LITE MANAGED ETHERNET SWITCH

SWITCH 4008GT- 8 × 10/100/1000

USER MANUAL

SALZ
AUTOMATION

1.1.1.1 COPYRIGHT

1.1.1.2 FCC WARNING

Warning

This equipment has been assessed and found to comply with the limits for a class A device, according to part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses and6 can radiate radio frequency energy and, if not installed, may cause harmful interference to radio communication. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at the user's own expense.

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warning

Take special care to read and understand all the content in the warning boxes.

Warning

Do not work on the system or connect or disconnect cables during periods of lightning activity.

Warning

Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Warning

Do not stack the chassis on any other equipment. If the chassis falls, it can cause severe bodily injury and equipment damage.

Warning

An exposed wire lead from a DC-input power source can conduct harmful levels of electricity. Be sure that no exposed portion of the DC-input power source wire extends from the terminal block plug.

Warning

Ethernet cables must be shielded when used in a central office environment.

Warning

If a redundant power system (RPS) is not connected to the switch, install an RPS connector cover on the back of the switch.

Warning

Read the wall-mounting instructions carefully before beginning installation. Failure to use the correct hardware or follow the correct procedures could result in a hazardous situation for people and damage the system.

Warning

Before performing any of the following procedures, ensure that power is removed from the DC circuit.

Warning

Read the installation instructions before connecting the system to the power source.

Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Warning

This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.

Warning

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Warning

When installing or replacing the unit, the ground connection must always be made first and disconnected last.

Warning

No user-serviceable parts inside. Do not open.

Warning

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Table of Contents

1 About this Manual

1.1 Introduction

SWITCH 4008GT is a Lite Managed Industrial Switch specifically designed to suit your heavy industrial environments and contains all the necessary standard features to deploy in automation systems. Engineered with hardened components and enclosed in a rugged IP30 case, the SWITCH 4008GT can operate in wide temperatures from -40°C to 70°C and has excellent tolerance capability to high vibration and shock. The SWITCH 4008GT features 8 x 10/100/1000 RJ45 ports to operate in extreme industrial conditions.

The switches are perfectly designed and equipped with a variety of management functions that let you configure communication parameters as you desire and monitor the network behavior in several different simple ways. In addition, the switches are built with dual redundant power inputs to ensure reliability and maximize network up timer integrated features of the switch such as Auto-negotiation, Rate limitation, a QoS optimizer network performance and provide a secure network, offering a cost-effective solution in a small but powerful package.

1.2 Purpose

This manual describes installing and configuring the SWITCH 4008GT - Lite Managed Industrial Ethernet Switch.

2 About the SWITCH 4008GT

2.1 Features

Configuration

Wizard Setting

Dashboard Setting

Port Setting

- Loop Detection
- Port Priority

Ring Setting

- ERPS
- STP

System Setting

- Modbus TCP
- IGMP Snooping

Network Topology

- LLDP
- ONVIF
- Topology Map

Ethernet Interface (10/100/1000Base-T interfaces**)**

Auto-negotiation and Auto-MDI/MDI-X

Flow control of half duplex back pressure

Flow control of full duplex

Security

- 802.1X Radius
- ACL
- Port Security
- Server Control
- Storm Control
- VLAN Setting

Diagnostic

- LED Status
- Port Mirroring
- Port Statistics
- Port Utilization and Threshold
- Remote System Log (Syslog)

Management

- SNMP v1/v2c/v3
- SNMP trap
- SNTP
- Firmware Upgrade & Reboot
- Configuration Upload/Download
- User Account Setting

2.2 Specifications

2.2.1.1 IEEE Standards

IEEE 802.3	10Base-T
IEEE 802.3u	100Base-TX/FX
IEEE 802.3ab	1000Base-T
IEEE 802.3x	Flow Control
IEEE 802.3	Nway Auto-negotiation
IEEE 802.1ab	Link Layer Discovery Protocol
IEEE 802.1p	Class of Service, priority protocols
IEEE 802.1D	Spanning Tree Protocol
IEEE 802.1w	Rapid Spanning Tree Protocol

IEEE 802.1Q	VLAN tagging
IEEE 802.1X	Network Access Control

2.2.1.2 Performance

Switch Fabric	16Gbps
L2 Forwarding	11.9Mpps
Packet buffer size	4.1Mbit
MAC Entries	8K
Jumbo frame	10K
Throughput	1,488,000pps when 1000Mbps speed

