MaxiiNet™ Vi30130
Operation and Installation Manual

20 + 4+2 1G Port Series 802.3bt PoE+ L2/Le Lite Plus Industrial Managed Switch

Firmware Version: (V2.1.0106)
Revision Date: ( )

About this Manual

Copyright

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.

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.

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

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.

EMC - Compliance

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

FCC – Class

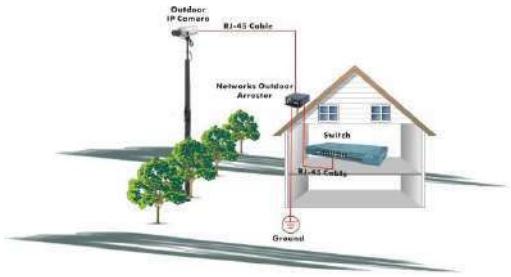
CE Mark Declaration of Conformance for EMI and Safety (EEC)

EMC - Compliance

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 Vi30130 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 Vi30130 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 of 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

The switch contains 20/10 1000BASE-T RJ-45 ports, 41G 100Mbps/1G combo ports and 2 100Mbps 1G/1G fiber 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.

Vi30130 supports the Small Form Factor Pluggable (SFP) transceiver slots. The SFP transceiver slots are with RJ-45 port 25 to 28. In the default configuration, if an SFP transceiver (purchased separately) is installed in a slot and has a valid link on the port. While all UTP ports provide PoE ports 21-24 are combo with Fiber either but not both can be used.

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

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

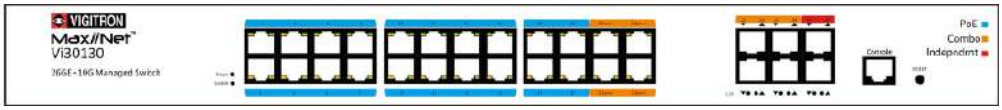
for fiber optic cabling, see “1000 Mbps Gigabit Ethernet Collision Domain”.

Supported SFP Transceivers

NOTE: Maximum distance may vary for different SFP vendors.

NOTE: The Vi01000CH copper SFP will not interface with the Vi30130.

Front Panel LED and Port Status



----------Standard UTP Ports----------Combo-UTP Combo Fiber Independent Fiber

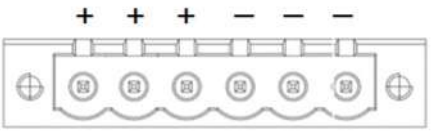
Note on LEDs

The Vi30130 has two alarm LEDs. Power and System. These LEDs are activity using the Configuration>System> System Log Configuration. When active the System LED will be steady even if not connection is present. When properly powered the Power and System LED will exhibit a steady on condition

1. Press the Reset button and hold for approximately 7 seconds
2. Hold until the Front panel LED flash
3. Release the button
4. Access the GUI using the default GUI setting

Rear Panel Operation

Connecting extender Power



Conenction Option:
2wires(+/-)≈400watts
4wires(2+/2-)≈800watts
6wires(3+/3-)≈1000watts

The rear panel has three separate DC inputs. The maximum for each input is 1000W watts.

The Vi30130 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.

Power indicator: PWR (Green)
Network indicator: 1-24(Link/Act)/ (Orange),25-28(Link/Act)/ (Green)
POE indicator: Pot (Green)
SYS: (Green)

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 Vi30130 has auto MDIX and 4 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:

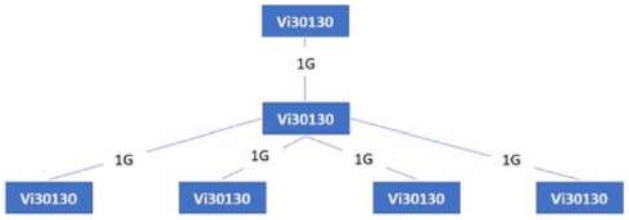
- Remote site application is used in enterprise or SMB.
- Peer-to-peer application is used in two remote offices.
- Office network.
- High-performance requirement environment.
- Advance security for network safety application.
- Suitable for data/voice and video conference applications.

NOTE: Fiber ports are labeled as Ports 21 to 24 and are combo ports with ports 25 and 26 are fiber ports only.

Application Examples

Network Connection between Remote Site and Central Site
This will be replaced with actual product images.

Single Headed Configuration ID-MDF



Installing the Switch

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 0°C to 40C (32°F to 104°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.

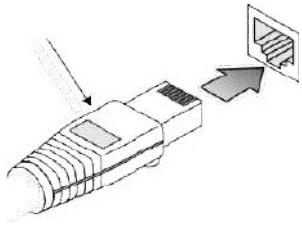
Make sure the twisted-pair Ethernet cable is always routed away from power lines, radios, transmitters, or any other electrical interference.
Make sure that Vi30130 is connected to a separate grounded power supply that provides 100 to 240 VAC, 50 to 60 Hz.
Make sure the power supply you are using provides 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.

RJ-45 Connections



SFP Transceiver

Equipment Checklist

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.

- Vi30130 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.

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.

SFP Transceiver

Inserting an SFP Transceiver into a Slot

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

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

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.

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.

To Install an SFP Transceiver, Do the Following:

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

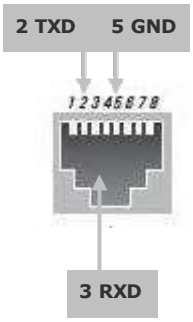
Step2: Insert the transceiver with the optical connector facing outward and the slot connector facing down. Note that SFP transceivers are keyed so they can only be installed in one orientation.

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

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

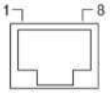
Connecting to the Console Port

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.



RJ-45pin Assignment

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

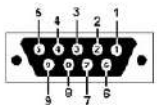


Pin	Ref	Definition	Direction
3	RxD	Receive Data	Out towards DTE
6	TxD	Transmit Data	In from DTE
5	SG	Signal Ground	na

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

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	Out the device towards DTE
3	6	TxD	Transmit Data	In the device from DTE
5	5	SG	Signal Ground	na

Plug in the Console Port

Serial Cable Wiring: Note no other connections are required.

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

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.

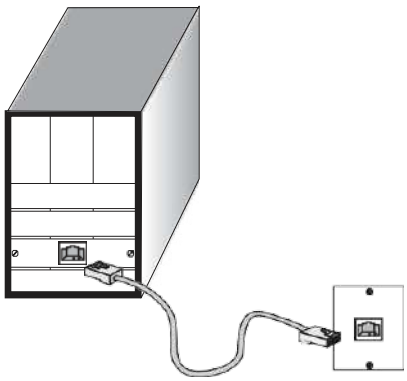
Each device requires an unshielded twisted-pair (UTP) cable with RJ-45 connectors at both ends. Use Category or c 5e, or 6 cables for 1000BASE-T connections, and Category 5 or better for 100BASE-TX connections.

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 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.

1000 Mbps Gigabit 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

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)		LC
		50km (31.06 miles)		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	

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 them 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 Vi30130 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 communication between the switch and the device.
- Make sure all devices connected to the Vi30130 are configured to auto-negotiate or are configured to connect at half-duplex (e.g. all hubs are configured this way).
- Faulty or loose 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 miss 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	• Check connections between the switch, the power cord, and the wall outlet. • Contact your dealer for assistance.
Link LED is Off	• Verify that the switch and attached device are powered on. • Be sure the cable is plugged into the switch and corresponding device. • If the switch is installed in a rack, check the • connections to the punch-down block and the patch panel. • Verify that the proper cable type is used and its length does not exceed specified limits. • Check the adapter on the attached device and cable 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 Vi30130'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).

Installation

The Vi30130 can operator under high temperature ranging from 0C to 40C. 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 Vi30130 does provide operation settings which monitor the switches internal temperature and will affect individual port shut downs 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.

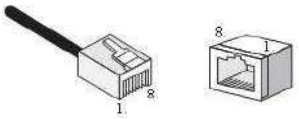


Figure 19: RJ-45 Connector Pin Numbers

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 Catgory 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.

Physical Characteristics

	Ports	2 1000/1000 SFP Fiber ports
	Network Interface	Ports 1-20: 100/1000Mbps ports RJ-45 Connector Ports 21-24 100/1000Mbps combo ports 10BASE-T: RJ-45 (100-ohm, UTP cable; Category 3 or better) 100BASE-TX: RJ-45 (100-ohm, UTP cable; Category 5 or better) *Maximum Cable Length - 100 m (328 ft) Ports 1-20: RJ-45 connector/ (100/1000M) UTP Ports 21-24 Combo UTP/Fiber ports (100/1000M Ports 25-26 – fiber connections (100/1000Mbps)
	Buffer Architecture	32M on-chip frame buffer
	Aggregate Bandwidth	52 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	8.4 lbs. 3.8kg
	Size	1.73’ X 17.4” X8.3” (44mm X 442mm X 221mm) (H x W x L)
	Temperature	Operating: 0°C to 40°C (32°F to 104°F)
	Humidity	Operating: 5% to 90% (non-condensing)
	External Power Input	Not to exceed 400 watts @ 57VDC per input 1000W total.
	Power Supply Mains	120/240VAC 50/60hz
	Power Consumption	8W maximum standby, 804W full load
Switch Features		
	Forwarding Mode	Store-and-forward
	Switching Capacity	52Gbps
	Throughput	38.688Mpps
	Flow Control	Full-Duplex: IEEE 802.3x Half-Duplex: Back pressure
Management		
	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) 802.3at/af /bt=> Power Over Ethernet (PoE)
Emissions		EN55022 (CISPR 22) Class A EN 61000-3 FCC Class A CE Mark
Immunity		EN 61000-4-2/3/4/5/6/8/11 EN 55024

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/bt	Defines Power Over Ethernet is used to transmit electrical power, PoE IEEE 802.3af (Class 4 PDs limited to 30W), 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

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

The house Icon returns the GUI to the home page which shows a graphical display of the Vi30130 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

- *Port Status LEDs*
  - Indicates the current status of each port. Users can check these LEDs to understand the port status in different modes, after changing the mode by pressing Mode button.

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

LED	Color	State	Descriptio n
System	Green	ON- Steady	The system is started and working normally
		OFF	The system is not working.

System LED

LED	Color	State	Description
Power	Green	ON	The power is working.
		OFF	The power is not working.

POWER LEDs

LED	Color	State	Description
POE	Green	ON	The PoE Port Status is ON and working
		OFF	The PoE Port is not working.
10/100/1000M Link/Act	Yellow	Blink	The Port Status LEDs are displaying link status, network activity.
		ON	The Port Status LEDs are link status, no data transmission
		OFF	The Port Status LEDs are link status, No Link
Blink	The Port Status LEDs are displaying link status, network activity.		
ON	The Port Status LEDs are link status, no data transmission		
OFF	The Port Status LEDs are link status, No Link		

1.1.1 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 Vi30130. The subnet mask is "255.255.255.0".

Open the WEB browser, enter the "192.168.0.1" in the address bar, note that "192.168.0.1" 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 username is "admin" and the password is "admin". Please distinguish the capital and small letter.

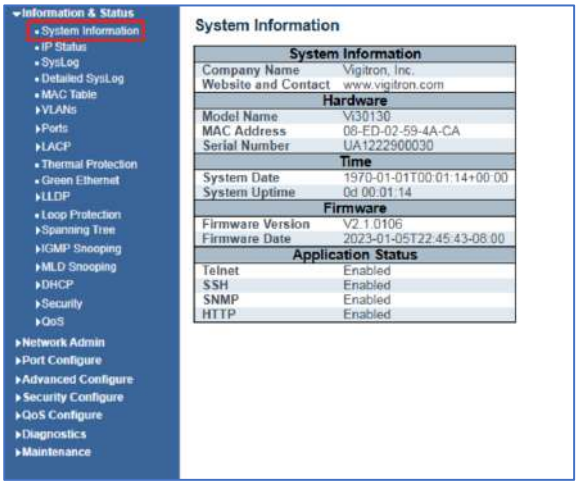
Picture 1: WEB Authentication Dialog.

Reset key – default function:

1. Remove power.
2. Reconnect the power.
3. Within 10 seconds press and hold the reset button on the front panel
4. The LED front panel lights will flash 4 times and the switch default settings will be restored.

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.



System Information Page of Switch

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

This Is the Home button. Click it, the management page will return back the original one.

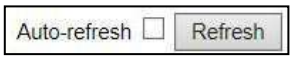
This's Logout button. After clicking "Confirm", you need to retype the account and passwords if WEB function is used again.

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.

1.1.2 Guide

1.1.3 Top Control

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



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.

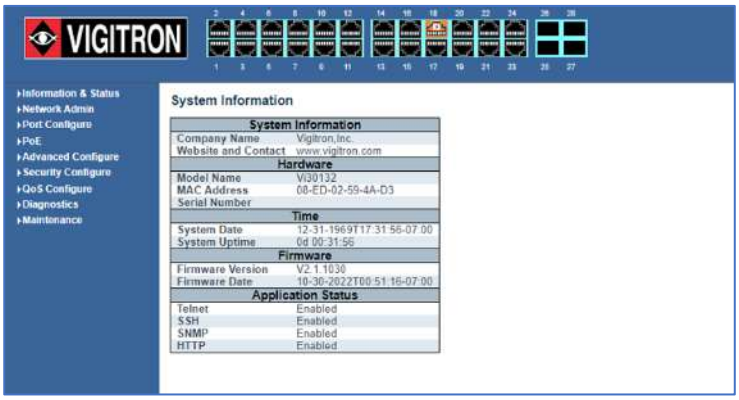
1.1.4 Web management Login

Open installed web browser on your PC, input the switch’s IP address link.
http://192.168.0.1, then open that URL to login web management.

Note: IP address of switch is 192.168.0.1 by default. So please input
http://192.168.0.1 in browser.
When the login window appears, please enter the default username and password then click OK to login.

Login Window- different browser will have different images

Default Username: admin
Default Password: admin



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.

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

1.1.5 Main Menu

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:

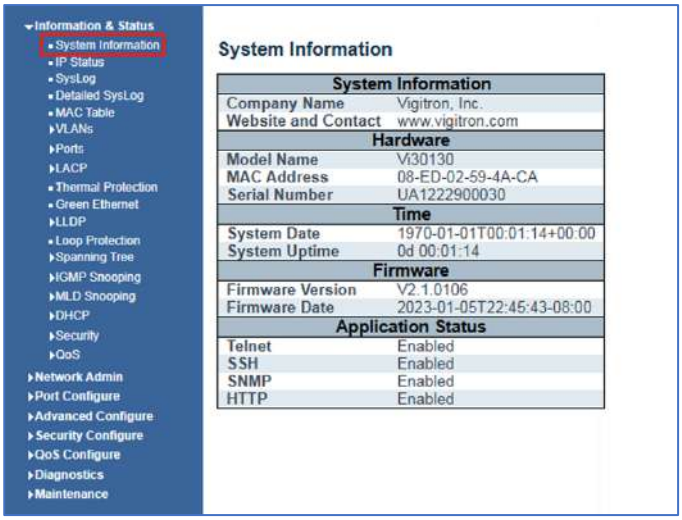
Information & status - Users can check switch information and working status under this menu.
Network Admin - Users can check and configure related features of network under this menu.
Port Configure - Users can check and configure specification of ports under this menu.
PoE - Users can check and configure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

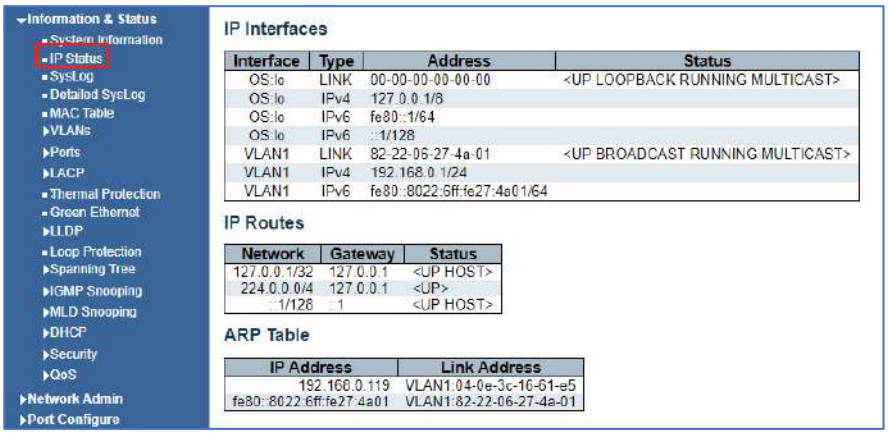
After click "Information & Status" > "System Information", followed screen will appear as:



System Information Screen

2.2 IP Status

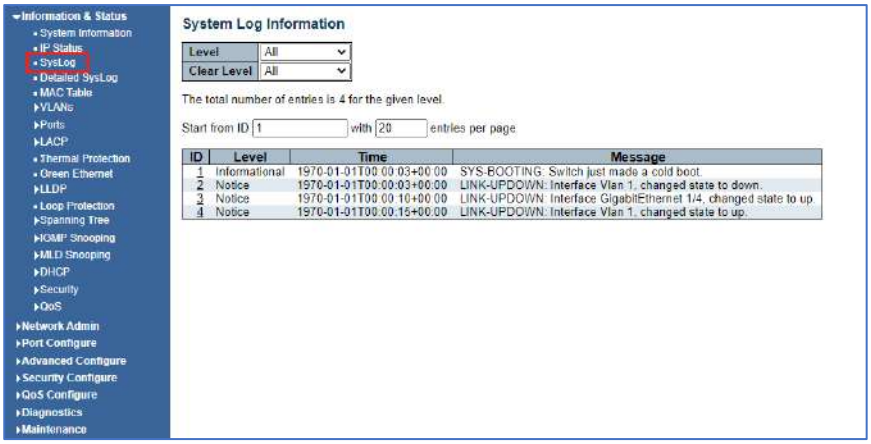
After click "Information & Status" > "IP Status", followed screen will appear as:
Clients can go to Section “Network Admin” > "IP Configuration" to do the detailed management.



System Information Screen

2.3 Syslog

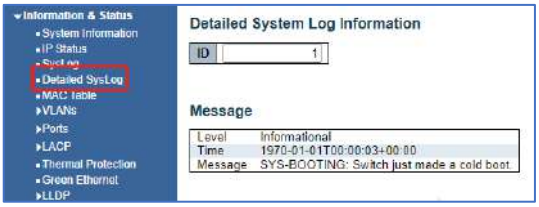
After click "Information & Status" > "System Information", followed screen will appear as:
Clients can go to Section “Network Admin” > "System Log Configuration" to do the detailed management.



Syslog Screen

2.4 Detailed Syslog

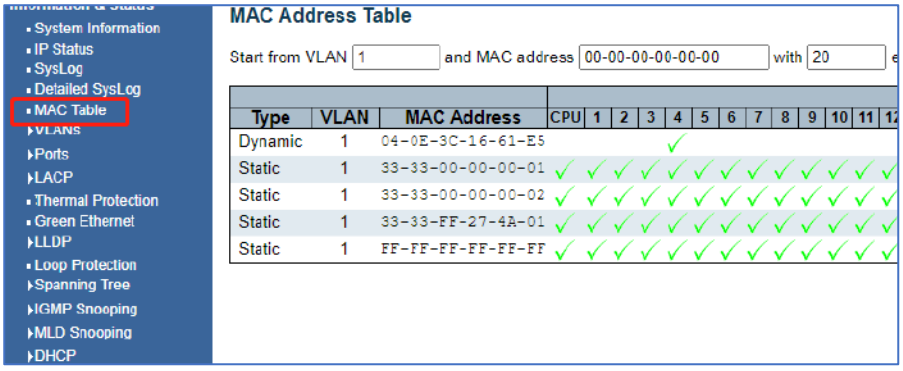
After click "Information & Status" > "Detailed Syslog", followed screen will appear as:
Clients can go to Section” Network Admin” > "System Log Configuration" to do the detailed management.



Detailed Syslog Screen

2.5 Mac Table

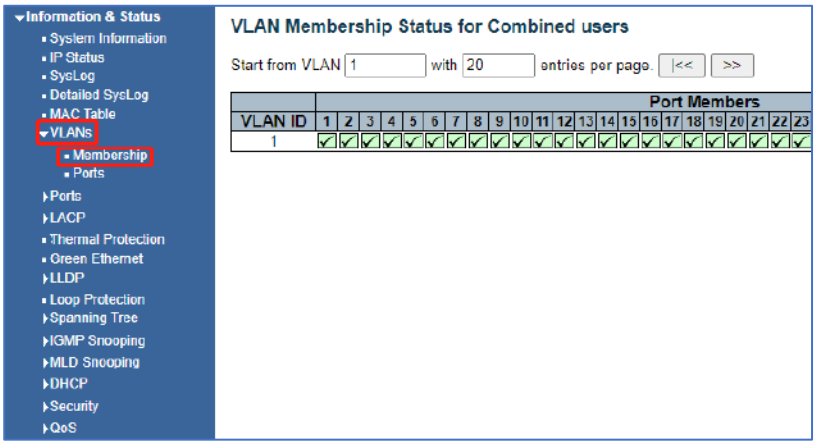
After click "Information & Status" > "Mac Table", followed screen will appear as:
Clients can go to Section “Advanced Configure” > "MAC Address Table" to do the detailed management.



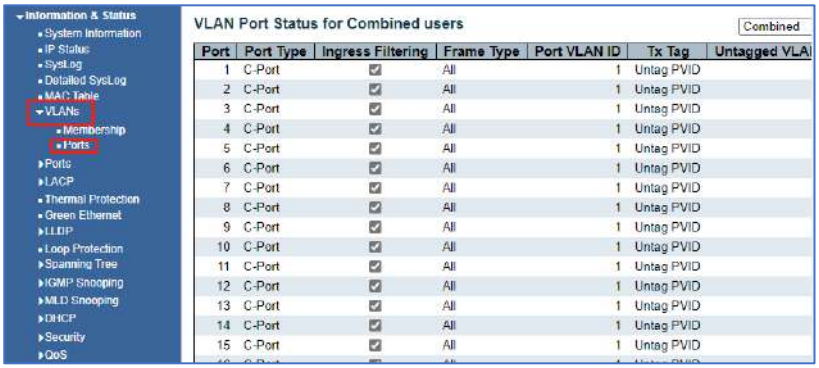
Mac Table Screen

2.6 VLANs

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



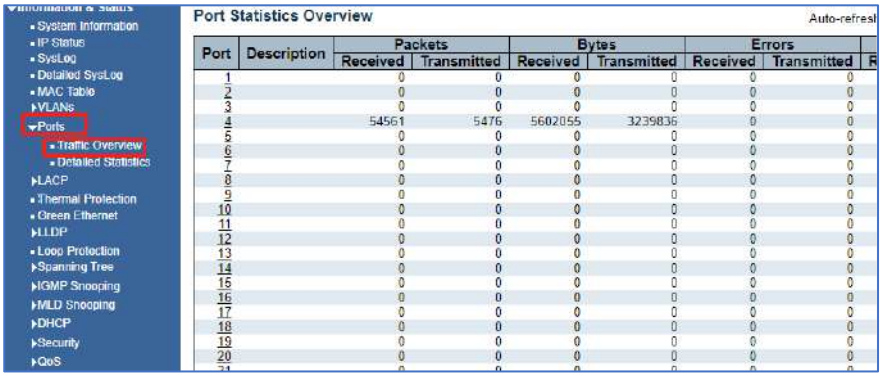
Membership Screen



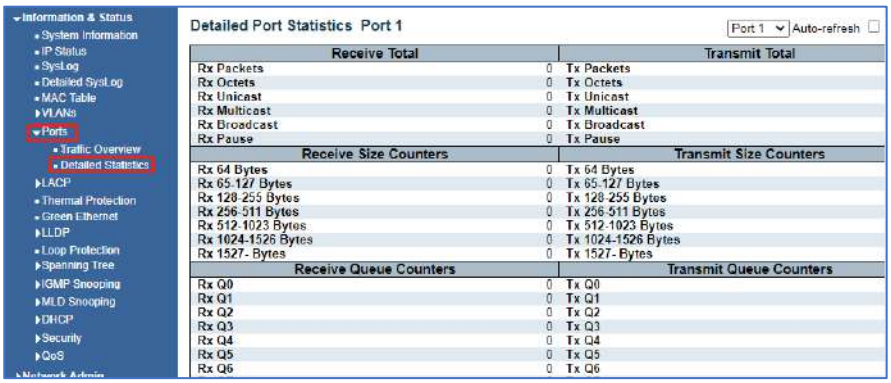
Ports Screen

2.7 Ports

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



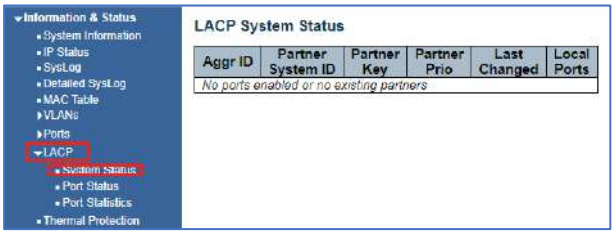
Ports-Traffic Overview Screen



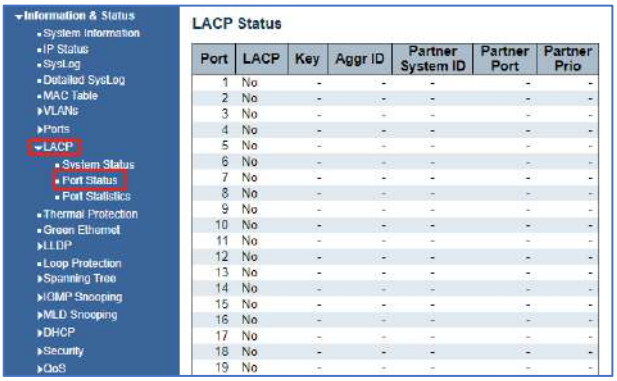
Ports-Detailed Statistics Screen

2.8 LACP

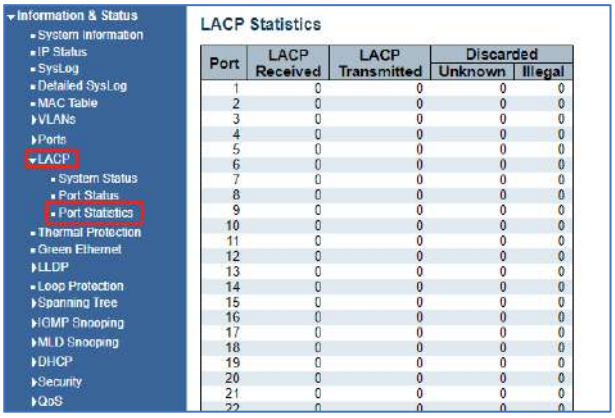
After click "Information & Status" > "LACP", followed screen will appear as:
Clients can go to section “Port Configure” > "Link Aggregation" > "LACP Aggregation" to do the detailed management.



