections
Wait Time	The number of seconds to wait for a response time 1-30 seconds
Egress	The VLAN ID of the egress of IPv6 packets – this applies to only to the given VID (VLAN) ranges 1-4094)

9.5 Link OAM MIB Retrieval

OAM stands for Operation, Administration, Maintenance which is used to retrieve and provide ethernet services assessment. It is data injected into the packets. It can detect various failures such as packet loss, packet delays along a path. Note the required MIB must be present in order to be read and that they are read only contained in the connected device through the port assigned.



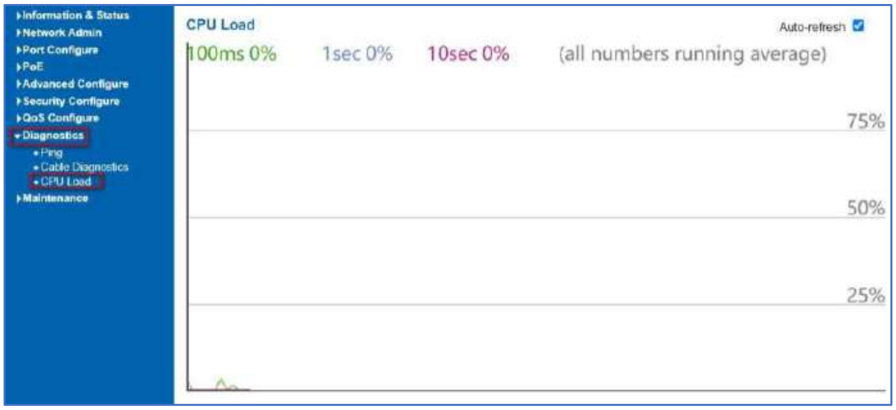
Local	●
Peer	○
Port	

9.5 Link OAM MIB Retrieval

Name	Description
Local	Used for a local connection
Peer	Use for multiple connections with the same port and MIB
Port	Assign the port data is transmitted on

9.6 CPU Load

This is display of the CPU load with set time durations showing how the load changes with time.



9.6 CPU Load

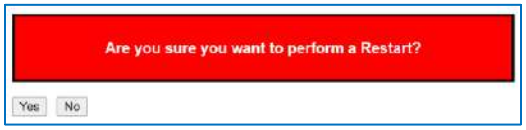
This page displays the CPU load, using an SVG graph. The load is measured as average over the last 100ms, 1 sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support.
Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

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

Chapter 10: Maintenance

10.1 Restart Device

This is display of the CPU load with set time durations showing how the load changes with time.

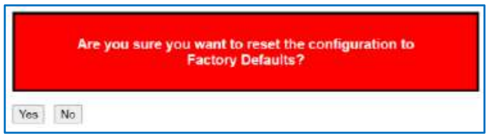


Are you sure you want to perform a Restart?

10.1 Restart Device

Name	Description
Are you sure you want to perform a Restart	
Yes	Switch will restart
No	No action will be taken

10.2 Factory Defaults

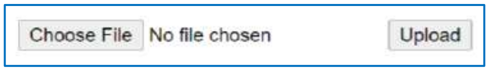


Are you sure you want to reset the configuration to Factory Defaults?

10.2 Factory Defaults

Name	Description
Are you sure you want to reset the configuration to factory defaults	
Yes	Switch reset to factory defaults and all previous programming will be deleted
No	No action will be taken

10.3 Software Upload

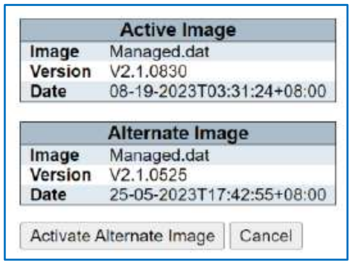


No file chosen

10.3 Software Upload

Name	Description
Choose File	Select and a Window™ based file view will appear. Select the replacement software.
Upload	After the software is selected- select Upload and wait for the process to be completed

10.4 Firmware Select



Active Image	
Image	Managed.dat
Version	V2.1.0830
Date	08-19-2023T03:31:24+08:00

Alternate Image	
Image	Managed.dat
Version	V2.1.0525
Date	25-05-2023T17:42:55+08:00

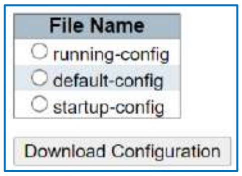
10.4 Firmware Select

Name	Description
Active Image	The current active firmware
Alternative Image	This is a previous version. As new firmware is loaded the previous version is shown as the alternative image
Activate Alternative Image	When selected you will be asked to confirm the decision and if so the Active image will become the Alternative image and the Alternative image will become active