2.2.1.3 Physical ports

10/100/1000Base-T (RJ45)	8

Power

Input Voltage: - Primary input - Redundant input	24~48VDC at a maximum of 0.4A 24~48VDC at a maximum of 0.35A
Connection: - Removable 6-pin terminal block - 4pin Mini-DIN connector	One No
Relay output	One with a current carrying capacity of 1A @ 24VDC
Power Consumption	Max. 10W, 24 VDC@0.35A
Overload current protection	Support
Power Reverse Polarity Protection	Support

2.2.1.4 Mechanical

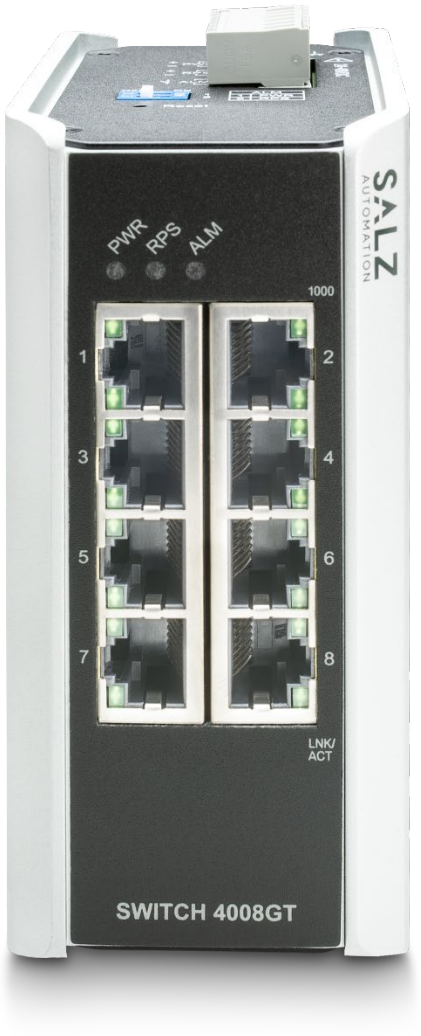
Dimension (W×H×D)	50mm×116mm×100mm
Weight	550g
Mounting	DIN-Rail
Housing	Metal
Dust and Water Protection Rating	IP30

Operating Requirement

Operating temperature	-40°C to 70°C
Storage temperature	-40°C to 85°C
Operating humidity	5 to 95% RH (non-condensing)
Storage humidity	5 to 95% RH (non-condensing)
Altitude	Up to 2000m

3 Hardware Description

SWITCH 4008GT Front Panel



8 x 10/100/1000 RJ45 Light Managed Industrial Switch

3.1 Connectors

The Switches utilize ports with copper connectors functioning under Ethernet/Fast Ethernet/Gigabit Ethernet standards.

10/100/1000Base-T Ports

The 10/100/1000 RJ45 ports support network speeds of 10Mbps, 100Mbps, or 1000Mbps and can operate in half- and full-duplex transfer modes. These ports also offer automatic MDI/MDI-X crossover detection that gives true “plug-n-play” capability – just plug the network cables into the ports and the ports will adjust according to the end-node devices. The following are recommended cabling for the RJ45 connectors: (1) 10Mbps – Cat 3 or better; (2) 100/1000Mbps – Cat 5e or better.

3.2 Installation

The location chosen for installing the Switch may greatly affect its performance. When selecting a site, we recommend considering the following rules:

- ✓ Install the Switch in an appropriate place. See Technical Specifications for the acceptable temperature and humidity ranges.
- ✓ Install the Switch in a location that is not affected by strong electromagnetic field generators (such as motors), vibration, dust, and direct sunlight.
- ✓ Leave at least 10cm of space at the front and rear of the unit for ventilation.

Attention:

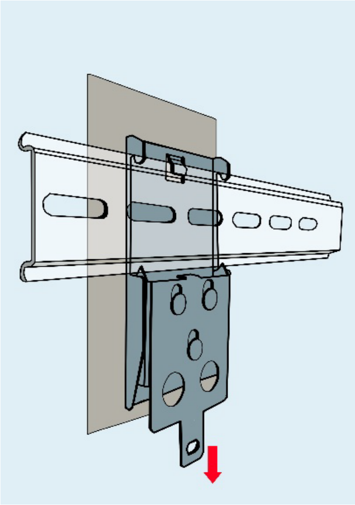
⚠ The SWITCH 4008GT switches are open-type devices and shall be DIN-Rail mounted or wall mounted (optional) in cabinet or enclosure

Hardware Installation

- ✓ **Step 1**: Unpack the device and other contents of the package.
- ✓ **Step 2**: Fasten the DIN-Rail kit on the rear of the switches.
- ✓ **Step 3:** Connect the 24~48 VDC power to the power terminal block.
- ✓ **Step 4**: Connect the Ethernet (RJ45) port to the networking device and check the LED status to confirm the connection is established.