LACP System Status Screen



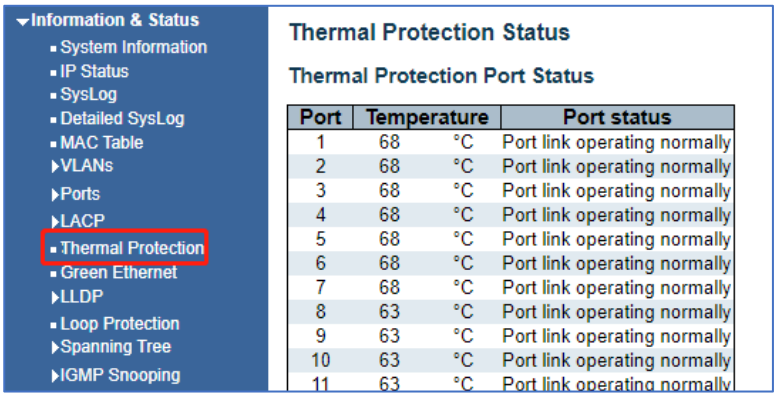
LACP Port Status Screen



LACP Port Statistics Screen

2.9 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.



Thermal Protection Screen

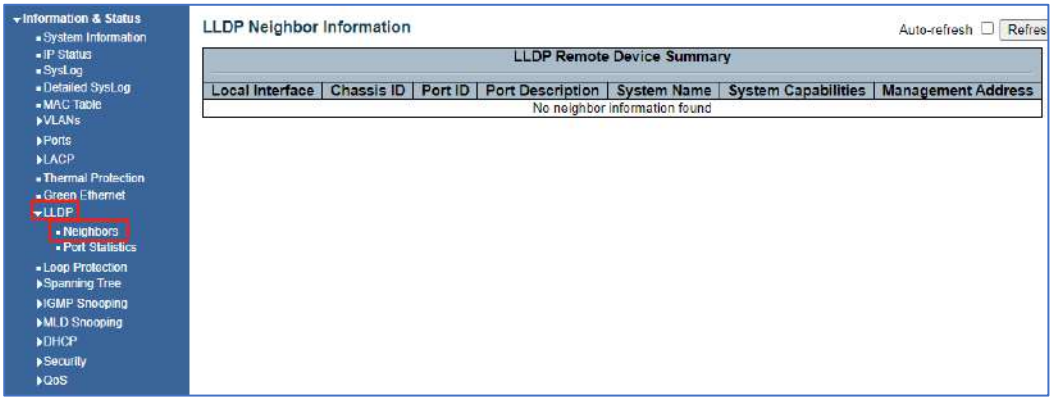
2.10 Green Ethernet

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.

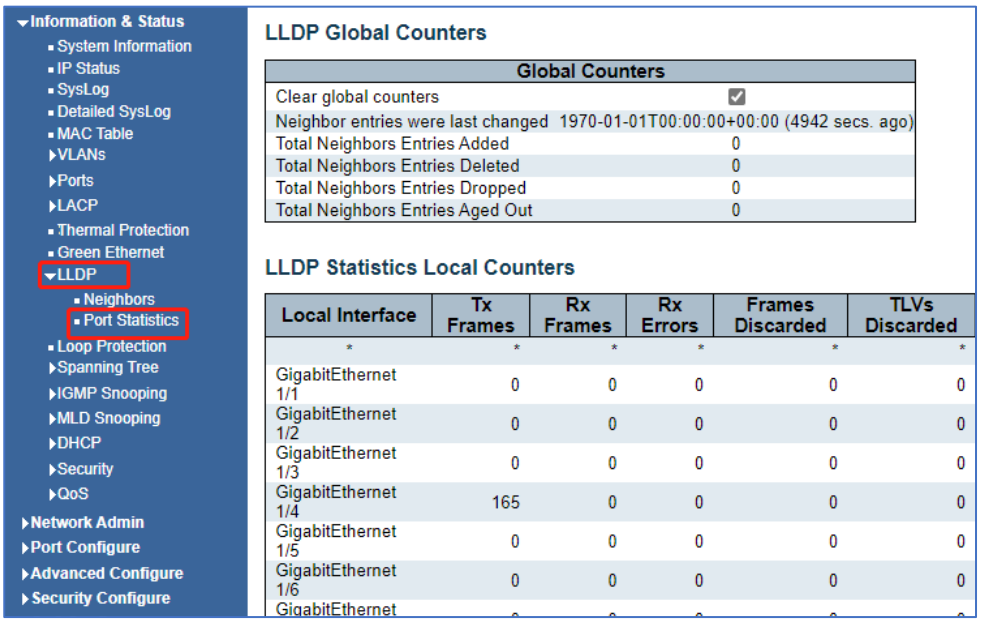
Green Ethernet Screen

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.



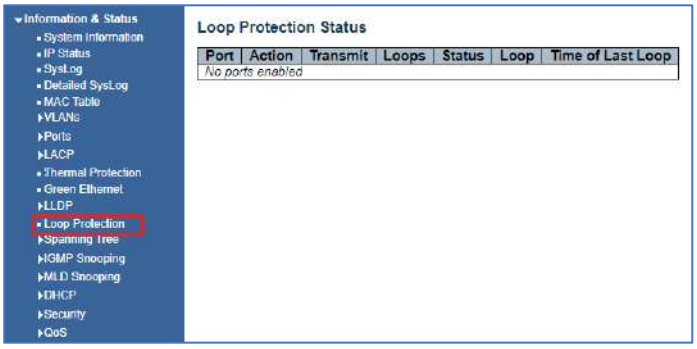
LLDP-Neighbors Screen



LLDP-Ports Statistics Screen

2.12 Loop Protection

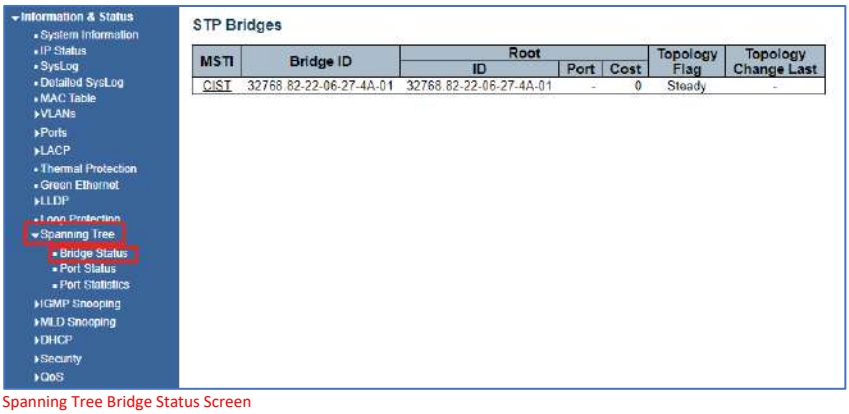
After click "Information & Status" > "Loop Protection", followed screen will appear as:
Clients can go to Section “Advanced Configure” > "Loop Protection” to do the detailed management.



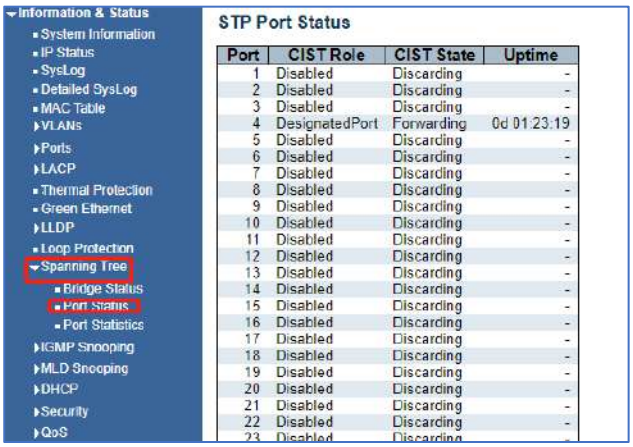
Loop Protection Screen

2.13 Spanning Tree

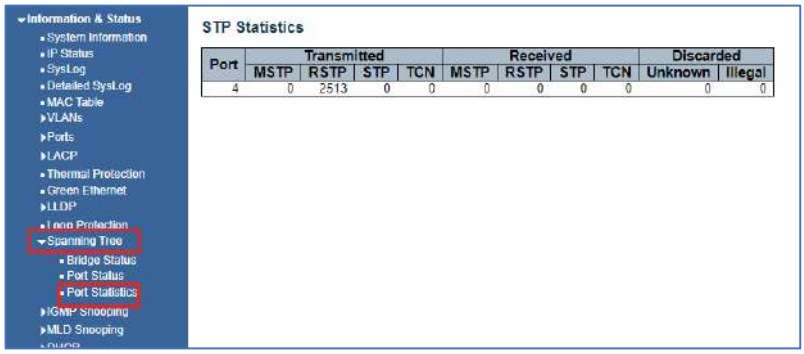
After click "Information & Status" > "Loop Protection", followed screen will appear as:
Clients can go to Section “Advanced Configure” > "STP” to do the detailed management.



Spanning Tree Bridge Status Screen



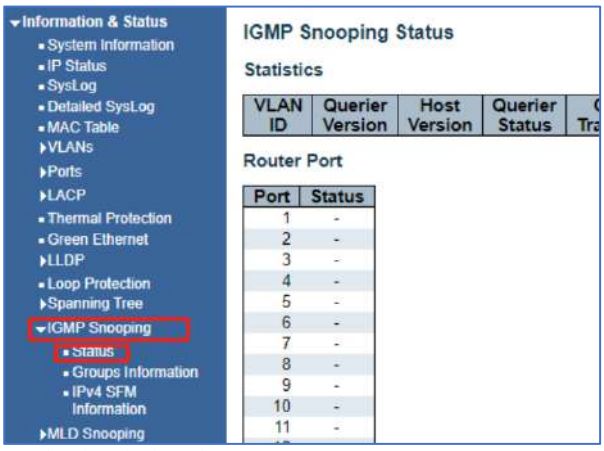
Spanning Tree Port Status Screen



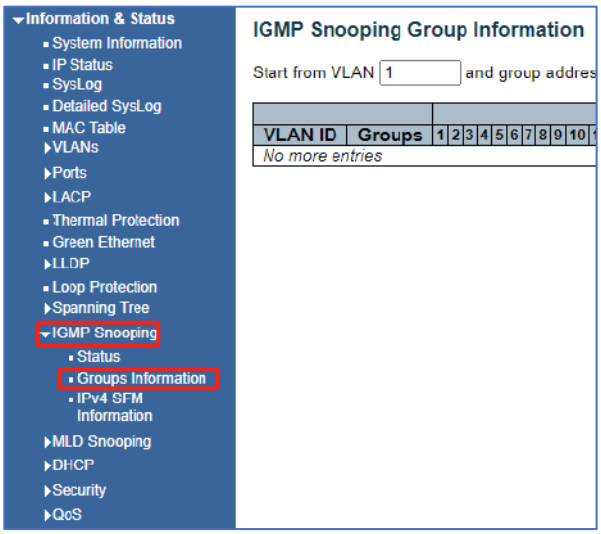
Spanning Tree Port Statistics Screen

2.14 IGMP Snooping

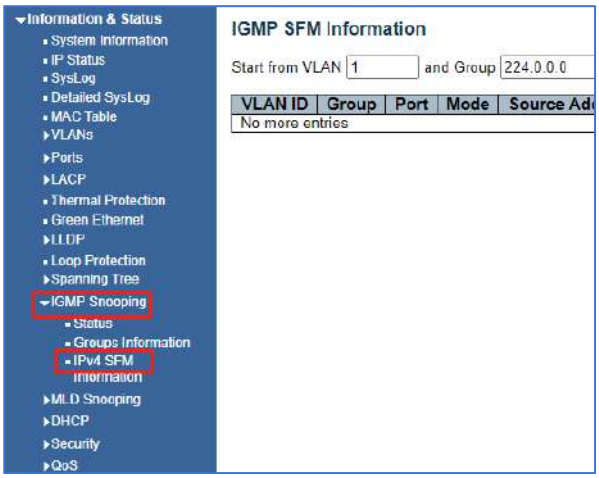
After click "Information & Status" > "IGMP Snooping", followed screen will appear as:
Clients can go to Section “Advanced Configure” > "IGMP Snooping” to do the detailed management.



14-1 IGMP Snooping Status Screen



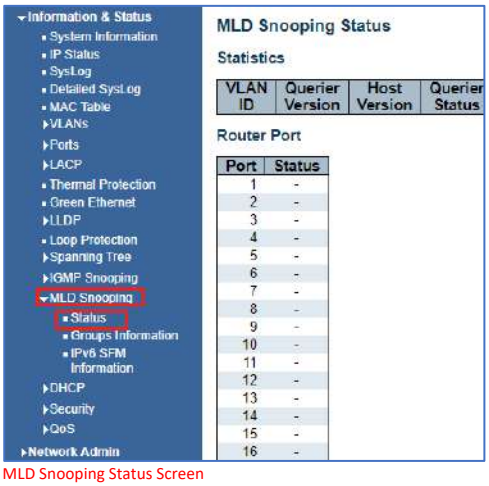
IGMP Snooping Group Information Screen



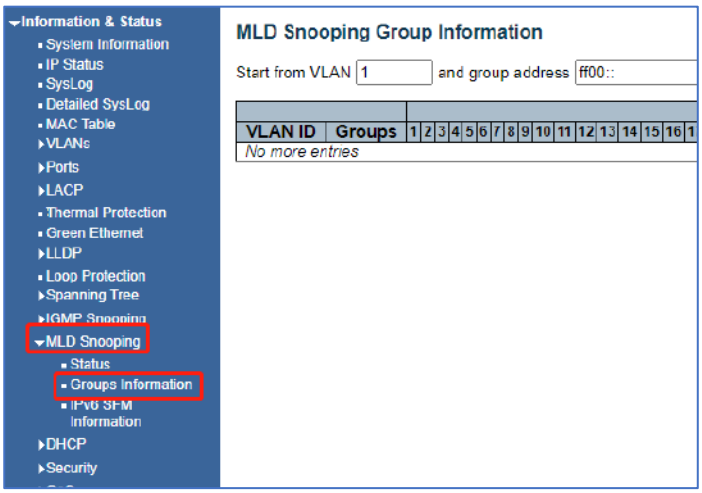
IGMP Snooping IPv4 SFM Information Screen

2.15 MLD Snooping

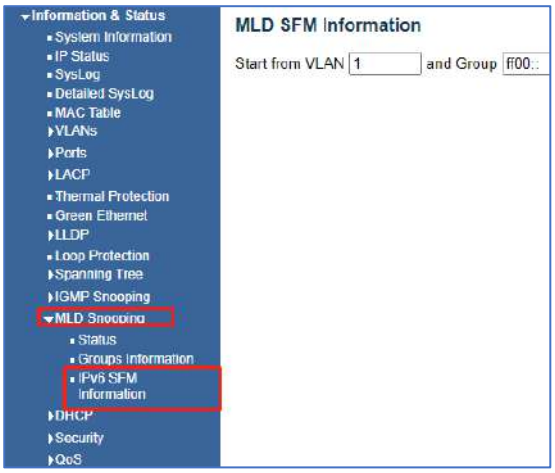
After click "Information & Status" > "MLD Snooping", followed screen will appear as:
Clients can go to Section “Advanced Configure” > "IPV6 MLD Snooping” to do the detailed management.



MLD Snooping Status Screen



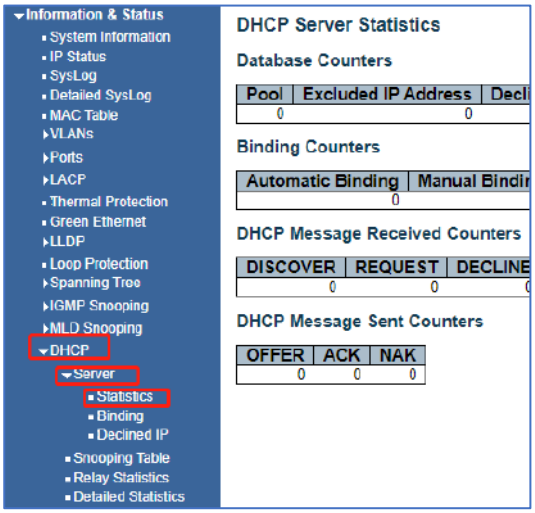
MLD Snooping Groups Information Screen



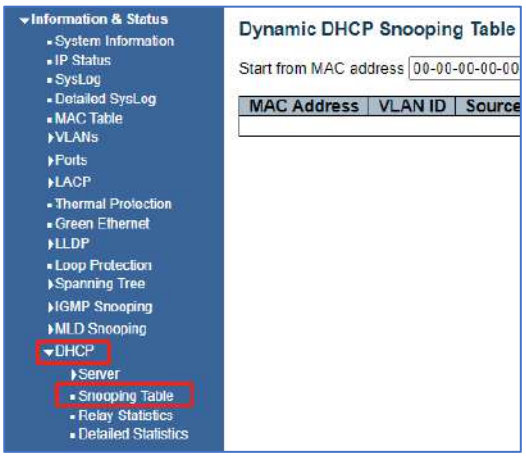
MLD Snooping IPv6 SFM Information Screen

2.16 DHCP

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



DHCP Server Statistics Screen



DHCP Server Binding Screen

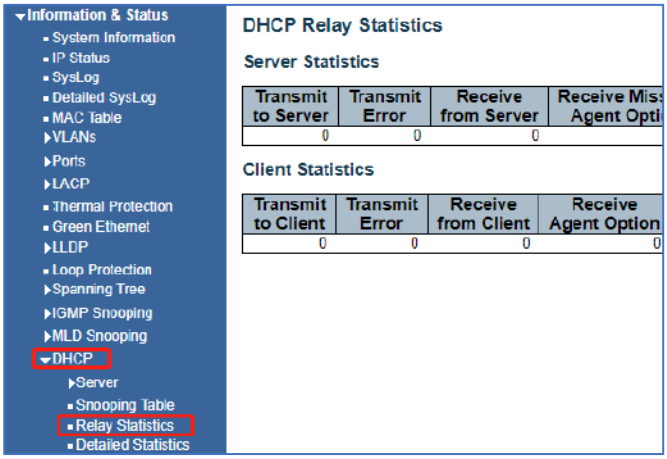
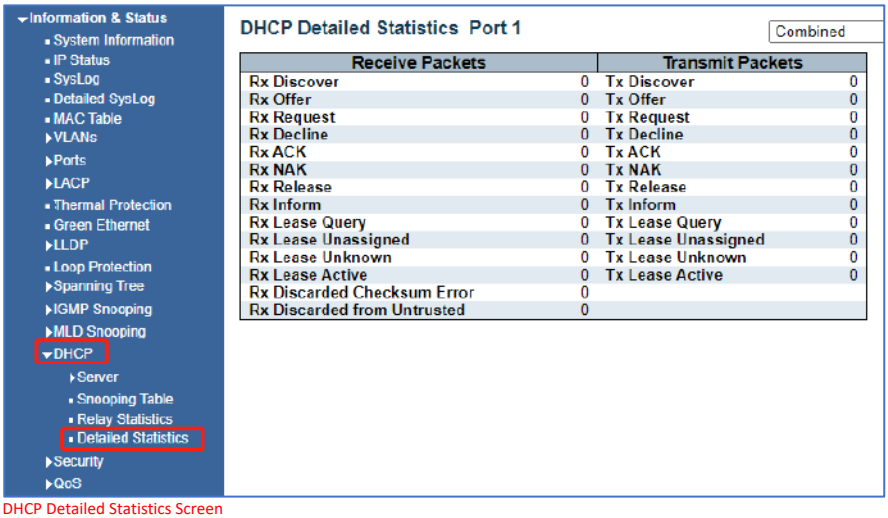


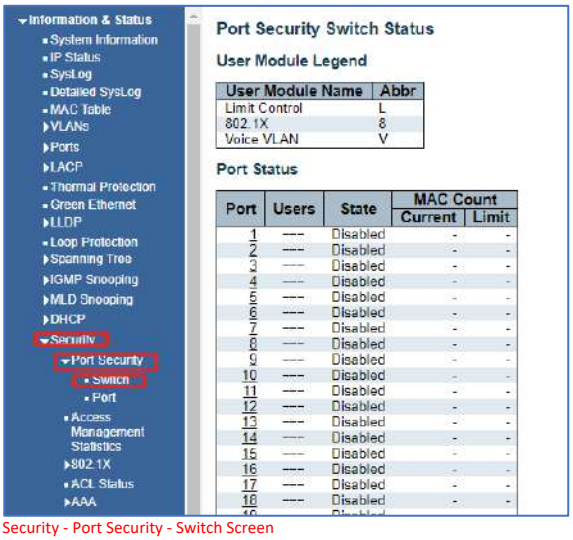
Figure 2-16-3 DHCP Relay Statistics Screen



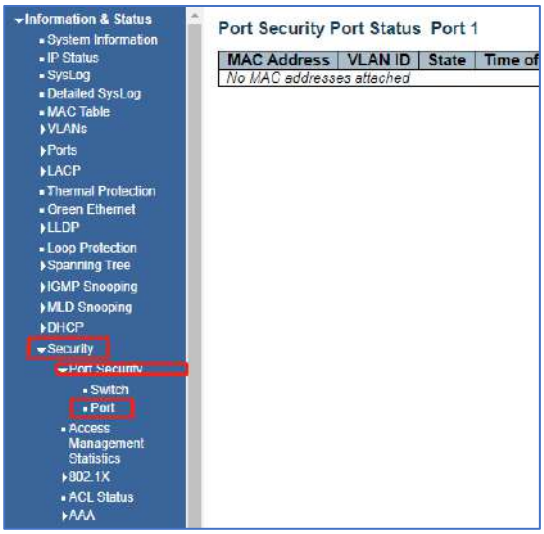
DHCP Detailed Statistics Screen

2.17 Security

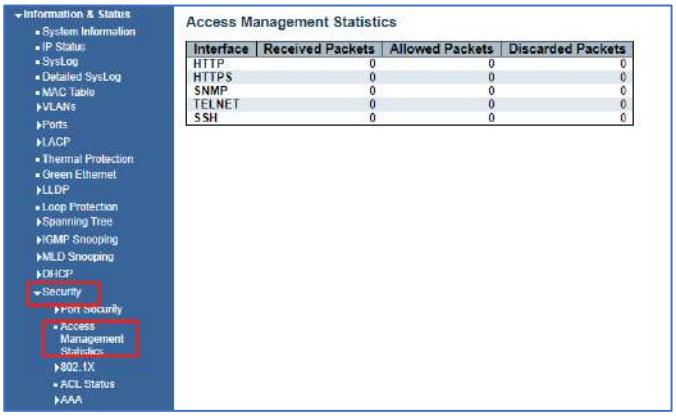
After click "Information & Status" > "Security", followed screen will appear as: Clients can go to Section" Security Configure" to do the detailed management.