10.5 Configuration

This section programs several firmware processes

10.5.1 Download Configuration



10.5.1 Download Configuration

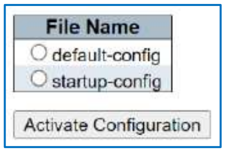
Name	Description
File name	Select the file to download
Running config	The existing firmware containing all programing that is currently running
Default Config	This is read only file containing the default settings
Startup config	This saves the current programming for use as the active programming if the switch is rebooted: IMPORTANT- you must use this feature so in the event of any power loss the changes you made to programming will be reloaded. If not, the switch will return to the default settings
Download Configuration	The selected configuration will be download and can be saved to a host computer

10.5.2 Upload configuration

Name	Description
Choose File	Select this to display the Windows™ file and select a file to be uploaded
Running config	Once upload this will become the current running program – switch programming will be change to this file
Running – config- Replace	When select the uploaded file will replace the running file
Running – config- Merge	This action will merge the uploaded file with the existing file- be careful when using this file upload that it only contains new features and not existing ones that will result in conflicts
Startup- config	This action will replace the startup configuration
Create new file	Enter a new file name followed by selecting an existing file when upload file is selected it will change the file name
Upload Configuration	Initiates the selected action

10.5.2 Upload configuration

10.5.3 Activate Configuration



10.5.3 Activate Configuration

Name	Description
Default- config	Default setting will become the active setting
Startup – config	The startup config will become the active setting- but will not be saved as the automatic start up
Active Configuration	Select to affect the setting

10.5.4 Delete Configuration (Startup) file.

Name	Description
Startup – config	Select this to delete the startup configuration – when active the switch will reset to the default settings
Delete Configuration File	Active settings

10.5.4 Delete Configuration (Startup) file.

10.5.5 Appendix 5 Glossary

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

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

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

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

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

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

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

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

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

CDP
CDP is an acronym for Cisco Discovery Protocol.

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

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

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

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

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

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

DoS
DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

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

EEE

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

EPS

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

Ethernet Type

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

FTP

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

Fast Leave

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

HTTP

HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW). HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested.

WEB

Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

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

HTTPS

HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection. HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logins. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is no longer considered an adequate degree of encryption for commercial exchange.

ICMP

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

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection, or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

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

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier. There will be only one IGMP Querier that wins Querier election on a particular link.

IMAP

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

IP

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

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

IPMC

IPMC is an acronym for IP MultiCast. IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IPMC Profile

IPMC Profile is an acronym for IP MultiCast Profile. IPMC Profile is used to deploy the access control on IP multicast streams.

IP Source Guard

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

LACP

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

LLC

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

LLDP

LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

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

LLQI

LLQI (Last Listener Query Interval) is the maximum response time used to calculate the Maximum Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC

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

MAC Table

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

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC

addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

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

MD5

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

Mirroring

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

MLD

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

MLD Querier

A router sends MLD Query messages onto a particular link. This router is called the Querier. There will be only one MLD Querier that wins Querier election on a particular link.

MSTP

In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

NAS

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

NetBIOS

NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

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

OAM

OAM is an acronym for Operation Administration and Maintenance.

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

Optional TLVs.

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

OUI

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

PCP

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

PD

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

PHY

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

PING

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

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

PoE

PoE is an acronym for Power Over Ethernet. Power over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN Access Points (AP), IP cameras and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

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

POP3

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

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

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

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

PPPoE

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

Private VLAN

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

PTP

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

QCE

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

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

QCI

QCI is an acronym for QoS Class Identifier. This is a special identifier defining the quality of packet communication provided by LTE (Long Term Evolution, marketed as 4G LTE).

QCL

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

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

QL

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

QoS

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

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

Achieving the required QoS becomes the secret to a successful end-to-end business solution.

Therefore, QoS is the set of techniques to manage network resources.

QoS class

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

Querier Election

Querier election is used to dedicate the Querier, the only one router sends Query messages, on a particular link. Querier election rule defines that IGMP Querier or MLD Querier with the lowest IPv4/IPv6 address wins the election.

RARP

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

RADIUS

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

RDI

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

Router Port

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

RSTP

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

SAMBA

Samba is a program running under UNIX-like operating systems (not the Brazilian dance) that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking. Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

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

sFlow

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

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

SHA

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

Shaper

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

SMTP

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

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

SNMP

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

SNTP

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

SPROUT

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

SSID

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

SSH

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

SSM

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

STP

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

Switch ID

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

SyncE

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

TACACS+

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

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame. The 3-bits provide 8 priority levels (0~7).

TCP

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

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

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

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

TELNET

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

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

TFTP

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

ToS

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

TLV

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

TKIP

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

UDP

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

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

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.
Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.
User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

VLAN

Virtual LAN.A method to restrict communication between switch ports. VLANs can be used for the following applications:
VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.
VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.
Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

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

Voice VLAN

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

WEP

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

WiFi

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

WPA

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

WPA-PSK

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

WPA-Radius

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

WPS

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

WRED

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

WTR

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