DIN rail Installation

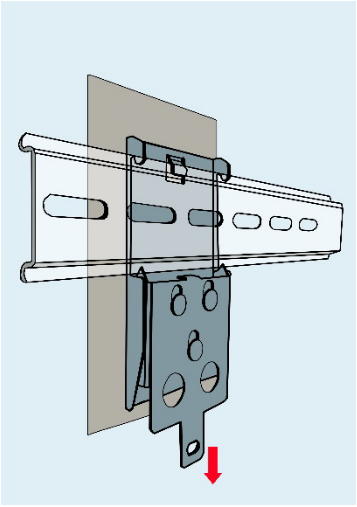
The SWITCH 4008GT switches have a DIN rail bracket on the back of the Switch to satisfy the mounting installation.



Location: The SWITCH 4008GT switches can be DIN-Rail-mounted in a cabinet or enclosure.

Mounting the switch:

1. Place the SWITCH 4008GT switches on the DIN rail from above using the slot.
2. Pull the bracket using a screwdriver or similar tool down.
3. Push the device in position.
4. Release the bracket.



Dismounting the switch

1. Pull the bracket to the bottom using screwdriver or similar tool.
2. Lift the lower part of the switch away from the DIN rail.
3. Lift the device, free the upper slots and remove from the DIN rail.

Wall mount Installation (Optional)

Location: The SWITCH 4008GT switches can be placed on a horizontal surface through the wall-mounted kit.

Place the switch by using mounting holes on the wall at the appropriate place.

Ground the Switch: Ground the switch to earth before powering on the switch.

Ensure the rack on which the switch is to be mounted is properly grounded and in compliance with ETSI ETS 300 253. Verify that there is a good electrical connection to the grounding point on the rack (no paint or isolating surface treatment).

Attention:

⚠ This product is intended to be mounted on a well-grounded mounting surface such as a metal panel.

Caution:

⚠ The earth connection must not be removed unless all power supply connection has been disconnected.

The device is installed in a restricted-access location it has a separate protective earthing terminal on the chassis that must be permanently connected to earth ground to adequately ground the chassis and protect the operator from electrical hazards.

Attention

⚠ The product should be mounted in an Industrial Control Panel and the ambient temperature should not exceed 70°C.

Attention

⚠ A corrosion-free mounting rail is advisable.

When installing, make sure to allow for enough space to properly install the cabling.

Caution

HOT surfaces do not touch. Wear protective equipment before coming into contact.

Wiring Power Inputs

You can use "Terminal Block (PWR)" for the Primary Power input and "Terminal Block (RPS)" for a secondary power source for Redundant Power Input.

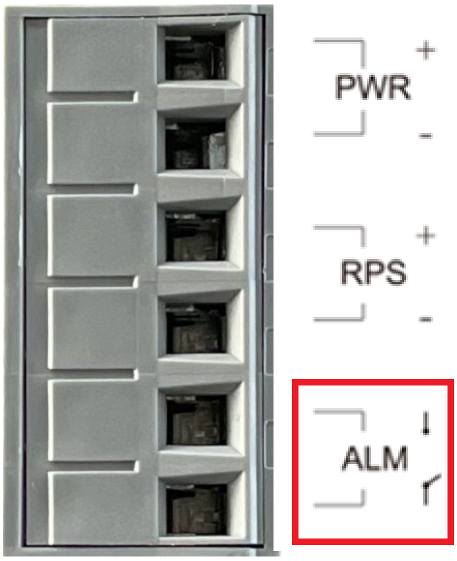
To insert the power wire and connect the 24~48 VDC power to the power terminal block, follow the steps below:

✓ **Step 1**: Insert the positive/negative DC wires into the V+/V- terminal.

✓ **Step 2**: Use your finger to press the green plug on top of the terminal block connector to insert power cables.

✓ **Step 3**: Insert the terminal block connector that includes "PWR" and "RPS" into the terminal block receptor located on the top panel.

The top view of the Terminal Block is shown in the picture:



Warning

⚠
- Use **copper** conductors only, **60/70˚C**, and tighten to **5lb.**
- The wire gauge for the terminal block should range between **12~24 AWG**.