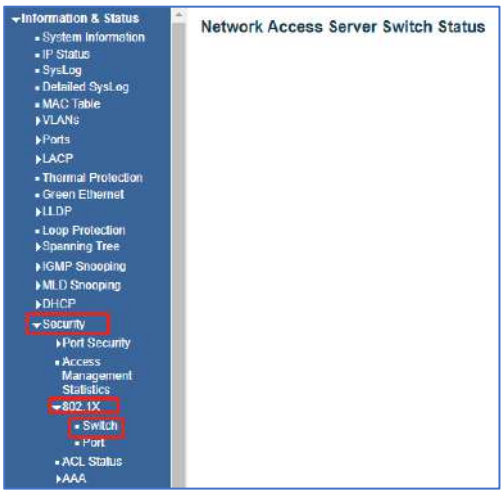
Security - Port Security - Switch Screen



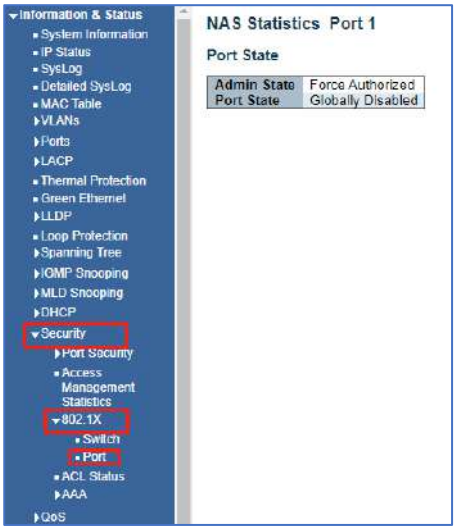
Security - Port Security - Port Screen



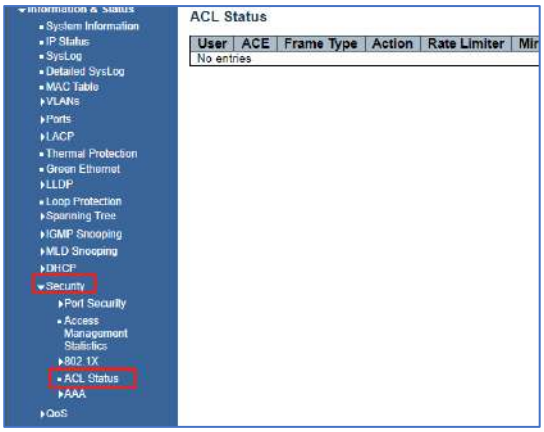
Security - Port Security - Access Screen



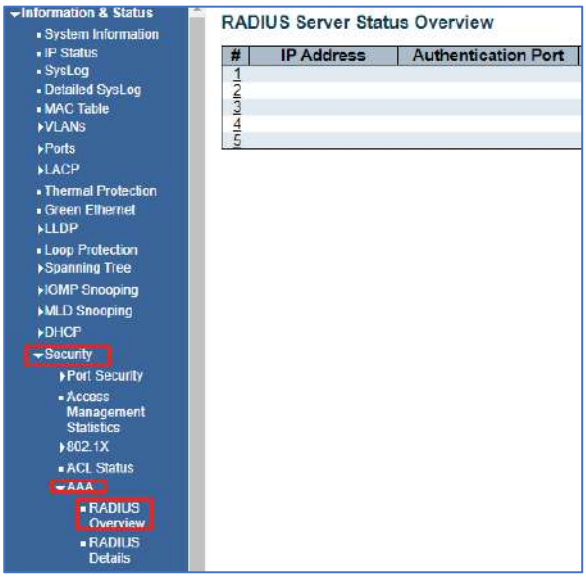
Security - 802.1X - Switch Screen



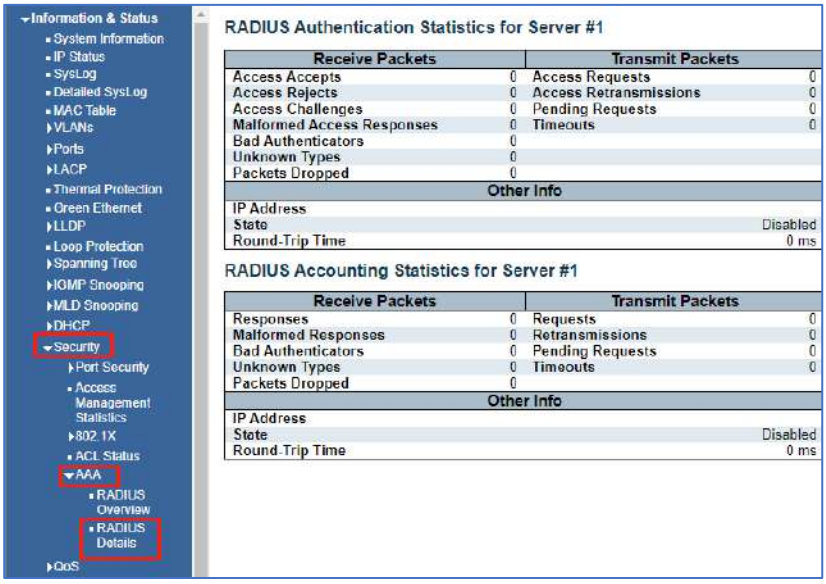
Security - 802.1X - Port Screen



Security - ACL Status Screen



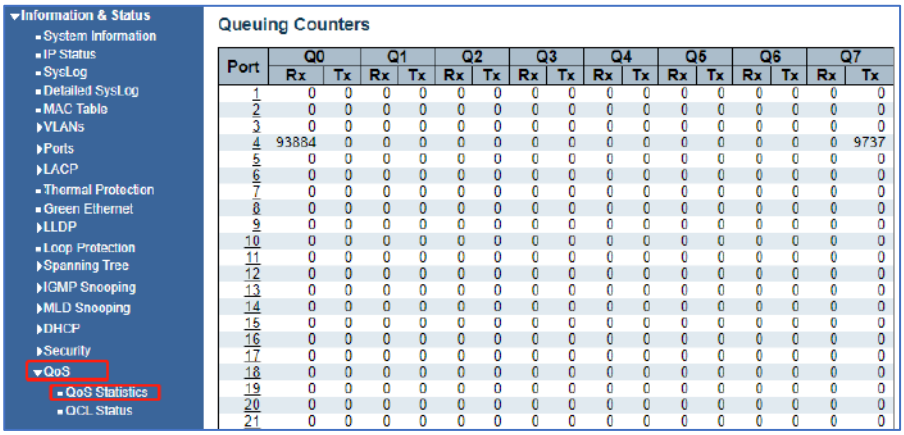
Security - AAA - RADIUS Overview Screen



Security - AAA - RADIUS Details Screen

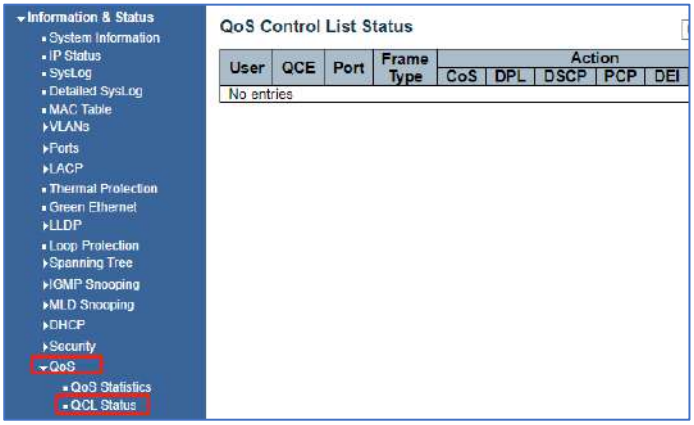
2.18 QOS

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



Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	93884	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9737
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

QOS Statistics Screen

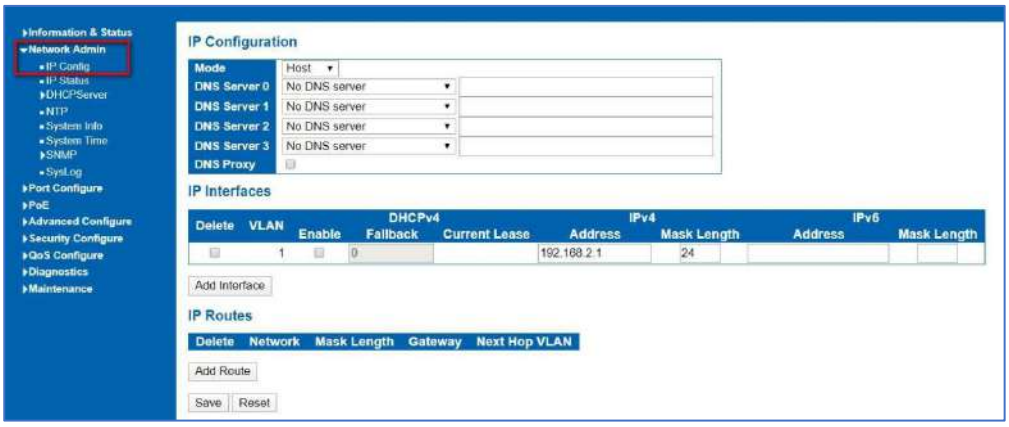


User	QCE	Port	Frame Type	Action				
				CoS	DPL	DSCP	PCP	DEI
No entries								

QOS Status Screen

3.1 IP Configuration

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 Screen

Following is description detail about IP configuration:

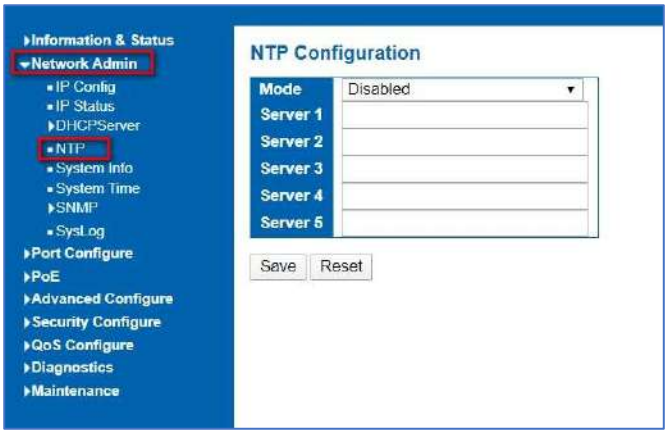
Name	Description
VLAN	VLAN for access and management of switch
IPv4 DHCP	- If enable, it means that VLAN port start IPv4 DHCP client, to dynamically get IPv4 addresses of the switch. Otherwise, it will use switch's static IP configuration. - Fallback (Seconds) means the waiting time for switch to get 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 NTP Configuration

Note: The switch only created VLAN1 by default. If user needs to use other VLAN for switch management, please first add VLAN in the VLAN module, and add the relevant port to the VLAN.

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.

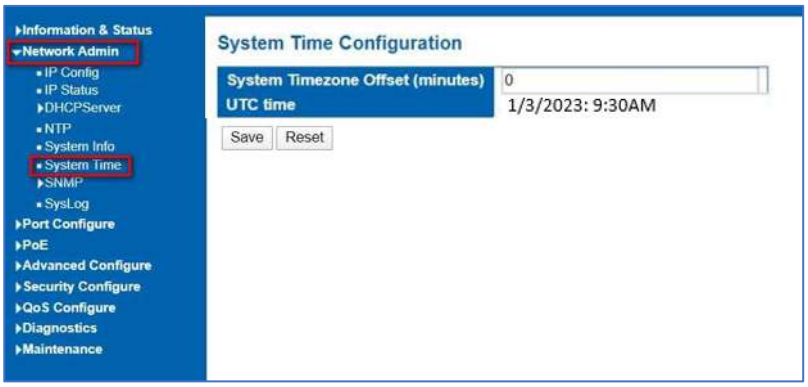


NTP Configuration Screen

Click ''Save'' to save settings.

3.3 system Time Configuration

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.
Click "Network Admin" > ''System Time'', screen will show as:



Time zone Configuration Screen

If power is lost the time/date reference must be re-established

3.4 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 similar to 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:

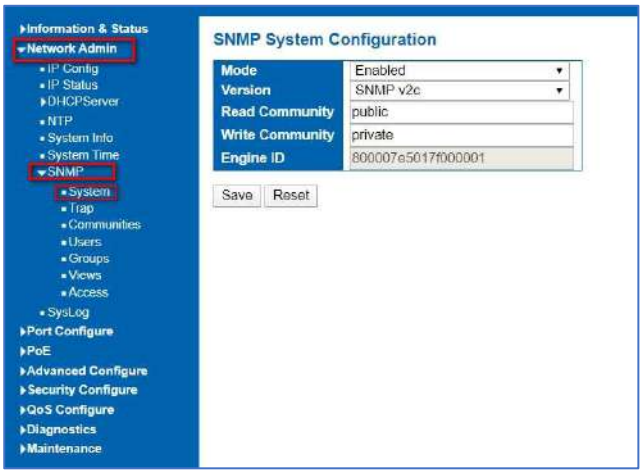
1. public – allow an authentication management station to read MIB objects.

2. private – allow an authentication management station to read, write and edit MIB objects.

Trap
Used by the agent to asynchronously inform the NMS of some event. These events may be very serious, such as reboot (someone accidentally turned off switch), or just general information, such as port status change. In these cases, switch create trap information and send then to receiver or network admin. Typical trap includes authentication failure, networking changes and cold/hot start trap.
MIB
A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules. Switch uses standard MIB-II information management module. So, MIB object value can be read by any SNMP web-managed software.
We can provide ALL the MIBs file including private MIBs to client if requested.

3.4.1 SNMP System Configuration

You can enable or disable the SNMP System Configuration. Its screen will appear after you click "Network Admin" > "SNMP" > "System."



SNMP System Configuration Screen

Configuration object and description is:

Object	Description
Mode	Enabled or Disable SNMP function
Version	Click drop-down menu to select SNMP v2c or SNMP v1 version
Read Community	Public: allow authentication management station to read MIB objects
Write Community	Private: allow authentication management station to read and write MIB objects.

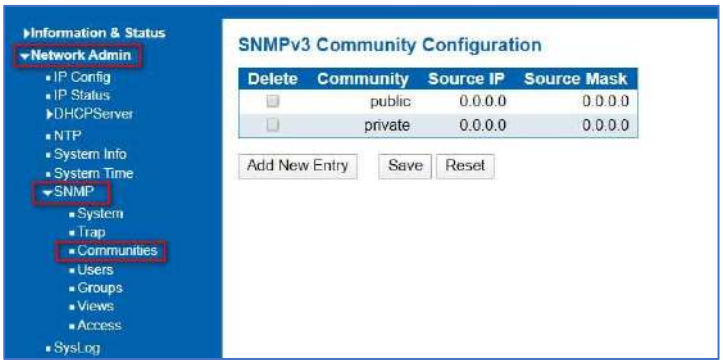
3.4.2 SNMP Trap Configuration

User can enable or disable SNMP Trap function and set configuration. Click "Network Admin" > "SNMP" >"Trap", then this screen will show as:

SNMP Trap Configuration Screen

3.4.3 SNMP Community Configuration

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



SNMP Communities Configuration Screen

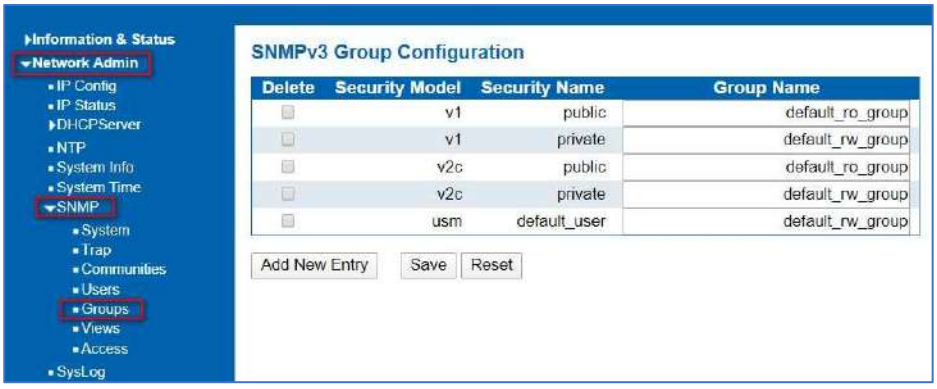
3.4.4 SNMP Users Configuration

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

Figure 3-4.4 SNMP User Configuration Screen

3.4.5 SNMP Group Configuration

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



SNMP Group Configuration Screen

3.4.6 SNMP View Configuration

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

SNMP View Configuration Screen

3.4.7 SNMP Access Configuration

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

SNMP Access Configuration Screen

3.5 System Log Configuration

User can configure switch's system log, via following screen after click "Network Admin" > "Syslog."

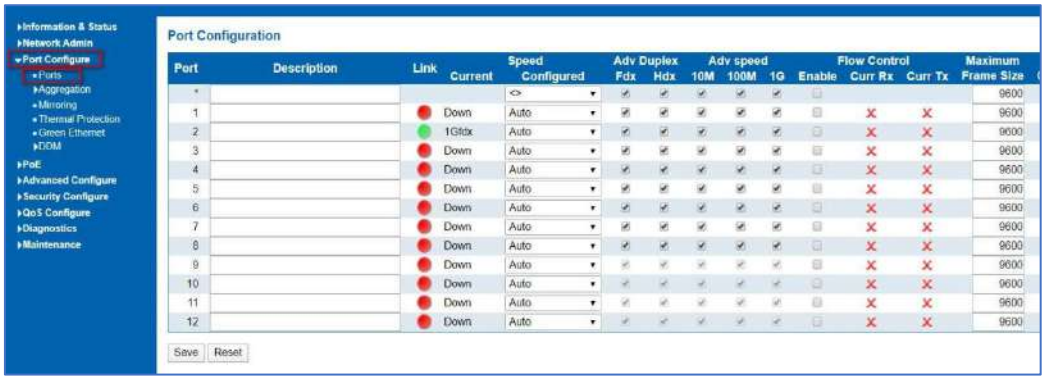
Figure 3-5 System Log Configuration Screen

Object	Description
Server Mode	Enabled or Disable SNMP System Log function. If ''Enable'' is selected, switch will send System Log to defined server.
Server Address	Defined server IP address
Syslog Level	To define System Log level, including: **Info:** Information, warnings and errors. **Warning:** warnings and errors. **Error:** errors.

Chapter 4: Port Configure

4.1 Port Configuration

This page is for configuring port specifications of switch. After click "Port Configure" > "Ports", this screen will appear as:



System Log Configuration Screen

Configuration object and description is:

Object	Description
Link	Red color means Link Down, green color means Link Up
Speed	Select the port speed and full / half duplex mode. "Disabled" means that port is disabled. "Auto" meaning in full-duplex (FDX) or half-duplex mode (HDX) (1000mbps always in full-duplex mode) auto negotiate among 10,100,1000Mbps devices. "Auto" setting allows the port to automatically determine the fastest settings for the device connected, and to apply these settings. "1000-X_AMS" means that port is Ethernet/Optical combo port, and optical port is prioritized. Other options are 10M HDX, 10M FDX, 100M HDX, 100M FDX, 1000M FDX, 1000-X.
Flow Control	It is a flow control mechanism for a variety of port configurations. Full-duplex ports use 802.3x flow control, half-duplex ports use backpressure flow control. It is disabled by default. Check to enable flow control.
Maximum Frame Size	It is used to set the maximum frame size for Ethernet. The default setting is 9600, which is to support Jumbo frames.

Click "Save" to store and active settings.

4.2 Link Aggregation

Users can set up multiple links among multiple switches. Link Aggregation is a method that tie some physical ports together as one logic port, to enlarge bandwidth. This switch supports up to 6 groups Link Aggregation, 2 to 8 ports as one group.

Note: If any port in the link aggregation group is disconnected, data packet that sent to disconnected port will share load with other connected port in this aggregation group.

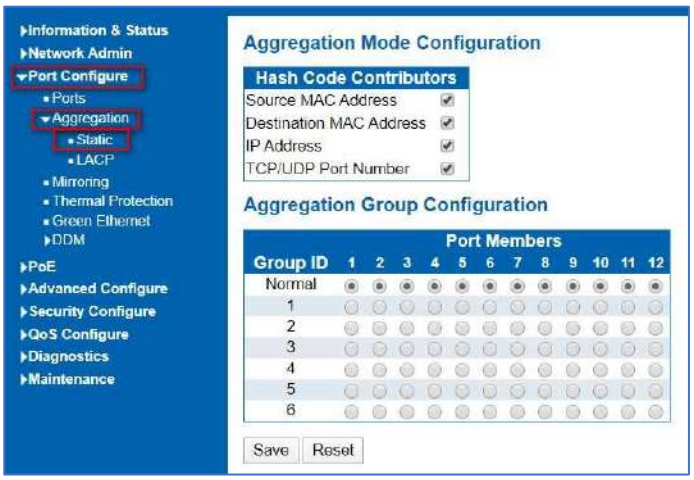
4.2.1 Static Aggregation

In this page, user can configure static aggregation of switch's ports. After clicking the menu "Port Configure" >"Aggregation" > "Static", followed window will appear for making static aggregation settings.

Vi30130
Pot Mode Option: Disable, PoE, PoEt, PoE++ and Manual.

1. Disable: Disable Pot function.
2. PoE: Enable 802.3af PoE function and provide up to 15.4 W according to the PD classes detected.
3. PoEt: Enable 802.3af/at/bt Poe function and provide up to 30 W according to the PD classes detected.
4. Pot++: Enable 802.3af/at/bt Po function and provide up to 90 W according to the PD classes detected.

Manual: Enable 802.3af/at/bt Pot function and set 90W Power Allocated Note: To configure the limit power for the port: 1. Go to PoE setting and select "Manual" option for "Reserved Powe determined by"; 2. Manually enter the power value on the "Maximum Power" column for the port.



Port Static Aggregation Configuration Screen

Configuration object and description is:

Object	Description
Aggregation Mode Configuration	This parameter is flow hash algorithm among LAG (Link Aggregated Group) ports.
Group ID	Static aggregation group ID
Port Members	This sample switch supports up to 6 groups Link Aggregation, 2 to 8 port as one group.

Note: It allows a maximum of 8 ports to be aggregated as 1 static trunk group at the same time.

Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems that require high-speed redundant links. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode. For more detailed information, refer to the IEEE 802.3ad standard.

Users can create dynamic aggregation group for switches. After click "Port Configure" > "Aggregation" > "LACP", users can set LACP configuration in followed screen.

4.2.2 LACP Aggregation

LACP Configuration Screen

Configuration object and description is:

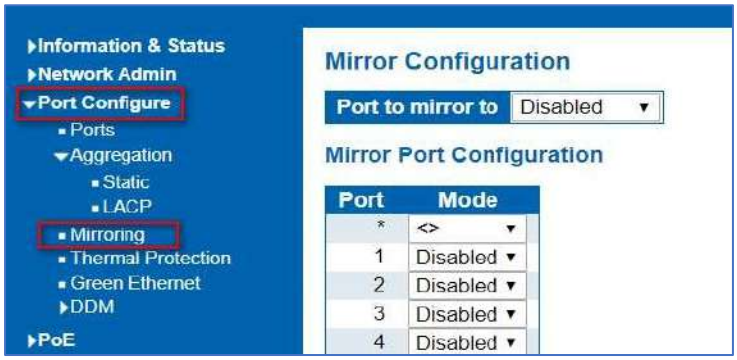
Object	Description
LACP	Enable or disable LACP function of that port.
Key	The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
Role	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
Timeout	The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.
Prio	The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device, then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Click "Save" to store and active settings.

4.3 Port Mirroring

Configure port Mirroring on this page. This function provides monitoring of network traffic that forwards a copy of each incoming or outgoing packet from one port of a network switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.
To configure Mirror settings, please click "Port Configure" > "Mirroring".

Then followed screen will appear as:



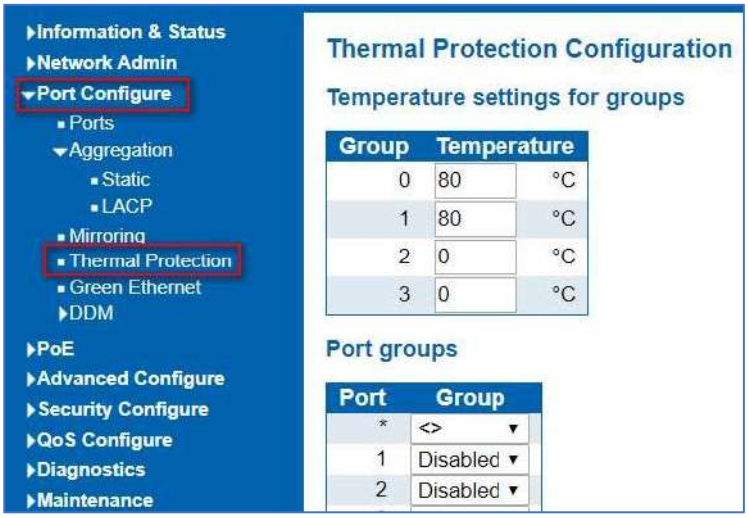
Mirroring Configuration Screen

Object	Description
Port mirror to	Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.
Mode	Select source port mirror mode. Rx only Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored. Tx only Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored. Disabled Neither frames transmitted nor frames received are mirrored. Enabled Frames received and frames transmitted are mirrored on the mirror port. Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror mirror port Tx frames. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

Note: You cannot set fast speed port(s) mirror to a low-speed port. For example, there is problem if you try to mirror 100Mbps port(s) to a 10 Mbps port. So destination port should has equal or higher speed comparing to source port. Besides, source port and destination port should not be same one.

4.4 Thermal Protection Configuration

Thermal protection is for detecting and protecting working switch. When switch detected port temperature is higher that defined temperature, system will disable the port, to protect switch itself.
After click "Port Configure" > "Thermal Protection", followed screen will appear as:



Mirroring Configuration Screen

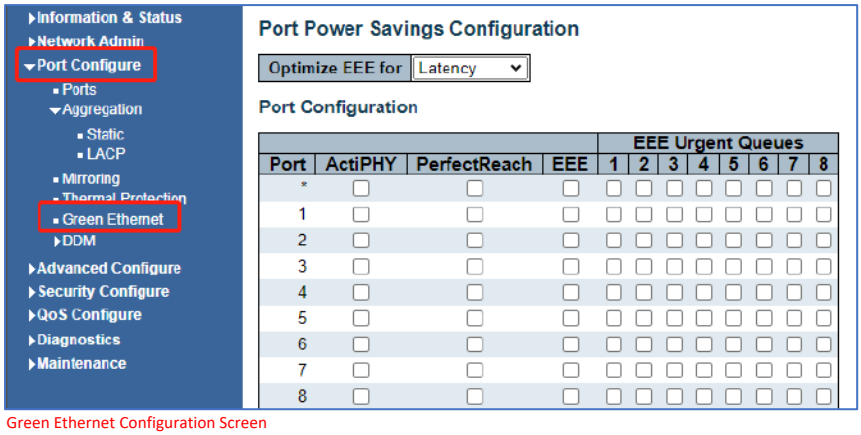
Configuration object and description is:

Object	Description
Temperature settings for priority groups	This switch support 4 Thermal Protection priority groups, and each of them can have a defined temperature for protection
Port priorities	Define which priority group that port belong to.

Click "Save" to store and active settings.
Note: By default, all ports of switch are belonging to Priority Group 0, with protected temperature 115-degree C.

4.5 Green Ethernet

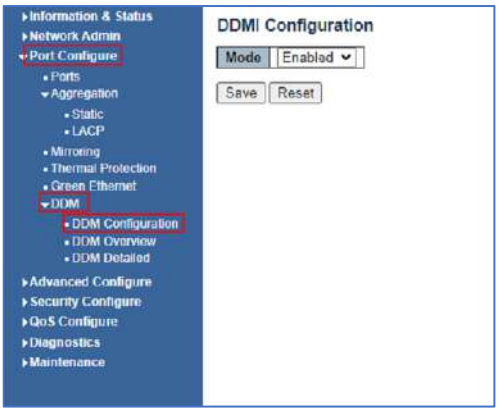
After click "Port Configure" > "Green Ethernet", followed screen will appear as:



Green Ethernet Configuration Screen

4.6 DDM

After click "Port Configure" > "DDM", followed screen will appear as:



DDMI Configuration Screen

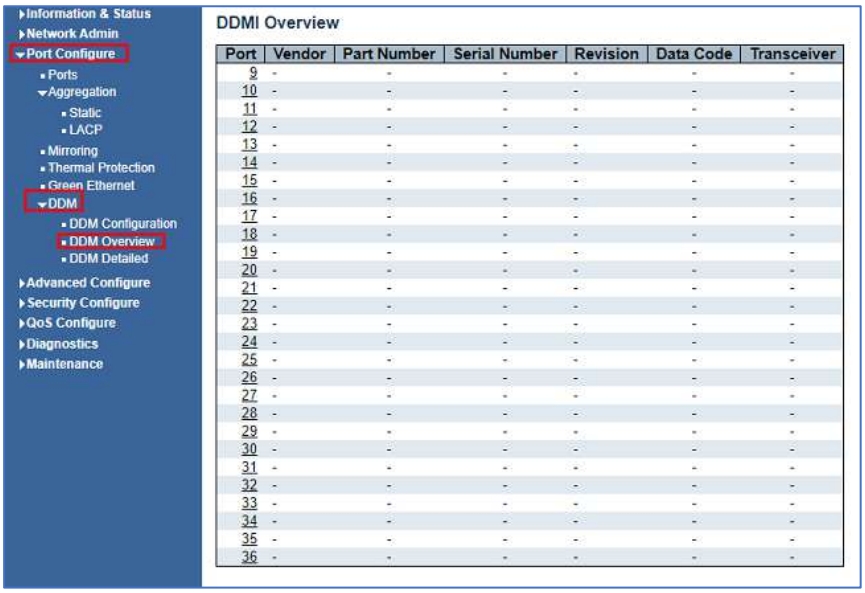


Figure 4-6.2 DDMI Overview Screen

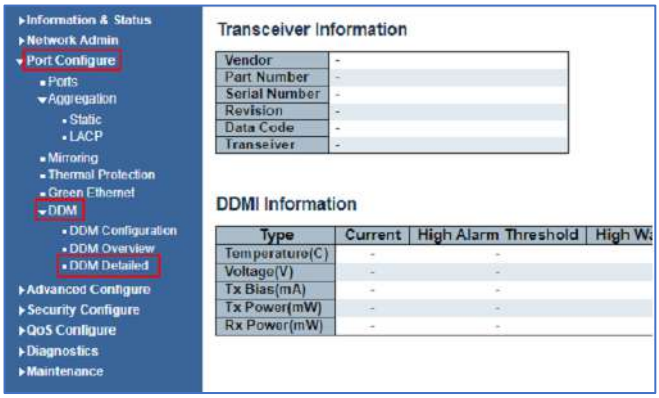


Figure 4-6.3 DDMI Detailed Screen

Chapter 5: PoE Configuration

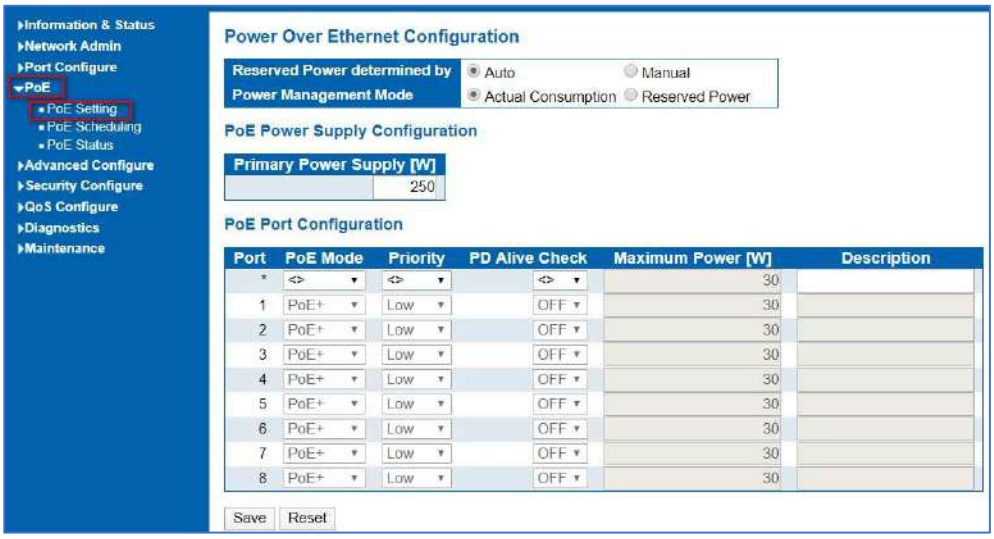
Power-over-Ethernet (PoE), means Ethernet network power supply via 100BASE-TX, 1000BASE-T. Its maximum power distance is 100 meters. By PoE power system, based on Ethernet wiring network of UTP Cat5 or higher Cable, it can give power to IP camera, VoIP phone, wireless AP, as well as transmit data. So there is no need to concern about the power wire building, reducing the cost of networking building.
PoE power supply system has unified standard, IEEE 802.3af,802.3at and 802.3bt. So devices from different manufacturers have no problem in general usage, as long as they are complied with these standards.
PD, it is defined as powered device in the PoE Power Supply System , primarily including IP camera, wireless AP, network VoIP phone, and other IP-based terminal equipment.
The whole process of PoE:

1. Detection: At beginning, PSE device output a very small voltage, to detect and judge if its linked PD is IEEE802.3af / IEEE802.3at/ 802.3bt compliant device. Only if detected that PD is a standard compliant device, then it will go to next step.
2. PD Classification: After detected PDs, PSE will classify them and recognize what is the power that PD required.
3. Power up: When above 2 steps finished, PSE start feeding required power for PD, with 44~57VDC output voltage.
4. Power supply: PSE provides stable 44~57V DC to PDs, and auto feeding power as requirement of PDs. Maximum power of single PoE port for IEEE 802.3af devices: 15.4W; Maximum power of single PoE port for IEEE 802.3at devices: 25.5W. Over 30W will result in 802.3bt which is valid to sources up to 90W.
5. Disconnection: If PD is disconnected or user disable PoE from management software, PSE will quickly (300- 400ms) stop powering PD.

In any moment of PSE powering PD process, PSE will stop working and then restart from step1 if abnormal situation happens, such as PD Short circuit, power consumption is higher than feeding power, and so on.

After click "PoE"> "PoE Setting", user can make PoE settings in followed screen: -

5.1 PoE Setting



PoE Setting Screen

Object	Description
Reserved Power determined by	This switch supports 2 modes for reserved power determination. Auto: Switch automatically assigned maximum power of switch port according to detected PD class. About PD Class, please refer to the 802.3af / 802.3at definition. Manual: Maximum reserved power of the port is customize by the user.
Power Management Mode	This switch supports 2 modes for Power Management. Actual Consumption: In this mode, when the actual power consumption of all the ports exceeds the switch's power budget, the lowest priority port will be shut down. If all ports have the same priority, then the maximum port number would be shut down. Reserved Power: In this mode, when the reserved power consumption of all the ports exceeds the switch's power budget, the port that connect to new PD will not be enabled.
Primary Power Supply [W]	Users can set the maximum primary power of the whole switch. Default setting is 770W.
PoE Mode	This switch support 802.3af (PoE) ,802.3at(PoE+) and 802.3bt/PoE++ mode. Default setting is 802.3at.
Priority	Define the priority of the PoE port. Priority from low to high is Low, High, Critical.
PD Auto checking	The port could monitor the RX traffic statistics and POE status, if it detects to have no traffic received about ~2minutes while POE status is on, the switch will reset the POE output. Users could enable/disable this feature by each port
Maximum Power(W)	It is for define port's maximum Power when user set Manual as reserved power determination mode.

Click "Save" to store and active settings.

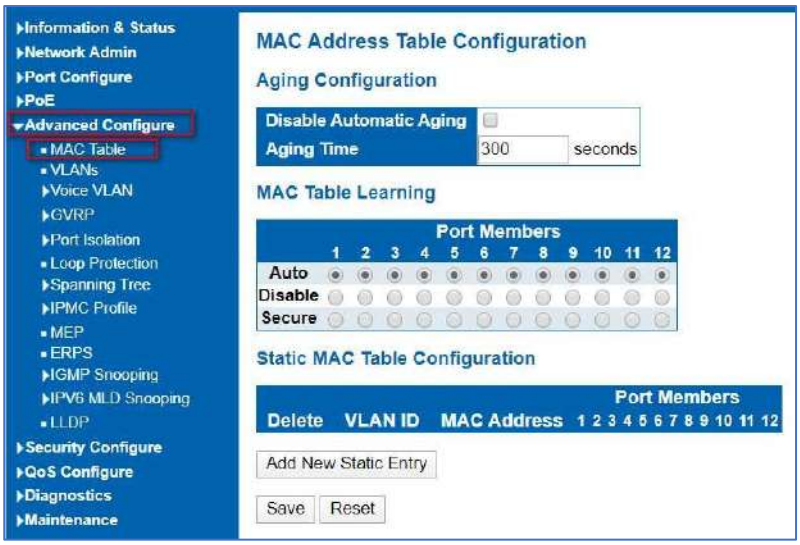
5.2 PoE Setting

In this page, user can check and look PoE status of all ports, after click "PoE"> "PoE Status".

PoE Status Screen

6.1 MAC Address Table

This page allows you to configure Mac address table settings. After Click "Advanced Configure" > "Mac Table", followed screen will appear.



MAC Address Table Configuration Screen

Configuration object and description is:

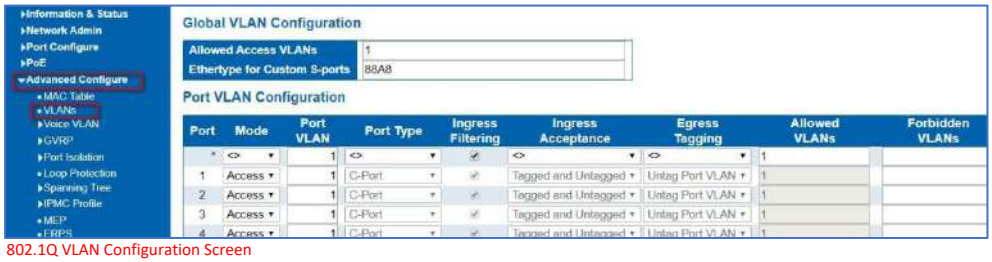
Object	Description
Disable Automatic Aging	If the box is checked, then the automatic aging function is disabled.
Aging Time	The time after which a learned entry is discarded. Range: 10-1000000 seconds. Default: 300 seconds.
MAC Table Learning	This switch supports 3 types for MAC Table Learning 1. Auto: port will auto learn Mac address. 2. Disable: port will NOT learn MAC address. 3. Secure: port only forward data of configured static MAC address.
Static MAC Table Configuration	The static entries in the MAC table are shown in this table. Click "Add New Static Entry" to create a new record.

Click "Save" to store and active settings.

6.2 VLAN

VLAN (Virtual Local Area Network) logically divide one LAN(Local Area Network) into a plurality of subsets, and each subset will form their own broadcast area network. In short, VLAN is a communication technology that logically divide one physical LAN into multiple broadcast area network (multiple VLAN). Hosts within a VLAN can communicate directly. But VLAN groups can not directly communicate with each other. So it will limit the broadcast packets within a VLAN. Since it cannot directly access between VLAN groups, thus it improves network security.

Click "Advanced Configure"> "VLANs" to see 802.1Q VLAN configuration screen as following:



802.1Q VLAN Configuration Screen

Object	Description
Allowed VLANs	Here displays created VLAN ID. It is 1 by default. If you want to create new VLAN, just need to add VLAN ID here.
Ethertype for Custom S-ports	This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.
Mode	The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied. **Access:** Access ports are normally used to connect to end stations. Access ports have the following characteristics: ➢ Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1 ➢ Accepts untagged and C-tagged frames ➢ Discards all frames that are not classified to the Access VLAN ➢ On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged **Trunk:** Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics: ➢ By default, a trunk port is member of all VLANs (1-4094) ➢ The VLANs that a trunk port is member of may be limited by the use of Allowed VLANS ➢ Frames classified to a VLAN that the port is not a member of are discarded ➢ By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress ➢ Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress **Hybrid:** Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities: ➢ Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware ➢ Ingress filtering can be controlled ➢ Ingress acceptance of frames and configuration of egress tagging can be configured independently

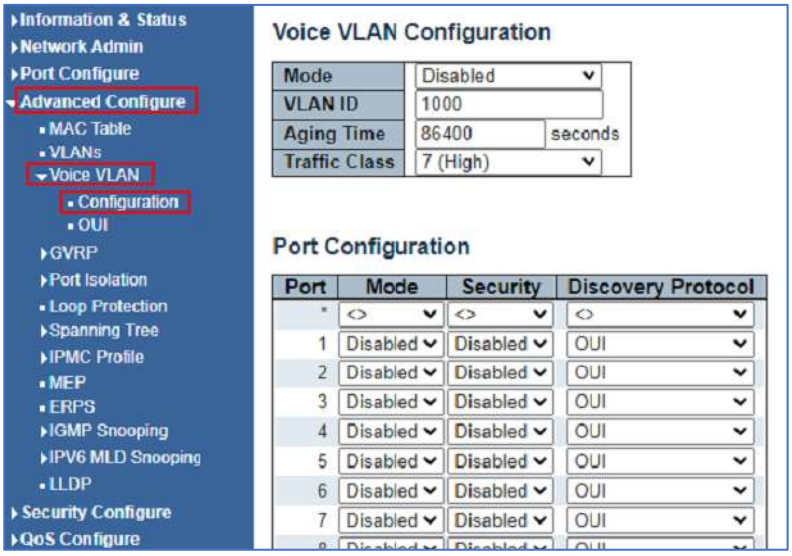
Port VLAN	Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4094, default being 1. On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untagged Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode
Port Type	Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required. **Unaware:** On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress. **C-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. **S-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag. **S-Custom-Port:** On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ether type configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.
Ingress Filter	Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.
Ingress Acceptance	Hybrid ports allow for changing the type of frames that are accepted on ingress. **Tagged and Untagged** Both tagged and untagged frames are accepted. **Tagged Only** Only tagged frames are accepted on ingress. Untagged frames are discarded. **Untagged Only** Only untagged frames are accepted on ingress. Tagged frames are discarded.
Egress Tagging	Ports in Trunk and Hybrid mode may control the tagging of frames on egress. **Untagged Port VLAN** Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. **Tag All** All frames, whether classified to the Port VLAN or not, are transmitted with a tag. **Untagged All** All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.
Allowed VLANs	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4094. The field may be left empty, which means that the port will not become member of any VLANs
Forbidden VLANs	A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.

	The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.

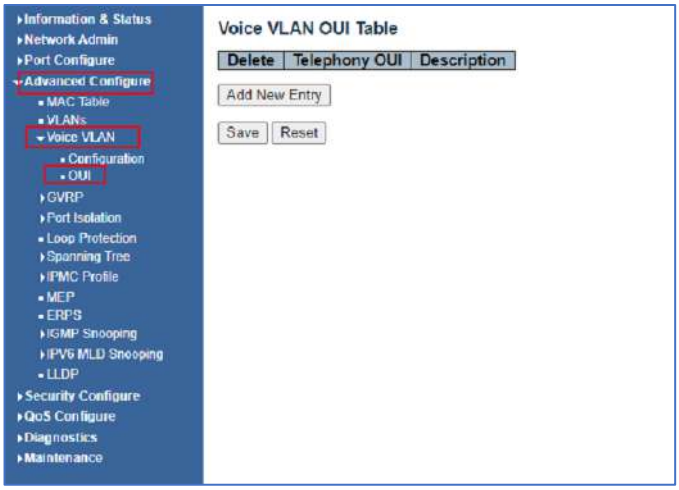
Click "Save" to store and active settings.

6.3 Voice VLAN

After click "Advanced Configure" > "Voice Vlan", followed screen will appear as:



Voice Vlan configuration screen



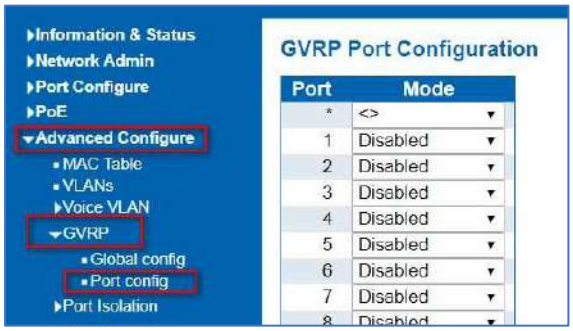
Voice Vlan OUI screen

6.4 GVRP

Adjacent Virtual Local Area Network (VLAN)-aware devices can exchange VLAN information with each other with the use of the Generic VLAN Registration Protocol (GVRP). GVRP is based on the Generic Attribute Registration Protocol (GARP) and propagates VLAN information throughout a bridged network. When GVRP is activated, it transmits and receives GARP Packet Data Units (GPDUs). This allows you to configure a VLAN on one switch and then propagate its information across the network, instead of the previously required creation of the VLAN on each switch in the network.

Click "Advanced Configure"> "GVRP" to see the configuration screen as following:

GVRP configuration screen



GVRP configuration screen

6.5 Port Isolation

Port isolation is for limiting data between ports. It is similar to VLAN, but more stricter.

6.5.1 Port Group

This switch support port groups. Members of port group can forward date.
Note: port can belong to to multiple port groups. Data can be forwarded among any port that belong tone port group.

After Click "Advanced Configure" > "Port Isolation" > "Port Group", then followed screen will appear for making port group configuration.

Port Group Configuration Screen

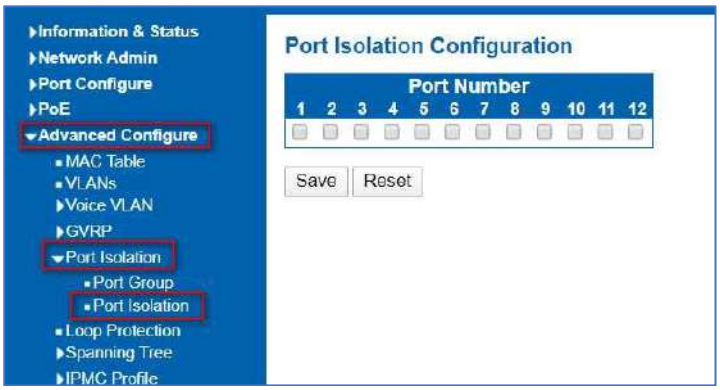
Configuration object and description is:

Object	Description
Port Members	Check the corresponding box to set them as one port group.

Click "Add New Port Group" to create a new port group, "Delete" to remove corresponding port group, and "Save" to store and active settings.

6.5.2 Port Isolation

After Click "Advanced Configure" > "Port Isolation" > "Port Isolation", then followed screen will appear for making port isolation configuration.



Port Isolation Configuration Screen

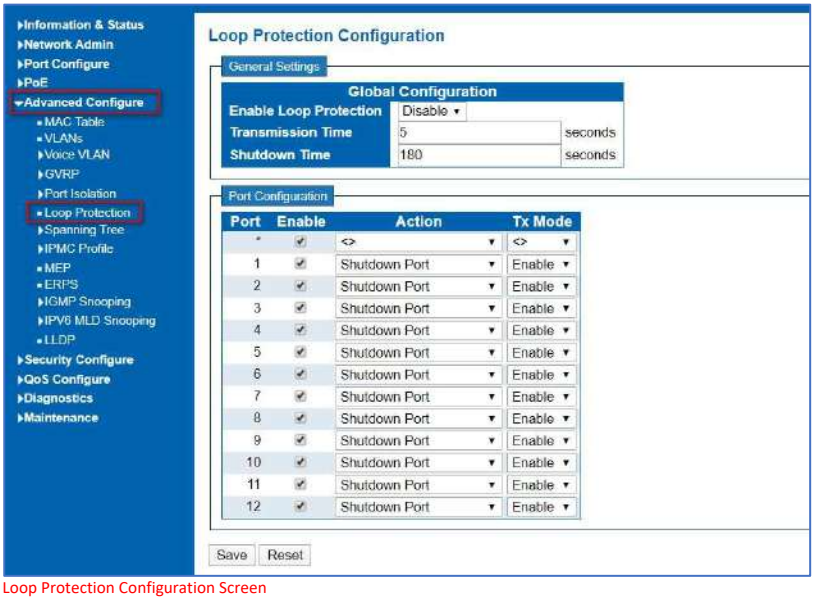
Configuration object and description is:

Object	Description
Port Number	Check box to set corresponding port as port isolation, so that they cannot forward data flow.

Click "Save" to store and active settings.

6.6 Loop Protection

Loop protection is to avoid broadcast loops. After Click "Advanced Configure" > "Loop Protection", followed screen will appear.



Loop Protection Configuration Screen

Configuration object and description is:

Object	Description
Global Configuration	Enable Loop Protection: click drop-down menu to disable or enable Loop Protection. Transmission Time: enter a number to set Loop Protection Interval Time; Shutdown Time: enter a number to set port Shutdown Time.
Enable	Check to enable corresponding port loop protection.
Action	Action take when the port detected loop. There are 3 types of action for users to select, Shutdown port, Shutdown port and Log, Log Only.
Tx Mode	To enable or disable Tx.

Click "Save" to store and active settings.

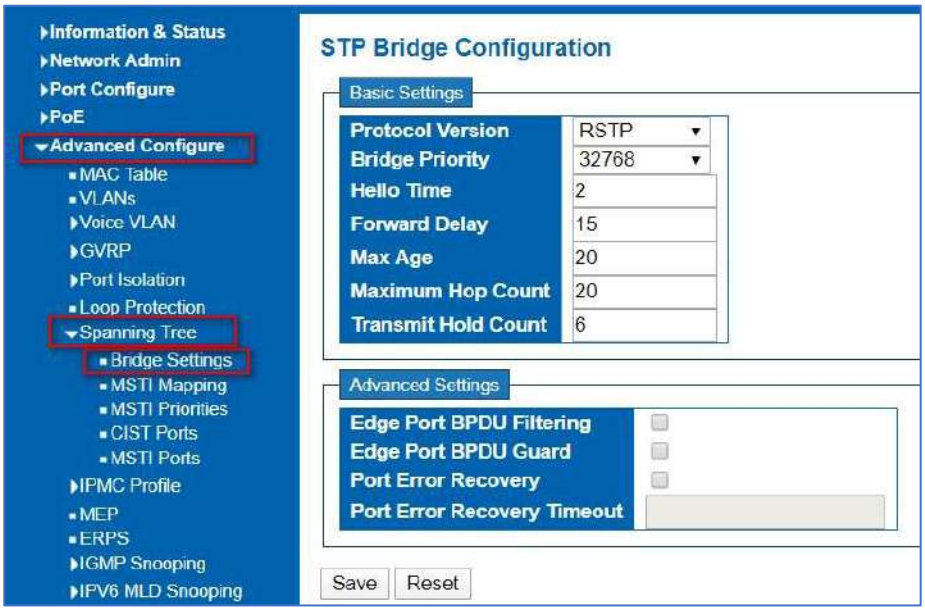
6.7 STP

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges, or routers. This allows the

switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network and provide backup links which automatically take over when a primary link goes down.

6.7.1 STP Bridge Setting

This page allows you to configure port STP settings. After Click "Advanced Configure" > "Spanning Tree" >"Bridge Settings", followed screen will appear.



Spanning Tree Configuration Screen

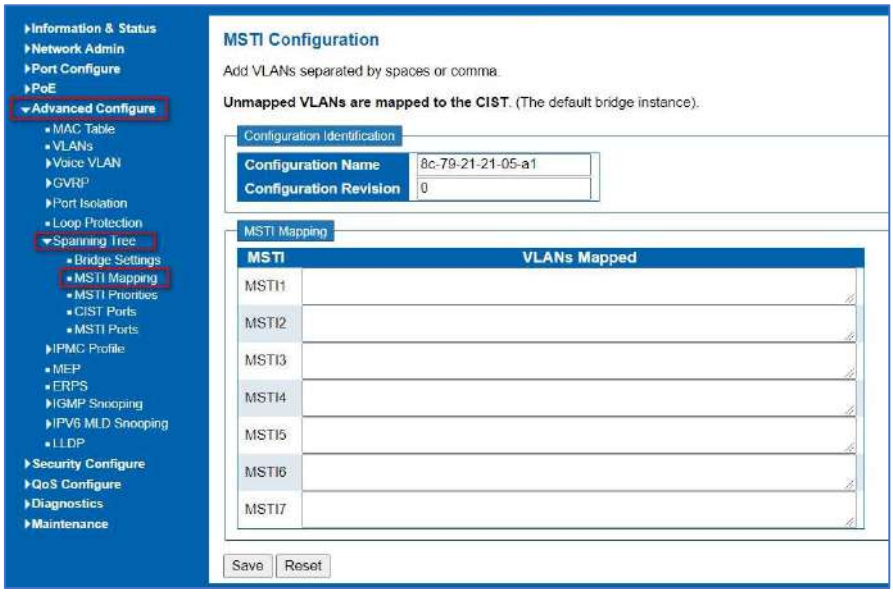
Configuration object and description is:

Object	Description
Protocol Version	Click drop-down menu to select STP protocol version, including: STP - Spanning Tree Protocol (IEEE802.1D); RSTP - Rapid Spanning Tree Protocol (IEEE802.1w)
Forward Delay (4-30)	Forward Delay setting range is from 4 to 30 seconds. Default value is 15 seconds.
Max Age (6-40)	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds. Default value is 20 .
Maximum Hop Count (6-40)	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 6 to 40 hops.
Transmit Hold Count (1-10)	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second. Default value is 6.

Click "Save" to store and active settings.

6.7.2 MSTI Mapping

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Configuration screen in Figure7-6-2-1 appears.



MSTI Configuration Page Screenshot

The page includes the following fields:
Configuration Identification

Object	Description
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to- MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

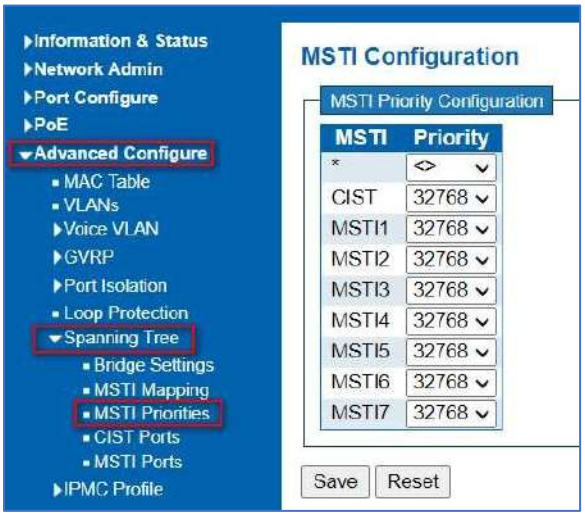
Object	Description
MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
VLANs Mapped	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. A unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)

Save : Click to apply changes.

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

6.7.3 MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Priority screen in Figure6- 7-3-1 appears.



MSTI Priority Page Screenshot

The page includes the following fields:

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

Save : Click to apply changes.

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

6.7.3 CIST Ports

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. The CIST port Configuration screen in Figure appears.

STP CIST Port Configuration Screenshot

Configuration object and description is:

Object	Description
Port	The switch port number of the logical STP port
STP Enabled	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user- defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above) Default: **128** Range: 0-240, in steps of 16
AdminEdge	Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized).
Restricted Role	If enabled, caused the port nor to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Altermatic Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as **Root Guard.**
Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.
BPDU Guard	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
Point-to- point	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transitions to the forwarding state is faster for point-to-point LANs than for shared media.

Save : Click to apply changes.

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

By default, the system automatically detects the speed and duplex mode used on each port and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Recommended STP Path Cost Range

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Recommended STP Path Costs

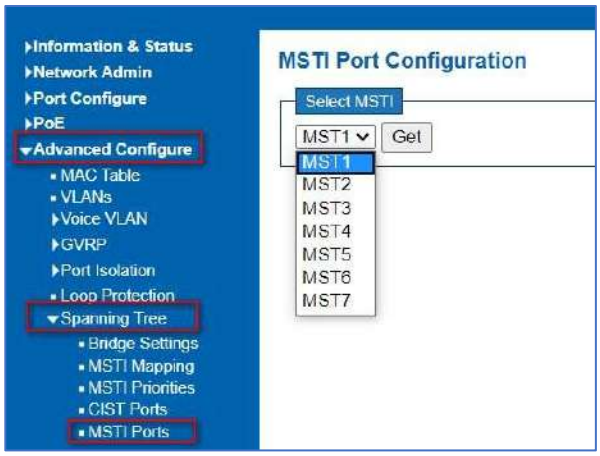
Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

Default STP Path Costs

6.7.5 MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

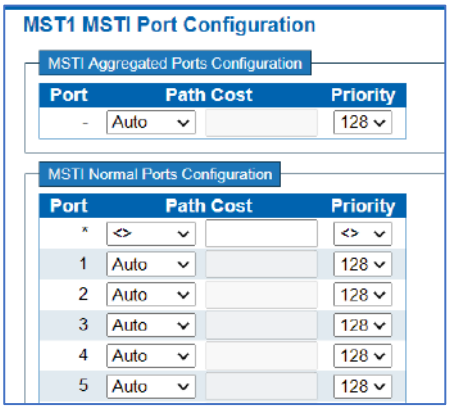
This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are global. The MSTI Port Configuration screen in Figure 6-7-5- 1& Figure 6-7-5-2 appears.



MSTI Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
Select MSTI	Select the bridge instance and set more detail configuration.



MST1 MSTI Port Configuration Page Screenshot

MSTx MSTI Port Configuration

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

Get : Click to set MSTx configuration.

Save : Click to apply changes.

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

6.8 IPMC Profile

This page provides IPMC Profile related configurations. The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each. The Profile Table screen in Figure 6-8-1 appears.

6.8.1 Profile Table

IPMC Profile Configuration Page

The page includes the following fields:

Object	Description
Global Profile Mode	Enable/Disable the Global IPMC Profile. System starts to do filtering based on profile settings only when theglobal profile mode is enabled.
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
Profile Name	The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.
Profile Description	Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.
Rule	When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons: : List the rules associated with the designated profile. : Adjust the rules associated with the designated profile

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

Save : Click to apply changes.

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

6.8.2 Address Entry

This page provides address range settings used in IPMC profile. The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create at maximum 128 address entries in the system. The Profile Table screen in Figure 6-8-2-1 appears.

IPMC Profile Address Configuration Page

The page includes the following fields:

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

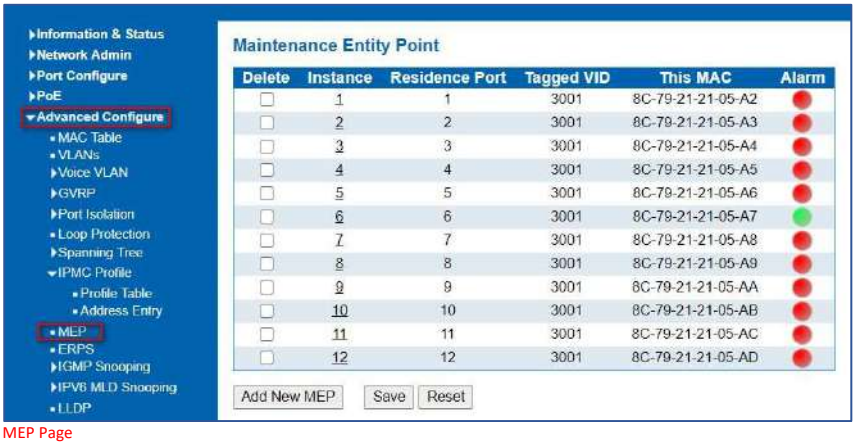
Add New Address (Range) Entry : Click to add new address range. Specify the name and configure the addresses. Click “Save”.

Save : Click to apply changes.

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

6.9 MEP

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



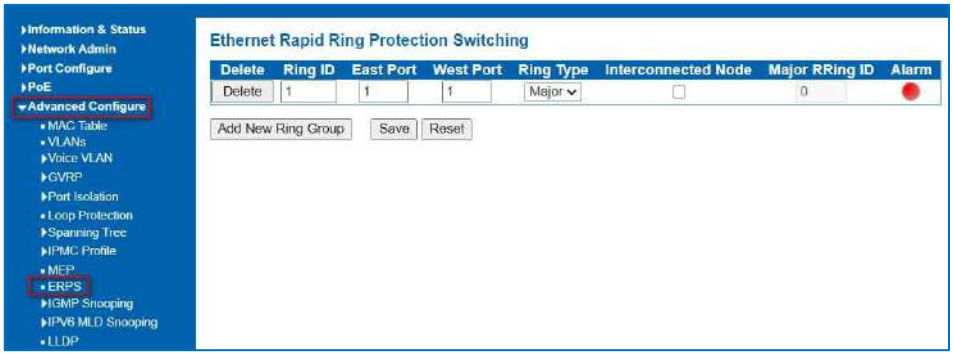
MEP Page

6.10 ERPS

ERPS (Ethernet Ring Protection Switching), it integrates OAM function and APS protocol. If the ring network was interrupted accidentally, the fault recovery times.

could be less than 50ms to quickly bring the network back to normal operation. ITU-T G.8032 is the first industry standard for ERPS.

Note: Before enable ERPS, STP of ring port should be disabled.
After Click "Advanced Configure" > "ERPS ", followed screen will appear.

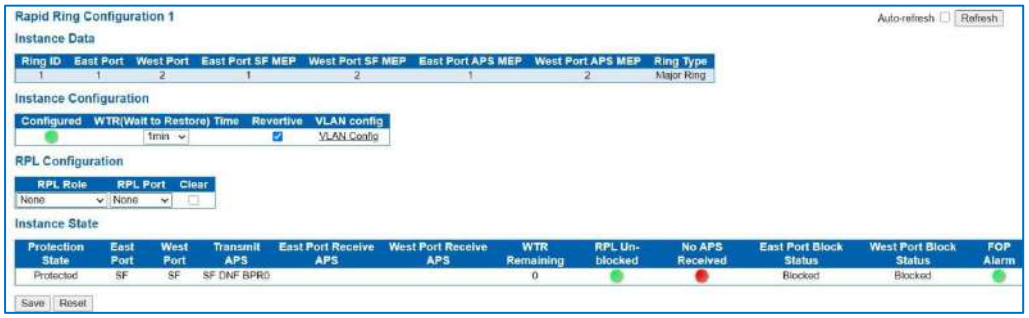


ERPS Configuration Screen

Configuration object and description is:

Object	Description
Ring ID	ERPS Ring ID
East Port	Number of the port which participate in this Ring protection.
West Port	Number of the other port which participate in this Ring protection.
Ring Type	Available selection: ''Major Ring'' or ''Sub Ring''. Only in case of Multi Ring application, ''Sub Ring'' is required to configure. Default Ring Type: ''Major Ring''. Only if there is multi ring application, it is required to set.
Interconnected Node	In Multi Ring application, Interconnected Node is the node that connect 2 or more rings.
Major Ring ID	In Single Ring application, Major Ring ID is same as Ring ID. In Multi Ring application, Sub Ring has to be type as Major Ring ID.
R-APS VLAN(1- 4094)	Define VLAN for R - APS VLAN.

Click "Add New Ring Group" to create a new ERPS ring application.
Click "Save" to store and active settings.
After click the number under "Ring ID", it will go to the page for Ring Configuration as followed screen:

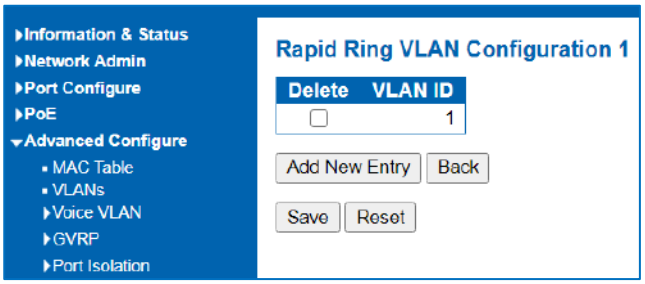


ERPS Ring Configuration Screen

Configuration object and description is:

Object	Description
WTR(Wait to Restore) Time(1-12)	Click drop-down menu to select WTR time for R-APS . Available selection: 1-12min Default: 1 min
Revertive	Check to enable Revertive status of R-APS.
VLAN config	After clicked '' VLAN config '', it will go the page of Rapid Ring VLAN Configuration.
RPL Role	Click drop-down menu to select ''None'', ''RPL Owner'', or ''RPL Neighbor'' role.
RPL Port	Click drop-down menu to select ''None'', ''East Port'', or ''West Port''.

Click "Save" to store and active settings.
After clicked '' VLAN config '', it will go the page of Rapid Ring VLAN Configuration as following screen:



Rapid Ring VLAN Configuration Screen

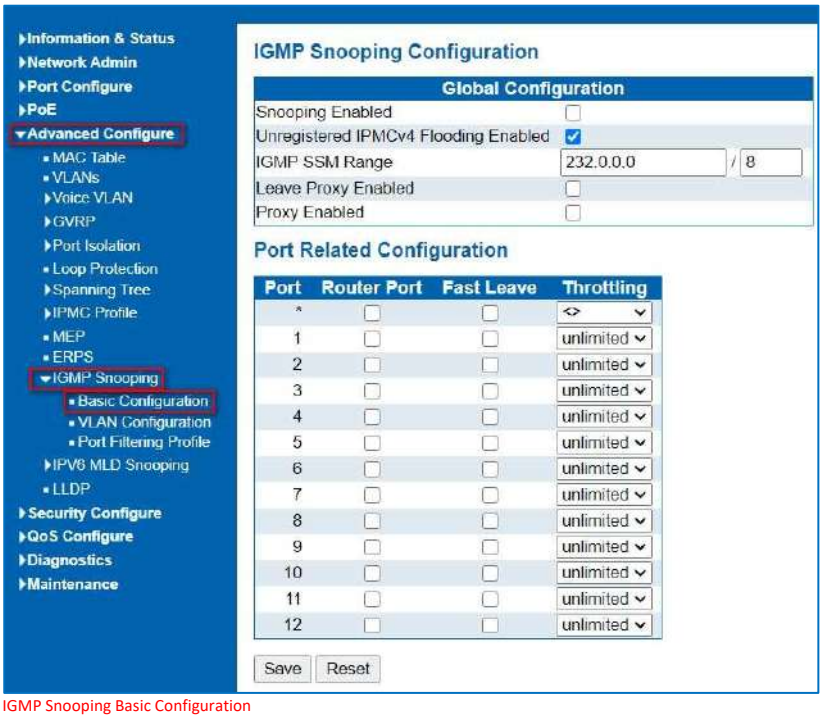
Click "Add New Entry" to create a new entry. Click "Save" to store and active settings.

6.11 IGMP Snooping

Internet Group Management Protocol (IGMP) lets host and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

6.11.1

After Click "Advanced Configure" > "IGMP Snooping" > "Basic Configuration", followed screen will appear.



IGMP Snooping Basic Configuration

Configuration object and description is:

Object	Description
Snooping Enabled	Enable or disable the IGMP snooping. The default value is "Disabled". Enable: check the box; Disable: do not check the box.
Unregistered IPMCv4 Flooding Enabled	Check the box to enable unregistered IPMCv4 Flooding
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Fast leave performs deleting MAC forward entry immediately upon receiving message for group de-registration

Click "Save" to store and active settings.

6.11.2 IGMP Snooping VLAN Configuration

After Click "Advanced Configure" > "IGMP Snooping" > "VLAN Configuration", followed screen will appear.

IGMP Snooping VLAN Configuration

Configuration object and description is:

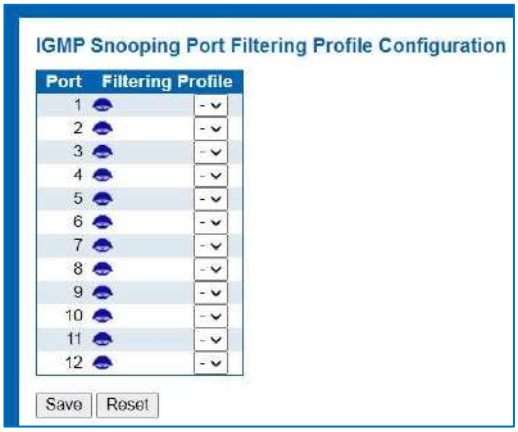
Object	Description
Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier Election	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier Address	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Click "Save" to store and active settings.

6.11.3 IGMP Snooping Port Filtering Profile

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.
IGMP filtering enables you to assign a profile to a switch port that specifies.

multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped. IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a a port, the switch can take one of two actions; either “deny” or “replace”. If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group. The IGMP Snooping Port Group Filtering Configuration screen in Figure 5-10-3 appears.



IGMP Snooping VLAN Configuration

Figure 6-11-4: IGMP Snooping Port Filtering Profile Configuration Page Screenshot

Configuration object and description is:

Object	Description
Port	The logical port for the settings
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

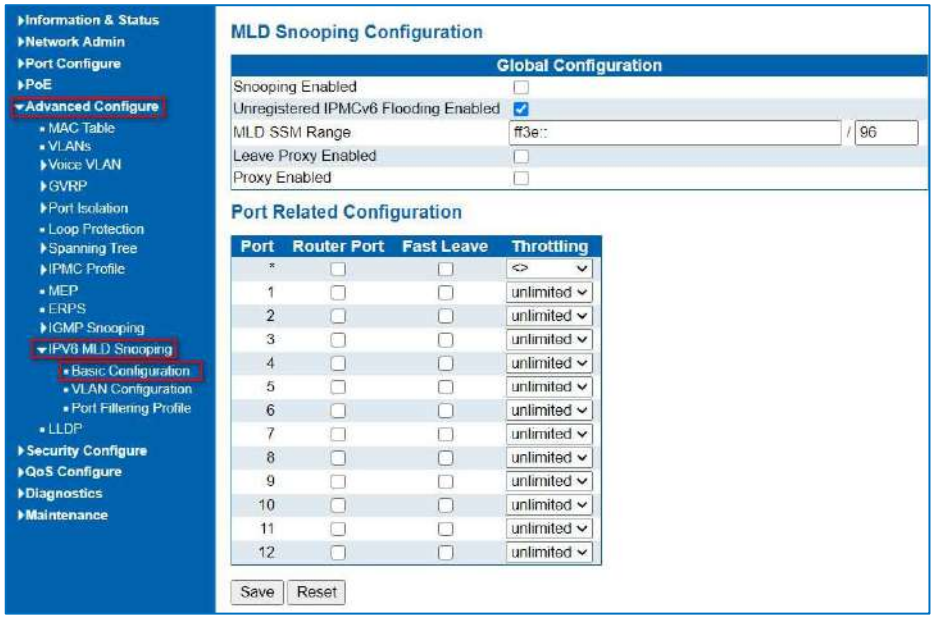
Save : Click to apply changes.

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

6.12 IPV6 MLD Snooping

This page provides MLD Snooping related configuration. The MLD Snooping Configuration screen in Figure 6-12-1 appears.

6.12.1 Basic Configuration



MLD Snooping Configuration Page Screenshot

Configuration object and description is:

Object	Description
Snooping Enabled	Enable the Global MLD Snooping
Unregistered IPMCv6 Flooding enabled	Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.
MLD SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
Leave Proxy Enable	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enable	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side..
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port. The allowed selection is **Auto**, Fix, Fone, default compatibility value is **Auto**.
Fast Leave	Enable the fast leave on the port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

Save : Click to apply changes.

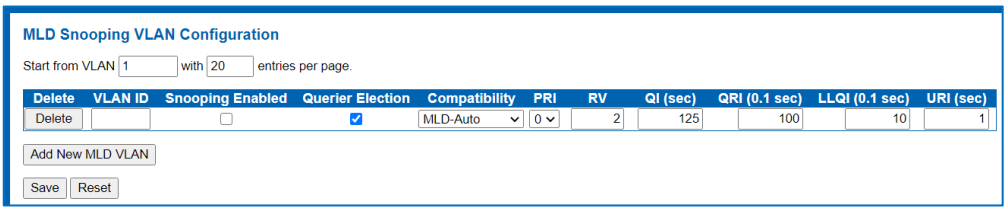
Reset : Click to undo any changes made locally and revert to previously saved values.

6.12.2 VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the

web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. The MLD Snooping VLAN Configuration screen in Figure5-11-2 appears.



IGMP Snooping VLAN Configuration Page Screenshot

Configuration object and description is:

Object	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
Vlan ID	The VLAN ID of the entry.
MLD Snooping Enable	Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.
Querier Election	Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.
Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto, Forced MLDv1, Forced MLDv2, default compatibility value is MLD-Auto.
PRI	(PRI) Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.
QRI	Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
LLQI (LMQI for IGMP)	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).
URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Refresh : Refreshes the displayed table starting from the "VLAN" input fields.

<< : Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

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

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

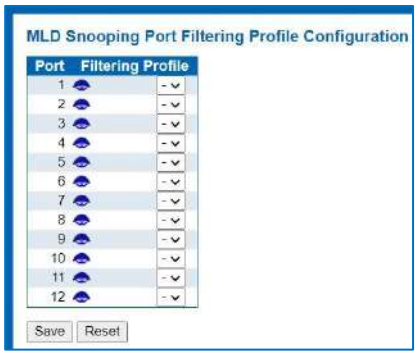
Save : Click to apply changes.

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

6.12.3 Port Filtering Profile

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The MLD filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and MLD throttling limits the number of simultaneous multicast groups a port can join.
MLD filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. A MLD filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, MLD join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the MLD join report is forwarded as normal. If a requested multicast group is denied, the MLD join report is dropped.

MLD throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace”. If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group. The MLD Snooping Port Group Filtering Configuration screen in Figure 5-11-3 appears.



MLD Snooping Port Group Filtering Configuration Page Screenshot

Object	Description
Port	The logical port for the settings
Filtering Group	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button

Save : Click to apply changes.

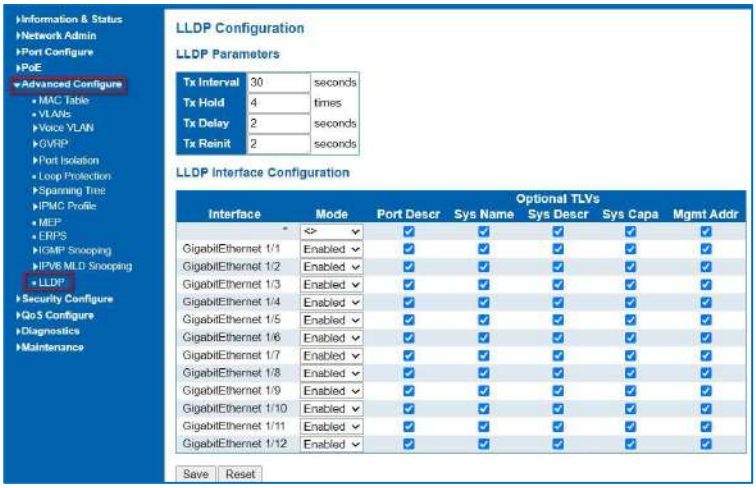
Reset : Click to undo any changes made locally and revert to previously saved values.

6.13 LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device.

Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities, and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

After Click "Advanced Configure" > "LLDP", followed screen will appear.



LLDP Configuration Screen

Configuration object and description is:

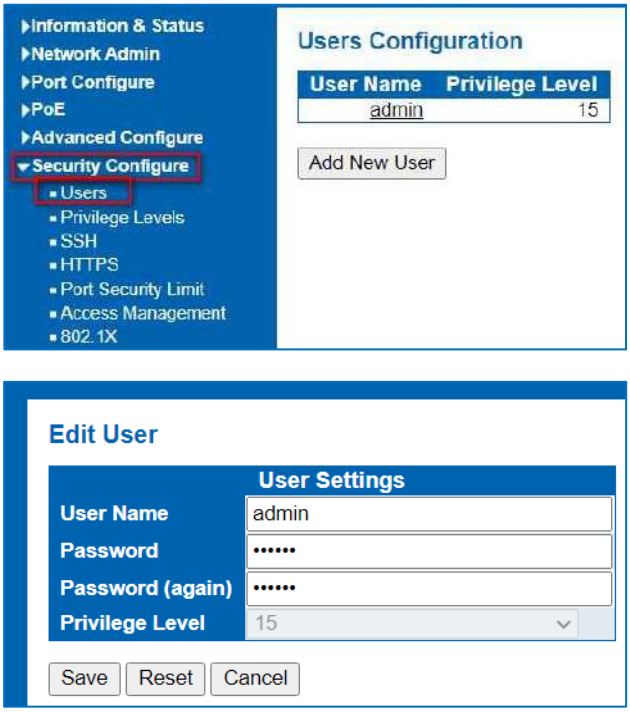
Object	Description
LLDP Parameters	Here allows the user to inspect and configure the current LLDP port settings: ➢ Tx Interval: Transmission Interval Time ➢ Tx Hold: Hold time Multiplier ➢ Tx Delay: Transmit Delay Time ➢ Tx Remit: Transmit Remit Time
Mode	Select LLDP messages transmit and receive modes for LLDP Protocol Data Units. Options are Tx only, Rx only, Enabled, and Disabled.
Optional TLVs	To configure the information included in the TLV field of advertised messages. When followed option is checked, corresponding information will be included in LLDP information transmitted. ➢ Port Descr: Port Description ➢ Sys Name: System Name ➢ Sys Descr: System Description ➢ Sys Capa: System Capability ➢ Mgmt Addr: Management Address

Click "Save" to store and active settings.

Chapter 7: Security Configure

7.1 User Configuration

Users can add user to manage the switch, please click “Security Configure”>” Users”>” Add New User”



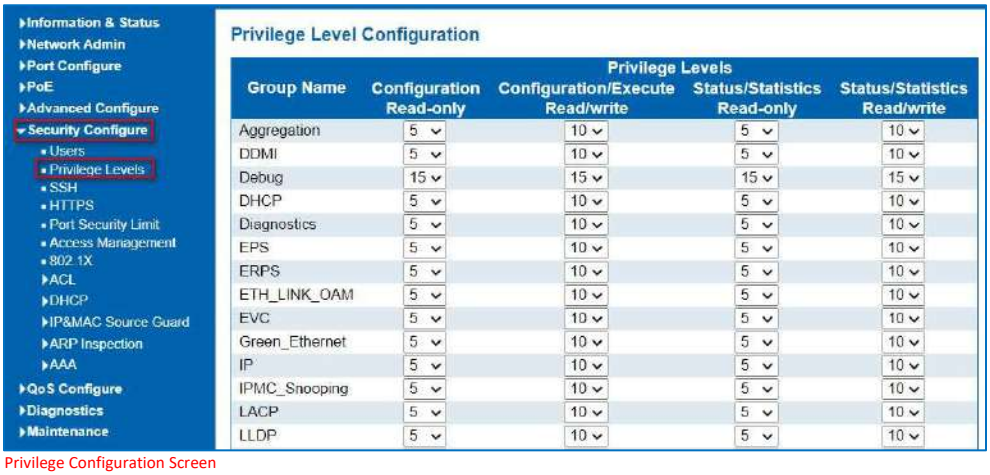
Users Configuration Screen

Click "Save" to store and active settings.

Note: Privilege Level 15 is the highest management authority.

7.2 Privilege Levels Configuration

This page provides an overview of the privilege levels. After setup is completed, please press the “Apply” button to take effect. Please login web interface with new username and password and the screen in Figure 6-2-1 appears. please click “Security Configure”>” Privilege Levels”.



Privilege Configuration Screen

The page includes the following fields:

Object	Description
Group Name	The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contain more than one. The following description defines these privilege level groups in details: System: Contact, Name, Location, Timezone, Log ➢ **Security:** Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard. ➢ **IP:** Everything except 'ping'. ➢ **Port:** Everything except 'VeriPHY'. ➢ **Diagnostics:** 'ping' and 'VeriPHY'. ➢ **Maintenance:** CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance. ➢ **Debug:** Only present in CLI.
Privilege Level	Every privilege level group has an authorization level for the following subgroups: ➢ **Configuration read-only** ➢ **Configuration/execute read-write.** ➢ **Status/statistics read-only** ➢ **Status/statistics read-write** (e.g. for clearing of statistics).

Save : Click to apply changes.

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

7.3 SSH Configuration

Configure SSH on this page. This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

Users can enable or disable the SSH configuration, please click “Security Configure”>”SSH”.

Privilege Configuration Screen

The page includes the following fields:

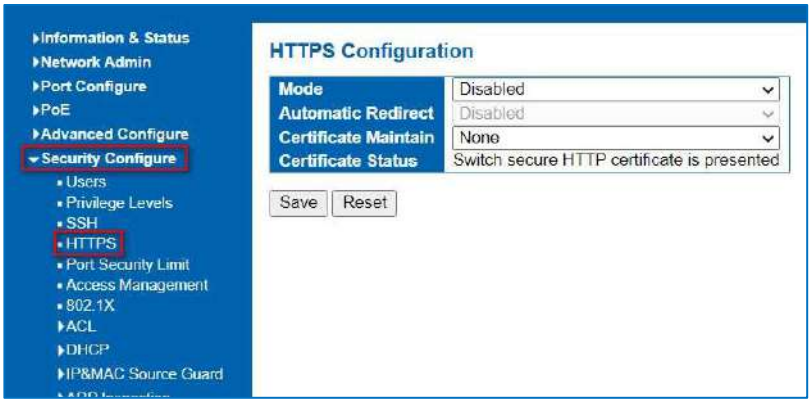
Object	Description
Mode	Indicates the SSH mode operation. Possible modes are: ➢ Enabled: Enable SSH mode operation. ➢ Disabled: Disable SSH mode operation.

Save : Click to apply changes.

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

7.4 HTTPS Configuration

Users can configure HTTPS function, please click “Security Configure”>” HTTPS.



HTTPS Configuration Screen

The page includes the following fields:

Object	Description
Mode	Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are: ➢ Enabled: Enable HTTPS mode operation. ➢ Disabled: Disable HTTPS mode operation.
Automatic Redirect	Indicates the HTTPS redirect mode operation. It only significant if HTTPS mode "Enabled" is selected. Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled or redirects web browser to an HTTP connection when both are disabled. Possible modes are: ➢ Enabled: Enable HTTPS redirect mode operation. ➢ Disabled: Disable HTTPS redirect mode operation.
Certificate 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.
Certificate Pass Phrase	Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.
Certificate Upload	Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39. Possible methods are: **Web Browser:** Upload a certificate via Web browser. **URL:** Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]< host>[:<port>][/<path>]/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/ne w_image.dat. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.
Certificate Status	Display the current 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 ...

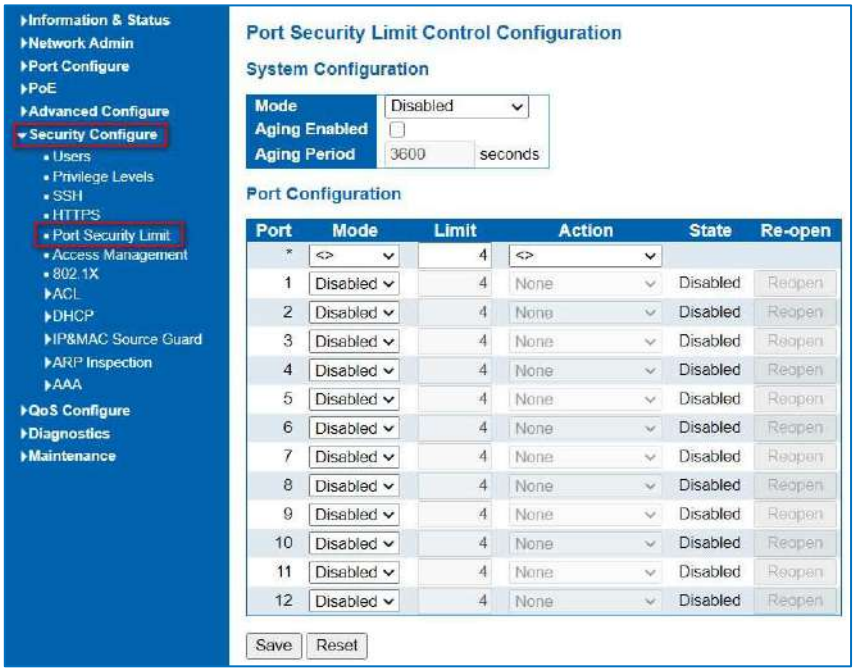
Save : Click to apply changes.

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

Refresh : Click to refresh the page. Any changes made locally will be undone.

7.5 Ports Security Limit Configuration

In this page, user can make IP&MAC Source Guard Port Configuration. After click ''Security Configure''>''IP & MAC Source Guard'' >''Configuration'', followed screen will appear.



IP&MAC Guard-Port Configuration Screen

Configuration object and description is:

Object	Description
Global Mode	Click drop-down menu to enable or disable Global IP&MAC Source Guard function
Port Mode	Click drop-down menu to enable or disable the IP&MAC Source Guard function for corresponding port.
Max Dynamic Clients	Click drop-down menu to select Max Dynamic Clients. Available options: Unlimited, 0, 1, 2.

Click "Save" to store and active settings.

7.6 Access Management configuration

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

access to the switch. The Access Management Configuration screen in Figure 6-6-1 appears.

Access Management Configuration Overview Page Screenshot

The page includes the following fields:

Object	Description
Mode	Indicates the access management mode operation. Possible modes are: **Enabled:** Enable access management mode operation. **Disabled:** Disable access management mode operation.
Delete	Check to delete the entry. It will be deleted during the next apply
VLAN ID	Indicates the VLAN ID for the access management entry
Start IP address	Indicates the start IP address for the access management entry
End IP address	Indicates the end IP address for the access management entry
HTTP/HTTPS	Indicates the host can access the switch from HTTP/HTTPS interface that the host IP address matched the entry
SNMP	Indicates the host can access the switch from SNMP interface that the host IP address matched the entry
Telnet/SSH	Indicates the host can access the switch from TELNET/SSH interface that the host IP address matched the entry

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

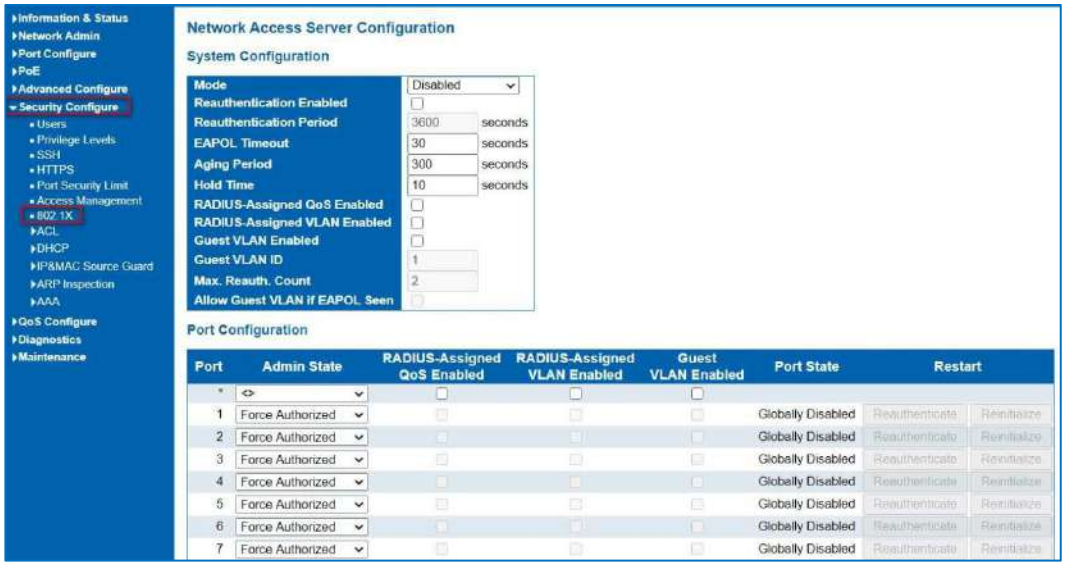
Apply : Click to apply changes.

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

7.7 802.1X Configuration

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the- middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets.
RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.
When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.
The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.
Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL)traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This switch supports 802.1X port-based authentication. In this page, user can configure 802.1X. After click "Security Configure" > "802.1X", followed screen will appear.



802.1X Configuration Screen

Configuration object and description is:

Object	Description
System Configuration	Here, user can enable or disable 802.1X or Reauthentication, as well as set Reauthentication Period / EAPOL Timeout / Aging Period / Hold Time
Port Configuration	Click drop-down menu to select a Admin State. Available options: Force Authorized, Force Unauthorized, 802.1X, Mac-based Auth.

Click "Save" to store and active settings.

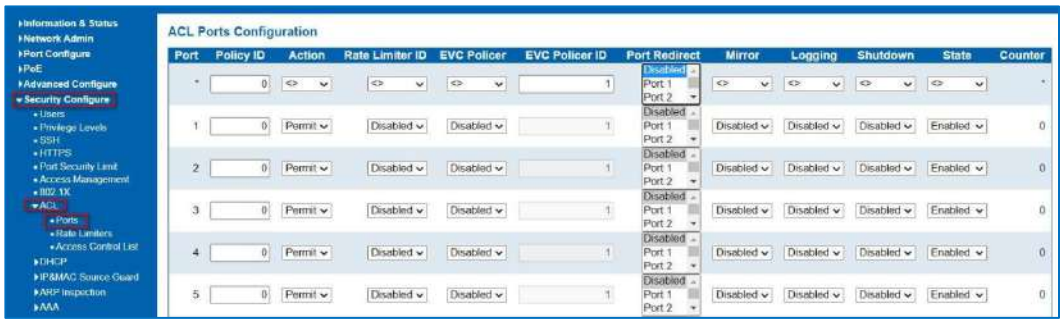
7.8 ACL Configuration

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.

7.8.1 ACL Ports Configure

After click ''Security Configure''>''ACL'' >''Ports'', followed screen will appear.



ACL Ports Configuration Screen

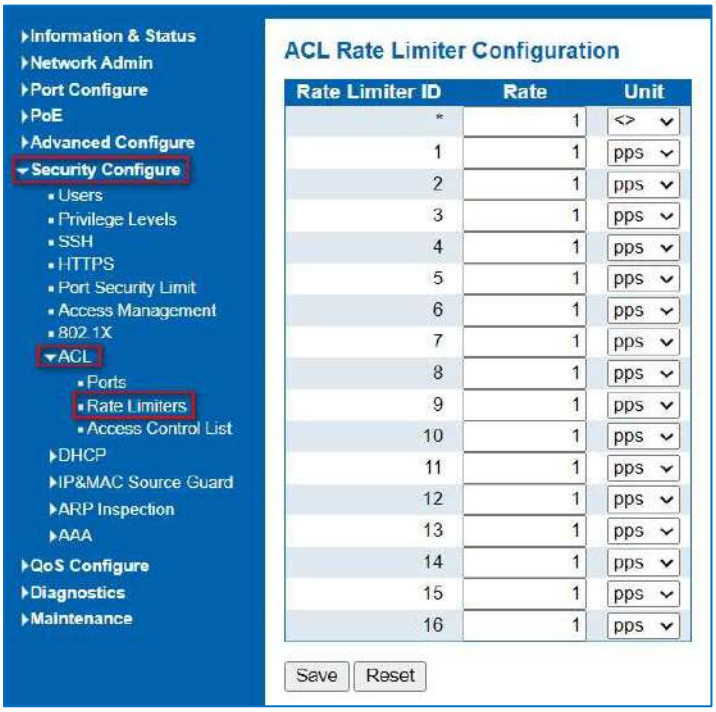
Configuration object and description is:

Object	Description
Action	There are 2 available options: Permit: that specific port allows data going through. Deny: that specific port forbid data going through.
Rate Limiter ID	Port's fixed Rate Limiter ID, please go to Rate Limiter Configuration for more details.
Port Redirect	Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".
Mirror	Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled".
Logging	Enabled or Disabled Log
Shut Down	Specify the port shut down operation of this port. The allowed values are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled. The default value is "Disabled". Note: The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).
State	Specify the port state of this port. The allowed values are: Enabled: To reopen ports by changing the volatile port configuration of the ACL user module. Disabled: To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".
Counter	Counts the number of frames that match this rule.

Click "Save" to store and active settings.

7.8.2 Rate limiter Configuration

User can make ACL Rate limiter configuration in this page. After click ''Security Configure''>''ACL'' >''Rate Limiter'', followed screen will appear.



ACL Rate Limiters Configuration Screen

Click "Save" to store and active settings.

7.8.3 Access Control List Configuration

User can make Access Control List Configuration in this page . After click ''Security Configure'' >''ACL'' >''Access Control List'', followed screen will appear.

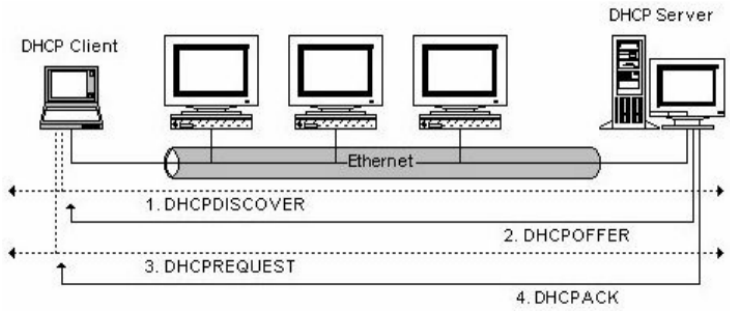
Access Control Limiters Configuration Screen

Click  button, to go to Access Control List, and edit it.

7.9 DHCP

DHCP protocol is widely used to dynamically allocate reusable network resources, such as IP address. A typical process of DHCP to obtain IP is as following:

DHCP Overview



DHCP Client sent DHCP DISCOVER message to DHCP Server, if Client did not receive respond from server within a period of time, it will resend DHCP DISCOVER message.
After received DHCP DISCOVER message, DHCP Server will assign sources (IP address for example) to client, and then send DHCP OFFER message to DHCP Client.
After received DHCP OFFER message, DHCP Client send DHCP REQUEST to ask for server lease, and notify the other servers that it has accepted this server to assign addresses.

After received DHCP REQUEST, server will verify whether resource can be allocated. If OK, it will send DHCP ACK message; If not OK, it will send DHCP NAK message. After received DHCP ACK message, start using the source which server assigned. If received DHCP NAK, DHCP Client will resend DHCP DISCOVER message.

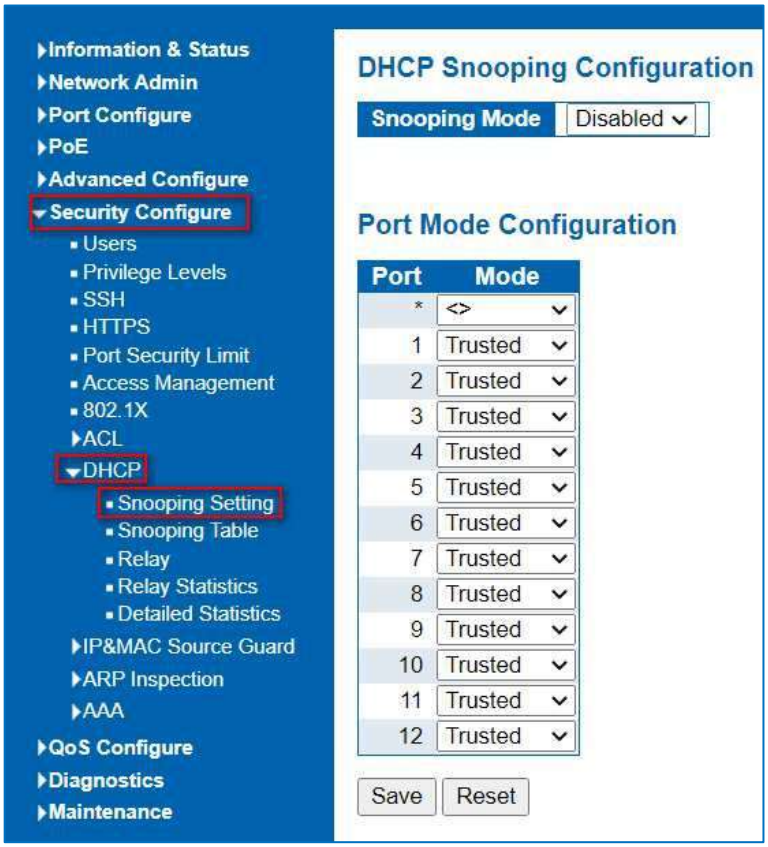
About DHCP Snooping

The addresses assigned to DHCP clients on insecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping. DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.
Command Usage

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or firewall When DHCP snooping is enabled globally and enabled on a VLAN interface, DHCP messages received on an entrusted interface from a device not listed in the DHCP snooping table will be dropped
- Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.
- When DHCP snooping is enabled, DHCP messages entering an entrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- If a DHCP packet from a client passes the filtering criteria, it will only be forwarded to trusted ports in the same VLAN
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and entrusted ports in the same VLAN.
- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

7.9.1 Snooping Setting

After click ''Security Configure'' > ''DHCP '' > ''Snooping Setting'', following screen will appear.



DHCP Snooping Configuration Screen

Configuration object and description is:

Object	Description
DHCP Snooping Mode	Click drop-down menu to enable or disable DHCP Snooping
Port 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.

Click "Save" to store and active settings.

7.9.2 Snooping Table

This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page. The Dynamic DHCP Snooping Table screen in Figure 6-9-2 appears.

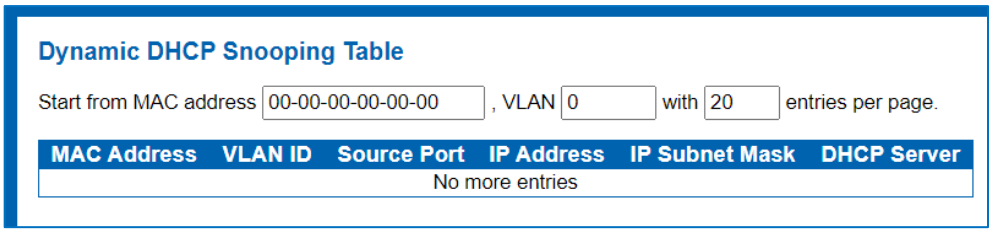


Figure 7-9-2 Dynamic DHCP Snooping Table Screen Page Screenshot

Configuration object and description is:

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

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

Refresh : Refreshes the displayed table starting from the input fields

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

>> : To start over

7.9.3 DHCP relay

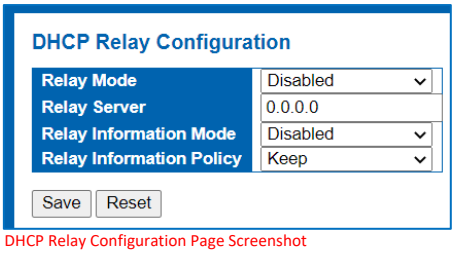
Configure **DHCP Relay** on this page. DHCP Relay is used to forward and transfer DHCP messages between the clients and the server when they are not on the same subnet domain.
The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically, the option works by setting two sub-options:

Circuit ID (option 1)

Remote ID (option 2)

The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.
The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes representing the VLAN ID. The parameter of "module_id" is the third byte for the module ID. The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value equals the DHCP relay agent's MAC address. The DHCP Relay Configuration screen in Figure 6-9-3 appears.



DHCP Relay Configuration Page Screenshot

Configuration object and description is:

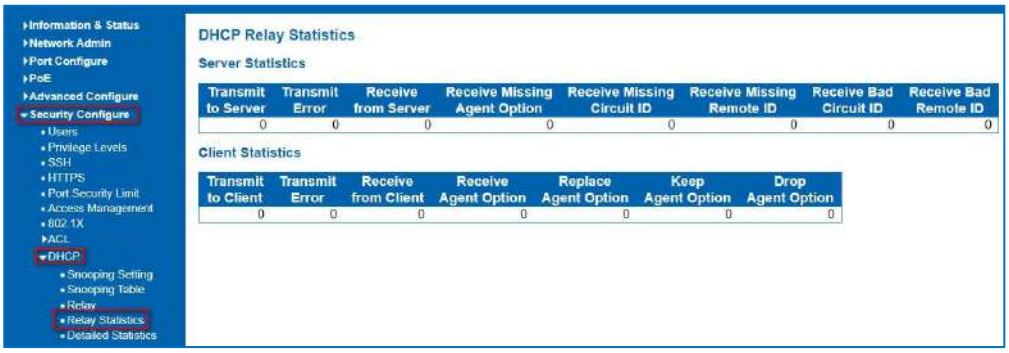
Object	Description
Relay mode	Indicates the DHCP relay mode operation. Possible modes are: ➢ **Enabled:** Enable DHCP relay mode operation. When enabling DHCP relay mode operation, the agent forwards and transfers DHCP messages between the clients and the server when they are not on the same subnet domain. And the DHCP broadcast message won't flood for security considered. ➢ **Disabled:** Disable DHCP relay mode operation
Relay Server	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when they are not on the same subnet domain.
Relay Information Mode	Indicates the DHCP relay information mode option operation. Possible modes are: ➢ **Enabled:** Enable DHCP relay information mode operation. When enabling DHCP relay information mode operation, the agent inserts specific information (option82) into a DHCP message when forwarding to DHCP server and removing it from a DHCP message when transferring to DHCP client. It only works under DHCP relay operation mode enabled. ➢ **Disabled:** Disable DHCP relay information mode operation
Relay Information Policy	Indicates the DHCP relay information option policy. When enabling DHCP relay information mode operation, if agent receives a DHCP message that already contains relay agent information. It will enforce the policy. And it only works under DHCP relay information operation mode enabled. Possible policies are: ➢ **Replace:** Replace the original relay information when receiving a DHCP message that already contains it. ➢ **Keep:** Keep the original relay information when receiving a DHCP message that already contains it. ➢ **Drop:** Drop the package when receiving a DHCP message that already ➢ contains relay information.

Save : Click to apply changes.

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

7.9.4 DHCP Relay Statistics

This page provides statistics for DHCP relay. The DHCP Relay Statistics screen in Figure 7-9-3-4 appears.



DHCP Relay Statistics Page Screenshot

Configuration object and description is:

Server Statistics

Object	Description
Transmit to Server	The packets number that relayed from client to server.
Transmit Error	The packets number that erroneously sent packets to clients.
Receive from Server	The packets number that received packets from server.
Receive Missing Agent Option	The packets number that received packets without agent information options.
Receive Missing Circuit ID	The packets number that received packets whose the Circuit ID option was missing.
Receive Missing Remote ID	The packets number that received packets whose Remote ID option was missing.
Receive Bad Circuit ID	The packets number whose the Circuit ID option did not match known circuit ID.
Receive Bad Remote ID	The packets number who's the Remote ID option did not match known Remote ID.

Client Statistics

Object	Description
Transmit to Client	The packets number that relayed packets from server to client.
Transmit Error	The packets number that erroneously sent packets to servers.
Receive from Client	The packets number that received packets from server.
Receive Agent Option	The packets number that received packets with relay agent information option.
Replace Agent Option	The packets number that replaced received packets with relay agent information option.
Keep Agent Option	The packets number that kept received packets with relay agent information option.
Drop Agent Option	The packets number that dropped received packets with relay agent information option.
Transmit to Client	The packets number that relayed packets from server to client.

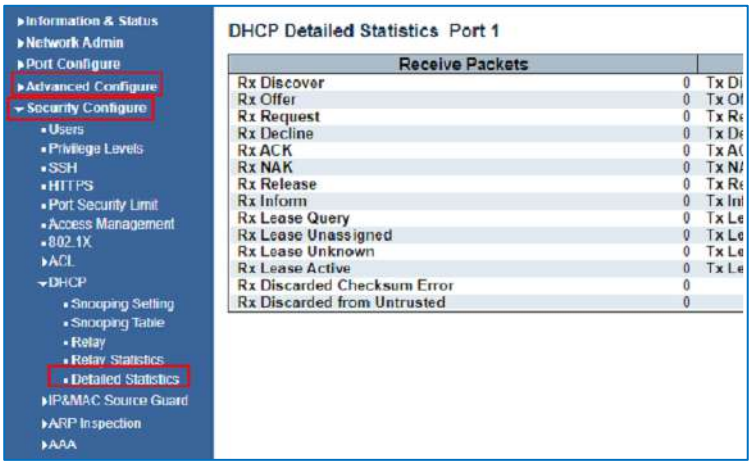
Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh : Click to refresh the page immediately.

Clear : Clears all statistics.

7.9.5 DHCP Detailed Statistics

After click "Advanced Configure" > "Security Configure" > “DHCP" > "Detailed Statistics" followed screen will appear as:



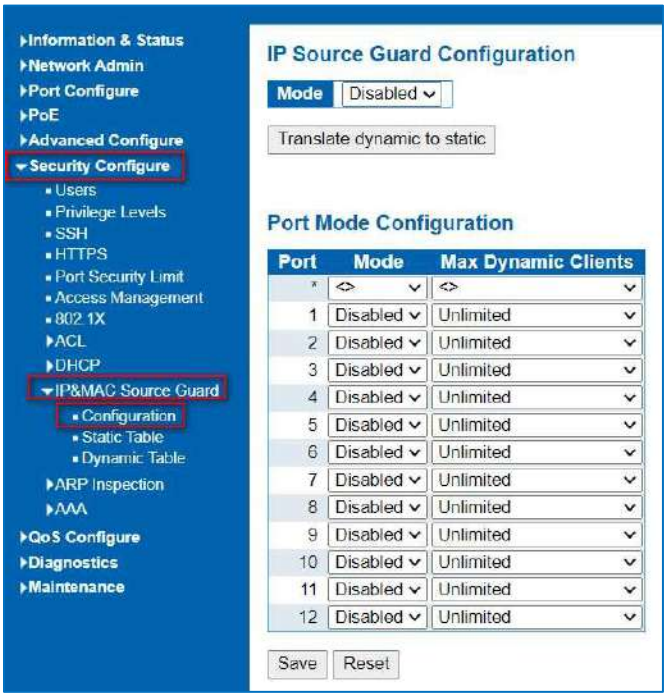
DHCP Detailed Statistics Screenshot

7.10 IP&MAC Source Guard

IP&MAC Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on 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.

7.10.1 Port Configuration

In this page, user can make IP&MAC Source Guard Port Configuration. After click ''Security Configure''>''IP & MAC Source Guard'' >''Configuration'', followed screen will appear.



IP&MAC Guard-Port Configuration Screen

Configuration object and description is:

Object	Description
Global Mode	Click drop-down menu to enable or disable Global IP&MAC Source Guard function
Port Mode	Click drop-down menu to enable or disable the IP&MAC Source Guard function for corresponding port.
Max Dynamic Clients	Click drop-down menu to select Max Dynamic Clients. Available options: Unlimited, 0, 1, 2.

Click "Save" to store and active settings.

7.10.2 Static Table

In this page, user can manually set Static Table of IP&MAC Guard to fulfill controlling function to port. After click ''Security Configure''>''IP&MAC Source Guard'' >''Static Table'', followed screen will appear.

Static Table Configuration Screen

Configuration object and description is:

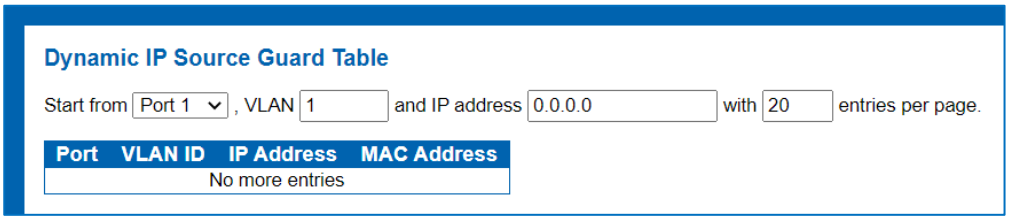
Object	Description
Port	Click drop-down menu to select which port should be fixed.
VLAN	Type VLAN ID that should be fixed to
IP Address	Type IP Address that should be fixed to
MAC Address	Type Mac Address that should be fixed to

Click ''Add New Entry'' button to create a new record.

Click "Save" to store and active settings.

7.10.3 Dynamic Table

This page provides Static IP Source Guard Table. The Static IP Source Guard Table screen in Figure 6-10-3 appears.



Static IP Source Guard Table Screen Page Screenshot

Configuration object and description is:

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

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

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

<< : Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

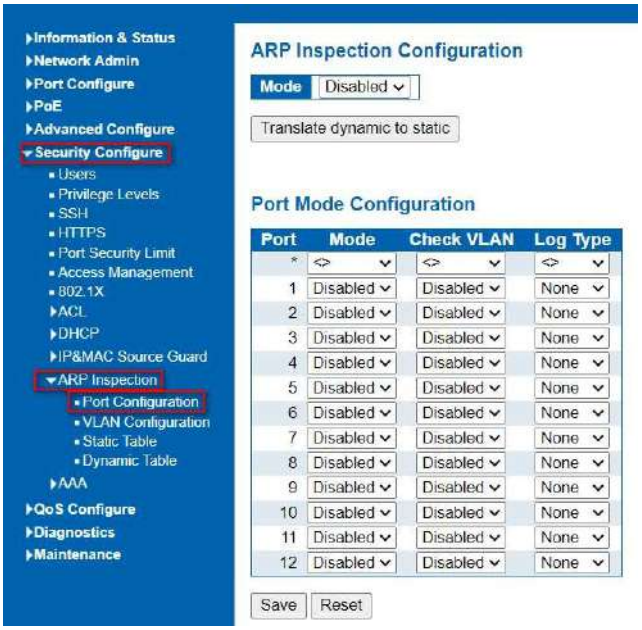
>> : Updates the table, starting with the entry after the last entry currently displayed.

7.11 ARP Inspection

Dynamic ARP Inspection (DAI) 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 DUT. A Dynamic ARP prevents the untrust ARP packets based on the DHCP Snooping Database. This page provides ARP Inspection related configuration.

7.11.1 Port Configuration

User can make port configuration in this page. After click ''Security Configure''>''ARP Inspection'' >''Port Configuration'', followed screen will appear.



ARP Inspection Port Configuration Screen

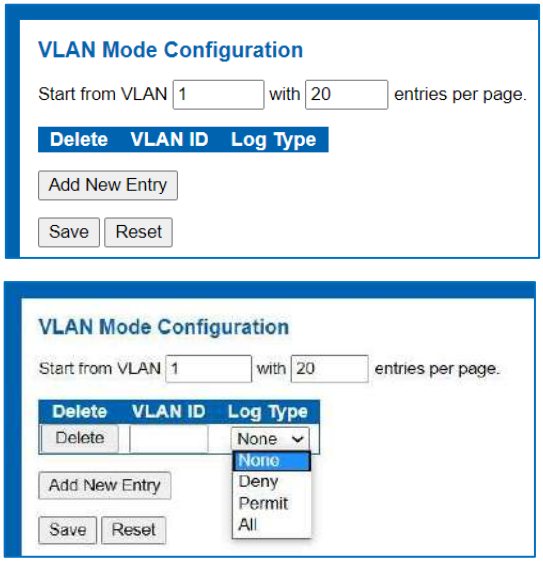
Configuration object and description is:

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

Click "Save" to store and active settings.

7.11.2 VLAN Configuration

After click ''Security Configure''>''ARP Inspection'' >''VLAN Configuration'', followed screen will appear.



ARP Inspection VLAN Configuration Screen

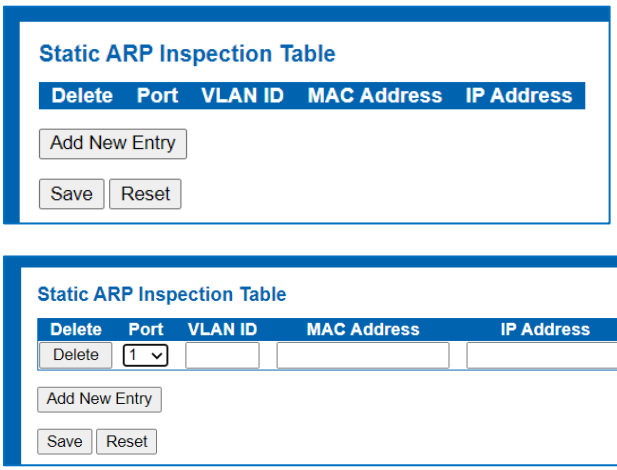
Configuration object and description is:

Object	Description
VLAN ID	Indicates the ID of this particular VLAN
Log Type	Click drop-down menu to enable or disable port-based ARP Inspection. Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting. Possible types are: None: Log nothing. Deny: Log denied entries. Permit: Log permitted entries. ALL: Log all entries.

Click ''Add New Entry'' button to create a new record of VLAN configuration. Click "Save" to store and active settings.

7.11.3 Static Table

User can manually configure ARP Inspection Static Table to control port. After click ''Security Configure''>''ARP Inspection'' >''Static Table'', followed screen will appear.



Static Table Configuration Screen

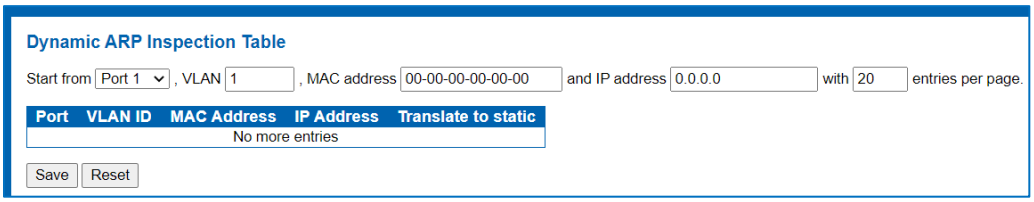
Configuration object and description is:

Object	Description
Port	Click drop-down menu to select which port should be fixed.
VLAN	Type VLAN ID that should be fixed to
IP Address	Type IP Address that should be fixed to
MAC Address	Type Mac Address that should be fixed to

Click ''Add New Entry'' button to create a new record. Click "Save" to store and active settings.

7.11.4 Dynamic table

After click ''Security Configure''>''ARP Inspection'' >''Dynamic Table', followed screen will appear. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. The Dynamic ARP Inspection Table screen in Figure –11-4 appears.



Dynamic ARP Inspection Table Screenshot

Navigating the ARP Inspection Table

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

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

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

Configuration object and description is:

Object	Description
Port	The port number for which the status applies. Click the port number to see the status for this particular port.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
IP Address	The IP address of the entry.

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

Refresh : Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

<< : Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

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

7.12 AAA

This section is to control the access to the Managed Switch, including the user access and management control. The Authentication section contains links to the following main topics:

User Authentication
IEEE 802.1X Port-based Network Access Control MAC-based Authentication
Overview of 802.1X (Port-Based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the- middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as **EAPOL (EAP Over LANs)** frames. **EAPOL** frames encapsulate **EAP PDU**s (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like **MD5-Challenge, PEAP,** and **TLS.** The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.
When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Overview of MAC-based Authentication
Unlike 802.1X, MAC-based authentication is not a standard, but merely a best- practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.
When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.
The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported. The 802.1X and MAC-Based Authentication configuration consists of two sections, a system- and a port-wide.

Overview of User Authentication

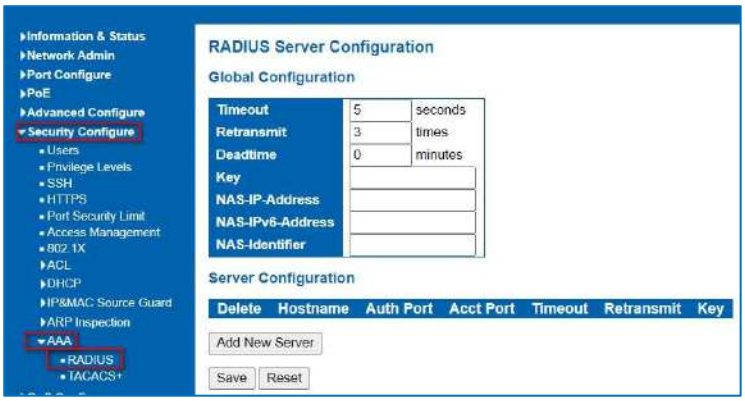
It is allowed to configure the Managed Switch to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and Web browser. This Managed Switch provides secure network management access using the following options:

- **Remote Authentication Dial-in User Service (RADIUS)**
- **Terminal Access Controller Access Control System Plus (TACACS+)**
- **Local user name and Privilege Level control**

RADIUS and **TACACS+** are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An authentication server contains a database of multiple user name / password pairs with associated privilege levels for each user that requires management access to the Managed Switch.

7.12.1 RADIUS

This page allows you to configure the RADIUS Servers. The RADIUS Configuration screen in Figure 6-12-1 appears.



RADIUS Server Configuration Page Screenshot

The page includes the following fields:

Global Configuration

These setting are common for all of the RADIUS Servers
Configuration object and description is:

Object	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
Retransmit	Retransmit is the number of times, in the range from 1 to 1000; a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit, it is considered to be dead.
Dead Time	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Key	The secret key - up to 63 characters long - shared between the RADIUS server and the switch.
NAS-IP-Address	The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets.
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request. If this field is left blank, the IP address of the outgoing interface is used.
NAS-IPv6-Address	The IPv6 address to be used as attribute 95 in RADIUS Access- Request packets. If this field is left blank, the IP address of the outgoing interface is used.

Server Configuration
The table has one row for each RADIUS Server and a number of columns, which are:

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

Add New Server : Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.

Save : Click to save changes.

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

7.12.2 TACACS+

This page allows you to configure the TACACS+ Servers. The TACACS+ Configuration screen in Figure 6-12-1 appears.

TACACS+ Server Configuration Page Screenshot

The page includes the following fields:

Global Configuration

These setting are common for all of the TACACS+ Servers.

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

Server Configuration

The table has one row for each TACACS+ server and a number of columns, which are:

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

Add New Server : Click to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.

Save : Click to save changes.

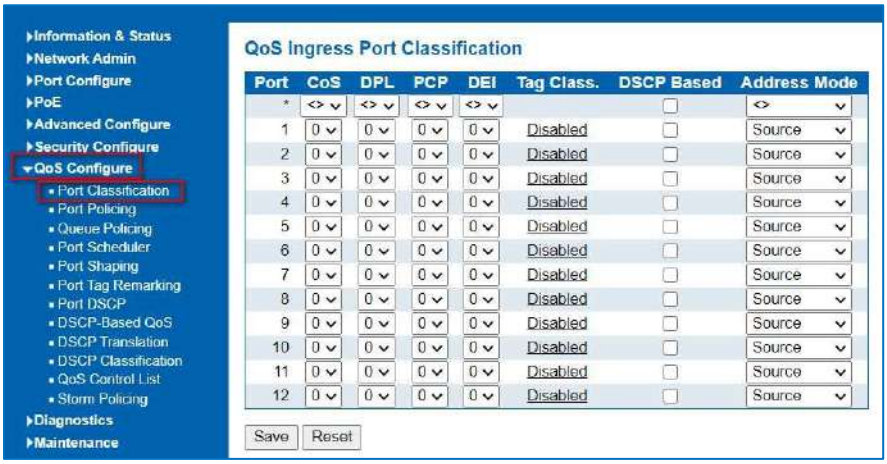
Reset : Click to undo any changes made locally and revert to previously saved values.

Chapter 8: QoS Configure

8.1 QoS Port Classification

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol- specific, time critical, and file-backup traffic. This function n can not only reserve bandwidth, but also limit other traffic that is not so important.

After Click "QoS Configure" > "Port Classification", followed screen will appear.



Port Classification Configuration Screen

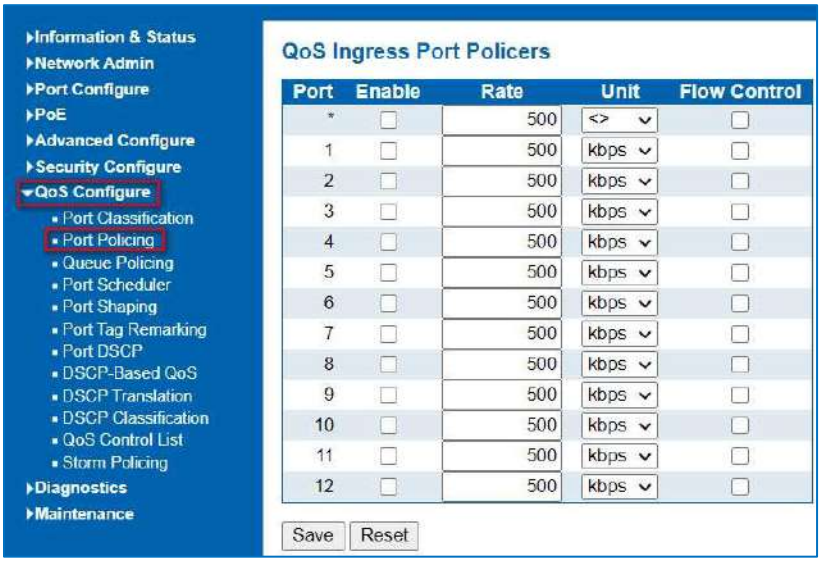
Configuration object and description is:

Object	Description
CoS	Controls the default class of service, ranging from 0 (lowest) to 7 (highest). All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority The classified CoS can be overruled by a QCL entry. Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.
DPL	Controls the default drop precedence level. All frames are classified to a drop precedence level. The classified DPL can be overruled by a QCL entry.
PCP	Controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise, the frame is classified to the default PCP value.
DEI	Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise, the frame is classified to the default DEI value.
Address Mode	The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are: Source: Enable SMAC/SIP matching. Destination: Enable DMAC/DIP matching.

Click "Save" to store and active settings.

8.2 Port Policing

After Click "QoS Configure" > "Port Policing", followed screen will appear.



Port Policing Configuration Screen

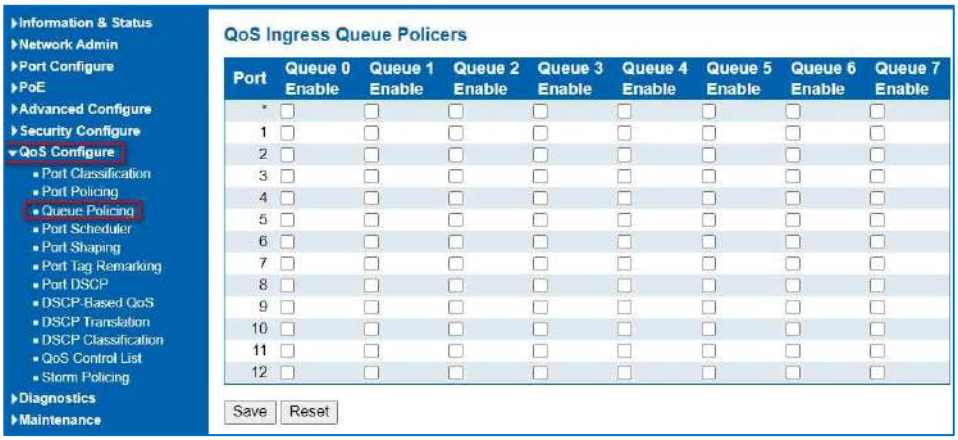
Configuration object and description is：

Object	Description
Enabled	Check the box to enable Port Policing.
Rate	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps".
Unit	Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Click "Save" to store and active settings.

8.3 Queue Policing

This page allows you to configure the Queue Policer settings for all switch ports. The Queue Policing screen in Figure 8-3 appears.



QoS Ingress Port Classification Page Screenshot

The page includes the following fields:

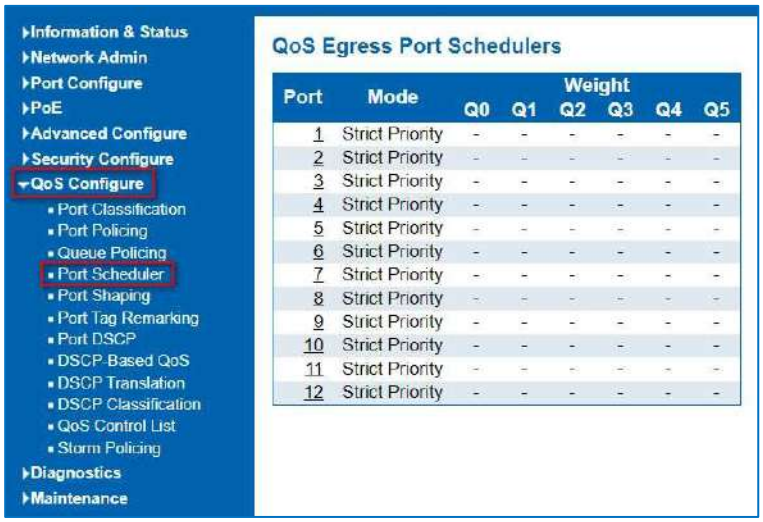
Object	Description
Port	The port number for which the configuration below applies.
Enable (E)	Enable or disable the queue policer for this switch port.
Rate	Controls the rate for the queue policer. This value is restricted to 25-13128147 when "Unit" is kbps, and 1-13128 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if at least one of the queue policers are enabled.
Unit	Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if at least one of the queue policers are enabled.

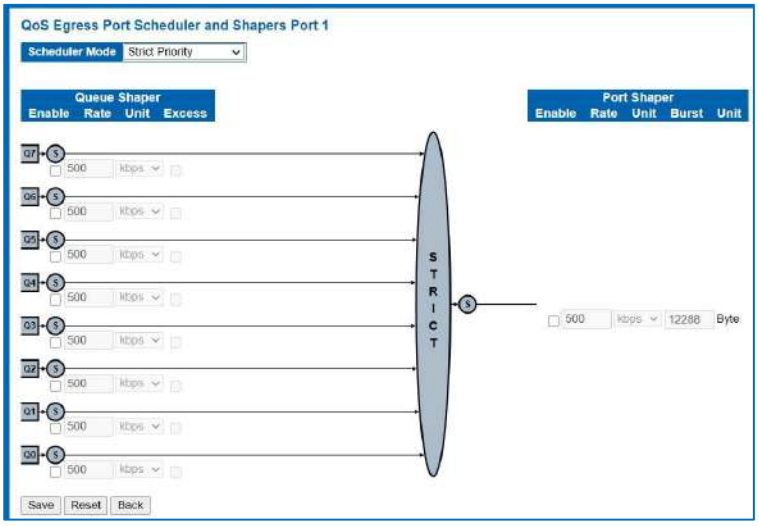
Save : Click to apply changes.

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

8.4 Port Scheduler

The Port Scheduler and Shapers for a specific port are configured on this page. The QoS Egress Port Schedule and Shaper screen in Figure 8-4 appears.





QoS Egress Port Schedule and Shapers Page Screenshot

Object	Description
Schedule Mode	Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
Queue Shaper Enable	Controls whether the queue shaper is enabled for this queue on this switch port.
Queue Shaper Rate	Controls the rate for the queue shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps". The default value is 500.
Queue Shaper Unit	Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".
Queue Shaper Excess	Controls whether the queue is allowed to use excess bandwidth.
Queue Scheduler Weight	Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted". The default value is "17".
Queue Scheduler Percent	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable	Controls whether the port shaper is enabled for this switch port.
Port Shaper Rate	Controls the rate for the port shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps". The default value is 500.
Port Shaper Unit	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

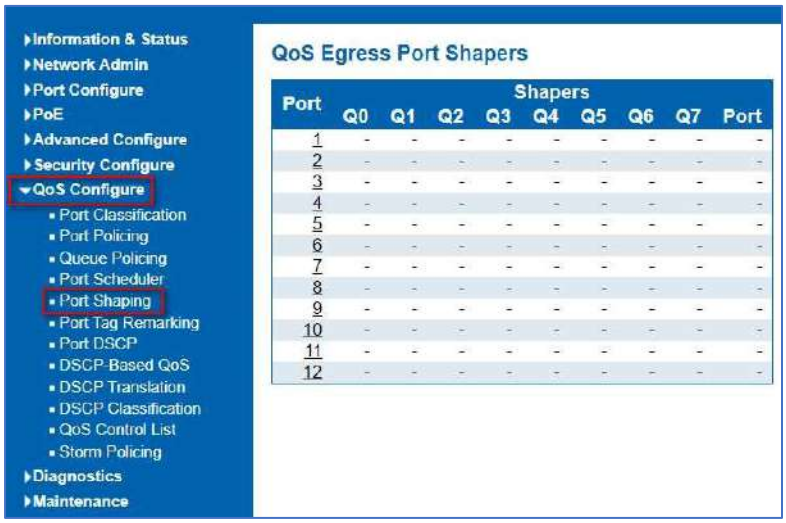
Save : Click to apply changes.

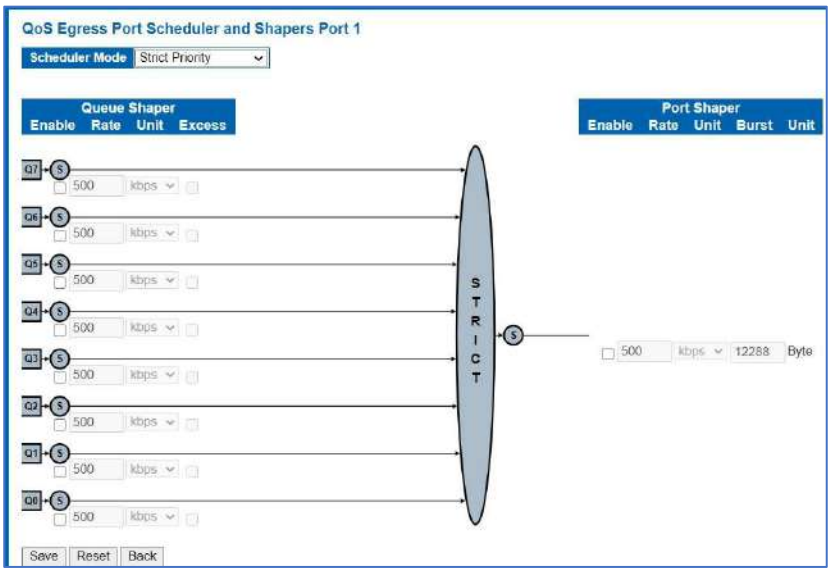
Reset : Click to undo any changes made locally and revert to previously saved values.

Back : Click to undo any changes made locally and return to the previous page.

8.5 Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.. The Port shaping screen in Figure 8.5 appears.





QoS Egress Port Schedule and Shapers Page Screenshot

The page includes the following fields:

Object	Description
Schedule Mode	Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
Queue Shaper Enable	Controls whether the queue shaper is enabled for this queue on this switch port.
Queue Shaper Rate	Controls the rate for the queue shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1- 13200 when the "Unit" is "Mbps". The default value is 500.
Queue Shaper Unit	Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".
Queue Shaper Excess	Controls whether the queue is allowed to use excess bandwidth.
Queue Scheduler Weight	Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted". The default value is "17".
Queue Scheduler Percent	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
Port Shaper Enable	Controls whether the port shaper is enabled for this switch port.
Port Shaper Rate	Controls the rate for the port shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps". The default value is 500.
Port Shaper Unit	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

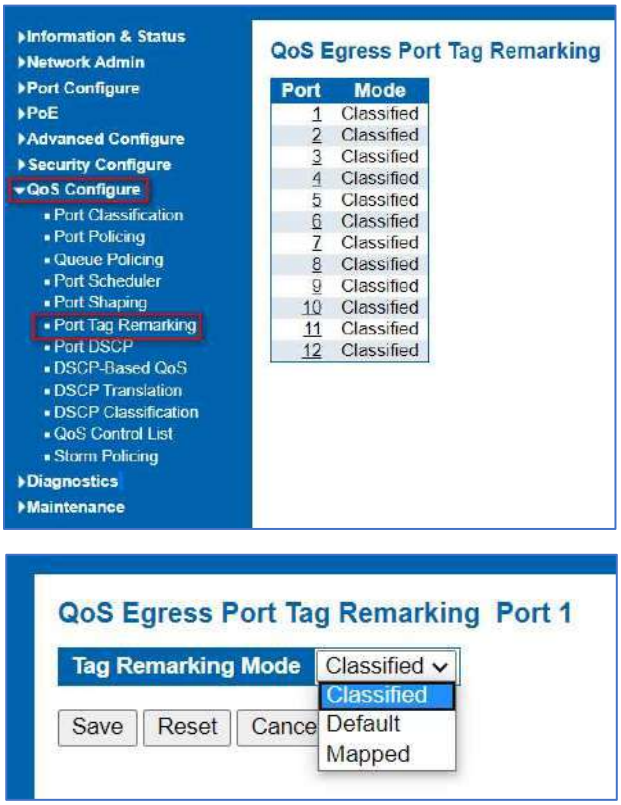
Save : Click to apply changes.

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

Back : Click to undo any changes made locally and return to the previous page.

8.6 Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports. The Port tag remarking screen in Figure 8.6 appears.



Port Tag Remarking Page Screenshot

The page includes the following fields:

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

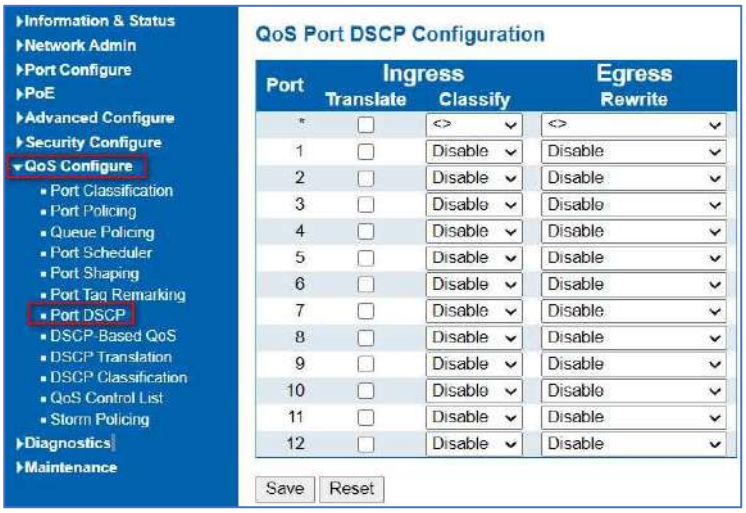
Save : Click to apply changes.

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

Back : Click to undo any changes made locally and return to the previous page.

8.7 Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports. The Port DSCP screen in Figure 8.7 appears.



QoS Port DSCP Configuration Page Screenshot

The page includes the following fields:

Object	Description
Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
Ingress	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: **Translate Classify**
Translate	To Enable the Ingress Translation, click the checkbox.
Classify	Classification for a port have 4 different values. ➢ **Disable:** No Ingress DSCP Classification. ➢ **DSCP=0:** Classify if incoming (or translated if enabled) DSCP is 0. ➢ **Selected:** Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSP.
Egress	Port Egress Rewriting can be one of - ➢ **Disable:** No Egress rewrite. ➢ **Enable:** Rewrite enable without remapped. ➢ **Remap DP Unaware:** DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. ➢ **Remap DP Aware:** DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP. ➢ **Translation**->Egress Remap DP1' table.

Save : Click to apply changes.

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

8.8 DSCP-based QoS

This page allows you to configure the basic QoS DSCP-based QoS Ingress Classification settings for all switches. The DSCP-based QoS screen in Figure 8.8 appears.

DSCP-based QoS Ingress Classification Page Screenshot

The page includes the following fields:

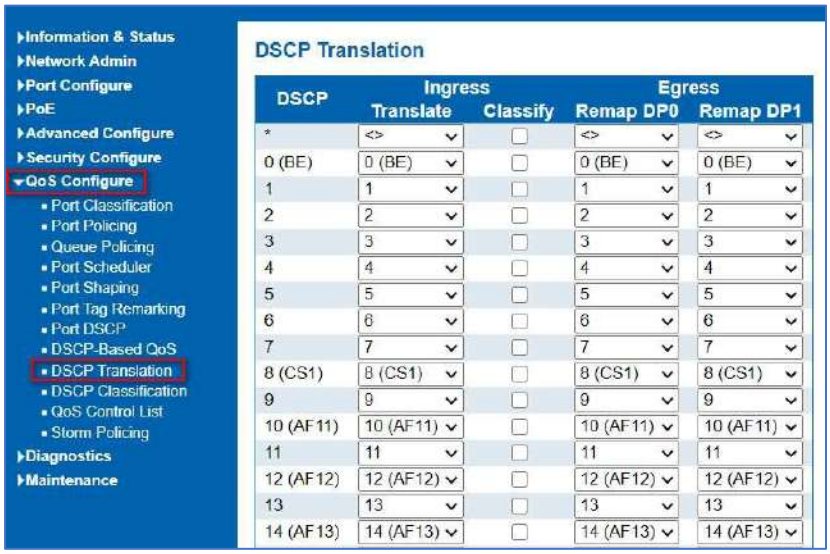
Object	Description
DSCP	Maximum number of supported DSCP values are 64.
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS Class	QoS Class value can be any of (0-7)
DPL	Drop Precedence Level (0-1)

Save : Click to apply changes.

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

8.9 DHCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress. The DSCP Translation screen in Figure 8-9 appears.



DSCP Translation Page Screenshot

The page includes the following fields:

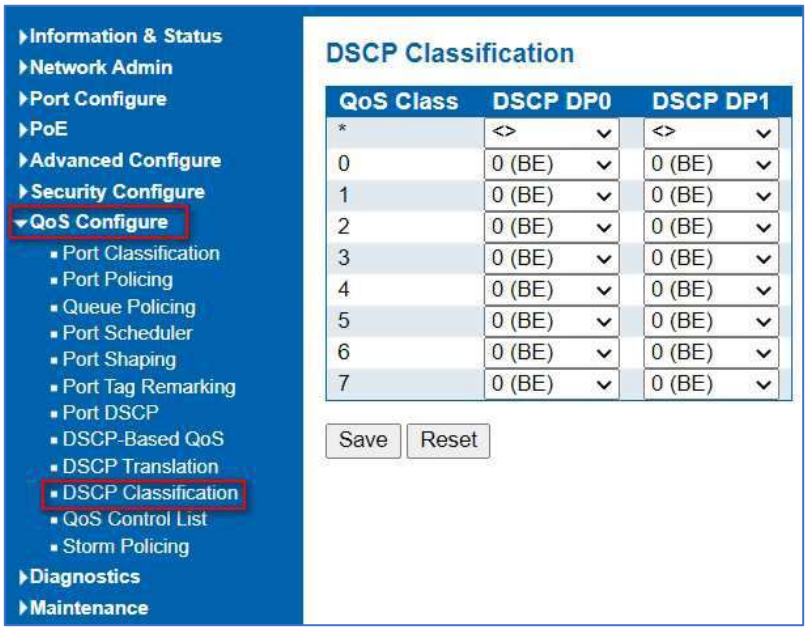
Object	Description
DSCP	Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
Ingress	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation – ➢ **Translate** ➢ **Classify**
Translate	DSCP at Ingress side can be translated to any of (0-63) DSCP values.
Classify	Click to enable Classification at Ingress side.
Egress	There is following configurable parameter for Egress side - **Remap**
Remap DP	Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

Save : Click to apply changes.

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

8.10 DHCP Classification

This page allows you to map DSCP value to a QoS Class and DPL value. The DSCP Classification screen in Figure 8-10 appears.



DSCP Translation Page Screenshot

The page includes the following fields:

Object	Description
QoS Class	Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to followed parameters.
DPL	Actual Drop Precedence Level.
DSCP	Select DSCP value (0-63) from DSCP menu to map DSCP to corresponding QoS Class and DPL value

Save : Click to apply changes.

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

8.11 QoS Control

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

8.11.1 QoS Control List

Click on the lowest plus sign to add a new QCE to the list. The QoS Control List screen in Figure 8.11 appears.

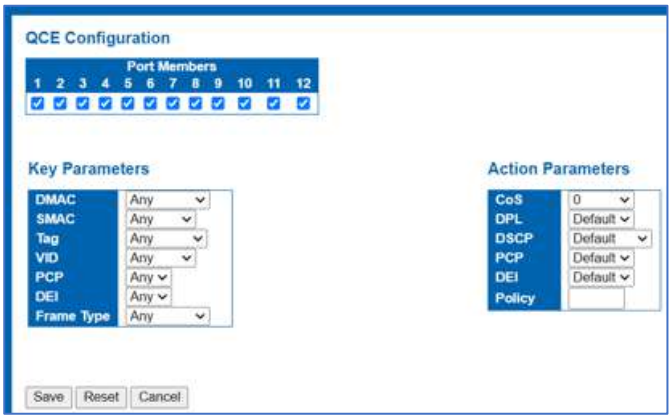
QoS Control List Configuration Page Screenshot

The page includes the following fields:

Object	Description
QCE#	Indicates the index of QCE.
Port	Indicates the list of ports configured with the QCE.
DMAC	Specify the type of Destination MAC addresses for incoming frame. Possible values are: **Any:** All types of Destination MAC addresses are allowed. **Unicast:** Only Unicast MAC addresses are allowed. **Multicast:** Only Multicast MAC addresses are allowed. **Broadcast:** Only Broadcast MAC addresses are allowed. The default value is 'Any'.
SMAC	Displays the OUI field of Source MAC address, i.e. first three octet (byte) of MAC address.
Tag Type	Indicates tag type. Possible values are: **Any:** Match tagged and untagged frames. **Untagged:** Match untagged frames. **Tagged:** Match tagged frames. The default value is 'Any'
VID	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
PCP	Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
DEI	Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or'Any'.
Frame Type	Indicates the type of frame to look for incoming frames. Possible frame types are: ➢ **Any:** The QCE will match all frame type. ➢ **Ethernet:** Only Ethernet frames (with Ether Type 0x600- 0xFFFF) are allowed. ➢ **LLC:** Only (LLC) frames are allowed. ➢ **SNAP:** Only (SNAP) frames are allowed. ➢ **IPv4:** The QCE will match only IPV4 frames. ➢ **IPv6:** The QCE will match only IPV6 frames.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP. ➢ **Class:** Classified QoS class. ➢ **DPL:** Classified Drop Precedence Level. ➢ **DSCP:** Classified DSCP value.
Modification Buttons	You can modify each QCE in the table using the following buttons: ⊕: Inserts a new QCE before the current row. : Edits the QCE. ⊕: Moves the QCE up the list. : Moves the QCE down the list. : Deletes the QCE. : The lowest plus sign adds a new entry at the bottom of the list of QCL.

8.11.2 QoS Control Entry Configuration

The QCE Configuration screen in Figure 8-11 appears.



QCE Configuration Page Screenshot

The page includes the following fields:

Object	Description
Port Members	Check the checkbox button in case you what to make any port member of the QCL entry. By default, all ports will be checked
Key Parameters	Key configuration are described as below: ➢ **DMAC Type** Destination MAC type: possible values are unicast (UC), multicast (MC), broadcast (BC) or 'Any' ➢ **SMAC** Source MAC address: 24 MS bits (OUI) or 'Any' ➢ **Tag** Value of Tag field can be 'Any', 'Untag' or 'Tag' ➢ **VID** Valid value of VLAN ID can be any value in the range 1- 4095 or 'Any'; user can enter either a specific value or a range of VIDs ➢ **PCP** Priority Code Point: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any' ➢ **DEI** Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any' ➢ **Frame Type** Frame Type can have any of the following values 1. **Ethernet** 2. **LLC** 3. **SNAP** 4. **IPv4** 5. **IPv6** Note: all frame types are explained below.
Any	Allow all types of frames.
EtherType	**Ethernet Type** Valid Ethernet type can have value within 0x600- 0xFFFF or 'Any' but excluding 0x800(IPv4) and 0x86DD(IPv6), default value is 'Any'.
LLC	➢ SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any' ➢ DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any' ➢ Control Address Valid Control Address can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'
SNAP	**PID** Valid PID(a.k.a Ethernet type) can have value within 0x00- 0xFFFF or 'Any', default value is 'Any'
IPv4	**Protocol** IP protocol number: (0-255, TCP or UDP) or 'Any' Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero **DSCP** Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43 **IP Fragment** IPv4 frame fragmented option: yes|no|any

	Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP **Dport** Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP
IPv6	**Protocol** IP protocol number: (0-255, TCP or UDP) or 'Any' Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits **DSCP** Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'. **DSCP** values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43 **Sport Source** TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP **Dport** Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP
Action Parameters	**Class** QoS class: (0-7) or 'Default'. **DPL** Valid Drop Precedence Level can be (0-3) or 'Default'. **DSCP** Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11- AF43) or 'Default'. 'Default' means that the default classified value is not modified by this QCE.

Save : Click to apply changes.

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

Cancel : Return to the previous page without saving the configuration change.

8.11.3 QCL Status

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

8.12 Storm Policing Configuration

After Click "QoS Configure" > "Storm Policing", followed screen will appear.

Storm Policing Configuration Screen

Configuration object and description is:

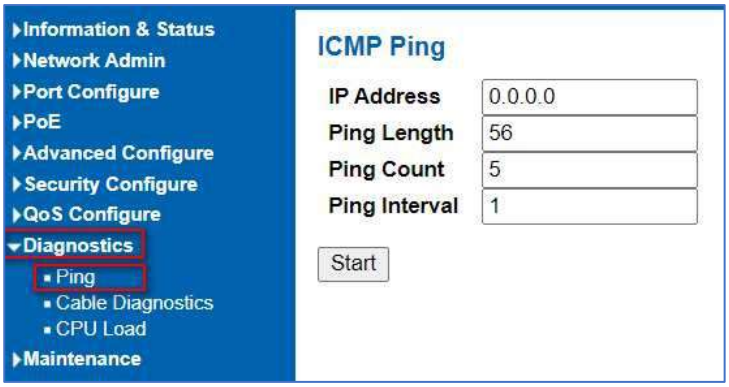
Object	Description
Frame Type	This switch supports 3 kinds of Frame Type: Unicast, Unknown Multicast, Broadcast.
Enable	Check the box to enable Storm Control.
Rate(pps)	The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K..

Chapter 9: Diagnostics

9.1 Ping test

Ping is a little program that can issue ICMP Echo packets to the IP address you defined. Destination node will respond to those packets sent from switch. So, Ping test is to troubleshoot IP connectivity issues.

After click ''Diagnostics ''>''Ping'', followed screen appear.



Ping Test Screen

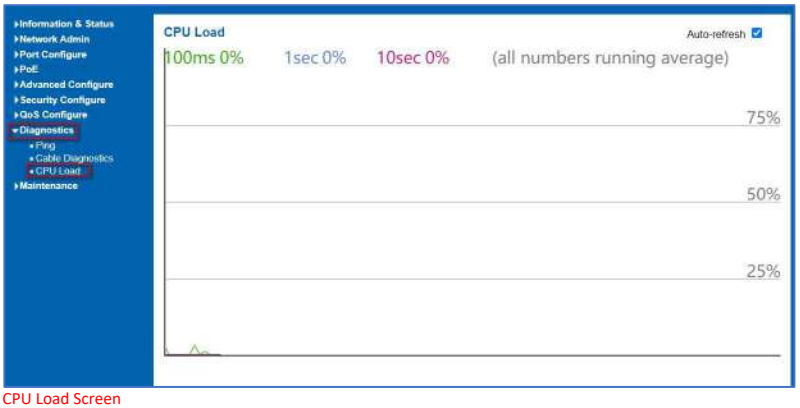
Configuration object and description is:

Object	Description
IP Address	The destination IP Address that needed to Ping
Ping Length	Input a number between 1 and 1452. Default: 56
Ping Count	The times for inputting Ping IPv4 address or IPv6 address (Number of echo requests to send). User can input a number between 1 and 60.
Ping Interval	Interval time for Ping (Send interval for each ICMP packet)

Click ''Start'' button to start Ping testing.

9.2 CPU Load

This page shows percent of CPU load. After click ''Diagnostics''>''CPU Load'', followed screen will appear.



CPU Load Screen

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 page is for restarting switch. After click ''Maintenance ''>''Restart Device'', followed screen will appear.

Restart Device Screen

Please click ''Yes'' to restart the switch.

10.2 Factory Defaults

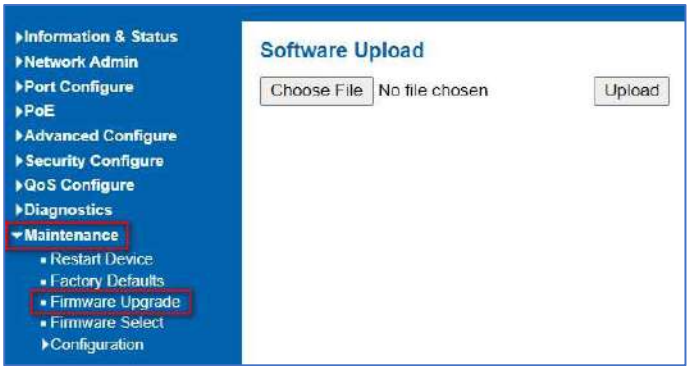
This page is for making all settings to factory defaults. After click ''Maintenance ''>''Factory Defaults'', followed screen will appear.

Factory Defaults Screen

Please click ''Yes'' to reset the configuration to Factory Defaults.

10.3 Firmware Update

This page is for upgrading system firmware. After click ''Maintenance ''>''Firmware Upgrade'', followed screen will appear.

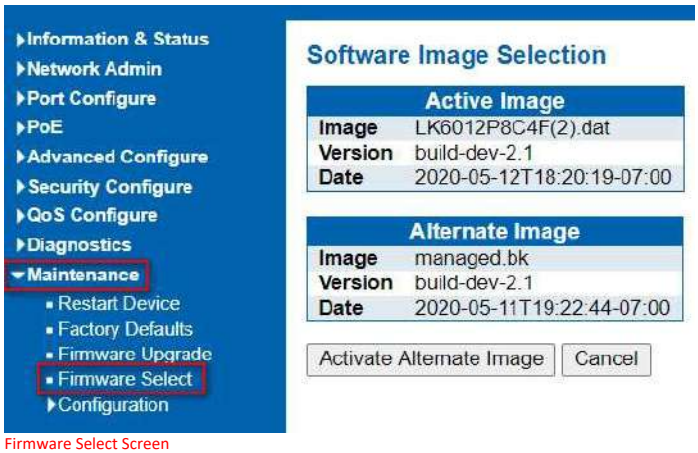


Firmware Upgrade Screen

Please click ''Browse'' to select the firmware that needed to upgrade. And then click ''Upload '' to start upgrading.

10.4 Firmware Select

s page provides information about the active and alternate (backup) firmware images in the device and allows you to revert to the alternate image. The web page displays two tables with information about the active and alternate firmware images. After click ''Maintenance ''>''Firmware Upgrade'', followed screen will appear.



Firmware Select Screen

Configuration object and description is:

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

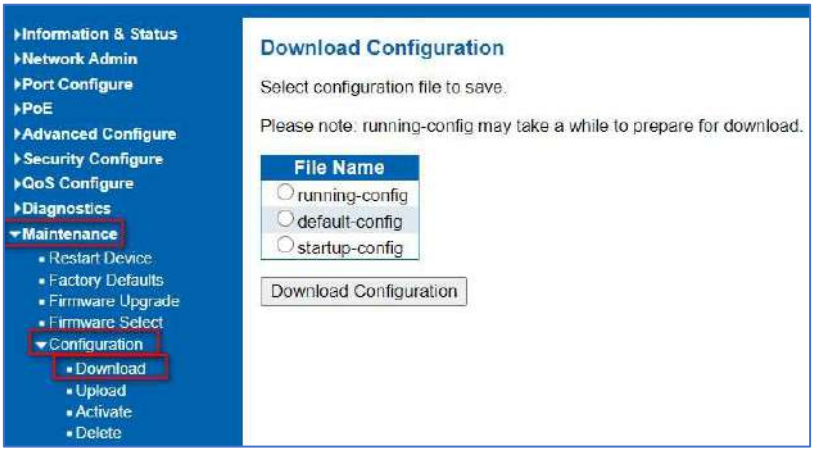
: Click to use the alternate image. This button may be disabled depending on system state.

10.5 Configuration

In this page, user can download, upload, activated or delete configuration files.

10.5.1 Download Configuration File

After click ''Maintenance ''>''Download'', followed screen will appear.

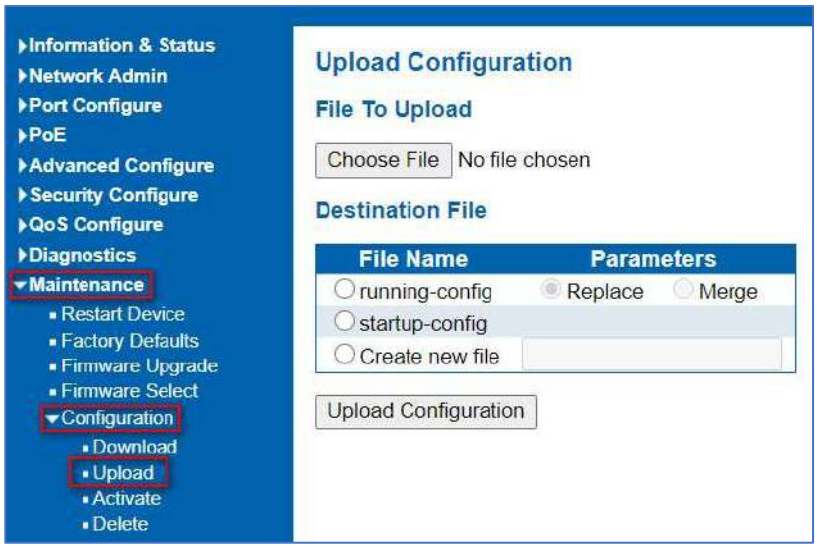


Download Configuration

Please choose a file and then click ''Download Configuration'' button to download.

10.5.2 Update configuration file

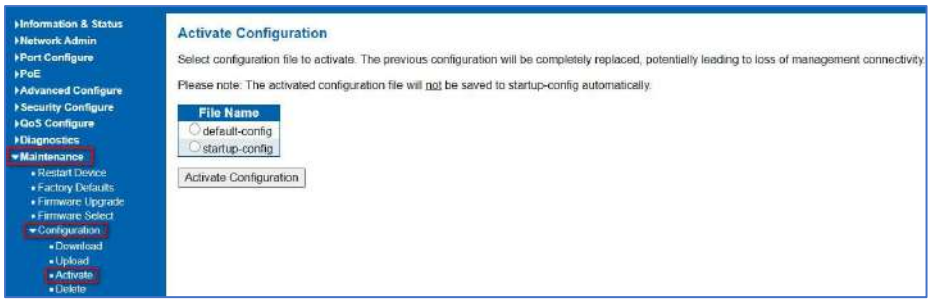
After click ''Maintenance ''>''Upload'', followed screen will appear. Then user can upload Configuration File.



Update Configuration file

10.5.3 Activate Configuration

After click ''Maintenance ''>''Activate'', followed screen will appear. Then user can activate Configuration File.



Activate Configuration

10.5.4 Delete Configuration file.

After click ''Maintenance ''>''Delete'', followed screen will appear. Then user can delete Configuration File.

Delete Configuration file.

ACE

ACE is an acronym for Access Control Entry. It describes the 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 and 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.

For example, the ACL implementations can be quite complex when the ACEs are prioritized for the various situations. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc.) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property. ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

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

APS

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

Aggregation

Use multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability (also Port Aggregation and Link Aggregation).

ARP Inspection

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.

Auto 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

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

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 an OAM frame transmitted from a MEP to its 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 is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations, which are based on a binary number called a key.

DHCP

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

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP relay

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

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0). The parameter of "port_no" is the fourth byte and it means the port number. The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

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

DNS

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

Dos

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

Dotted Decimal

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets. An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

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. 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 log-ons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sub-layer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

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.

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.

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 foremost of the Internet.
IPMC	IPMC is an acronym for IP MultiCast
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.
	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).
LOC	LOC is an acronym for Loss of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS.
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 has 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.

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 gives each computer in the network both a NetBIOS name and an IP address corresponding to a different host name. It 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. This means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

OAM

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 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 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.

PoE

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.

Policer

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 be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

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

Private VLAN	In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.
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.
GCL	QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects. Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.
QL	QL in SyncE; this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.
QoS	QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.
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 an OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP.
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 being backwards-compatible with STP.
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.
SMTP	A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues. 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.
SNMP	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 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.
SSID	Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs,

	and can choose one to connect to, based on pre-configuration or by displaying a list of SSIDs in range and asking the user to select one (Wikipedia).
SSH	SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).
SSM	SSM in SyncE; this is an abbreviation for Synchronization Status Message and is containing a QL indication.
STP	Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.
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.
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. 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. 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	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).
User Priority	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 is 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.

Contact Information

Vigitron, Inc

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