Redundant Power Input: Choose to use “terminal block (PWR)” as the primary power.

Insert the terminal block connector which includes “PWR” and “RPS” into the terminal block receptor.

Connect power cables to terminal block: *Use a screwdriver to insert the power cables.*

WARNING

⚠ Safety measures should be taken before connecting the power cable. Turn off the power before connecting modules or wires. The correct power supply voltage is specified on the product label. Check your power source’s voltage to ensure that you are using the correct voltage. DO NOT use a voltage greater than what is specified on the product label. Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If the current exceeds the maximum rating, the wiring can overheat causing severe damage to your equipment.

Please read and follow these guidelines:

- Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
  NOTE: Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
- You can use the type of signal transmitted through a wire to decide which wires should be kept separate. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together.
- You should separate input wiring from output wiring.
- We recommend that you label the wiring to all devices in the system.

Wiring the Alarm Contact:

The Alarm Contact consists of the two middle contacts of the terminal block on the switch’s top panel.

FAULT: The two middle contacts of the 6-contact terminal block connector are used to detect both power faults and port faults. The two wires attached to the

Fault contacts form an open circuit when:

1. The Switch has lost power from one of the DC power inputs.

If the condition is satisfied, the Fault circuit will be closed.

Warning

- Use **copper** conductors only, **60/70˚C**, and tighten to **5lb**
- The wire gauge for the terminal block should range between **12~24 AWG**.

Powering On the Unit

The Switch accepts the power input voltage of 24~48VDC.

✓ Insert the power cables into the terminal block on top of the device.

✓ Check the front-panel LEDs as the device is powered on to verify that the Power LED is lit. If not, check that the power cable is correctly and securely plugged in.

Notice: Turn off the power before connecting modules or wires.

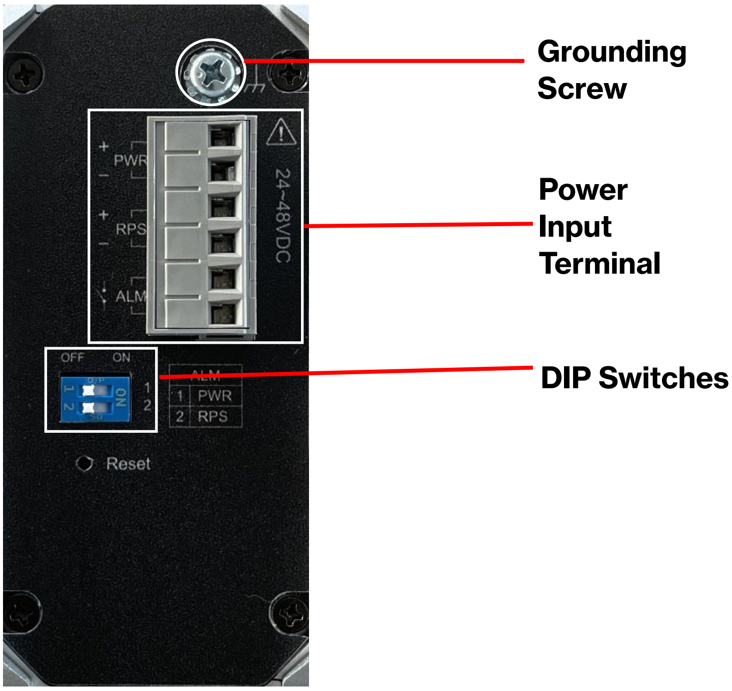
- *The correct power supply voltage is listed on the product label. Check your power source's voltage to ensure that you are using the correct voltage. Do NOT use a voltage greater than what is specified product label.*
- *Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If the current goes above the maximum ratings, the wiring could overheat, causing severe damage to your equipment.*

Manual Reboot / Reset Switch

Switch contains a "Reset" button through which you can manually reboot or reload to factory default settings.

✓ Press the "Reset" button for **more** than 2 seconds to reboot the switch.

✓ Press the "Reset" button for **more** than 5 seconds to reload the factory default settings to the switch.



3.3 LED Indicators

This Switch is equipped with Unit LEDs to enable you to determine the Switch's status and Port LEDs to display what is happening in all your connections. They are as follows:

System LEDs		
PWR	Illuminated	Primary Power on
	Off	Primary Power off or failure
RPS	Illuminated	Redundant (secondary) Power on
	Off	Redundant Power off or failure
ALM	Illuminated	Alarm for the following conditions - when DIP switches are turned on ✓ Primary Power lost ✓ Secondary power lost - Software functions
	Off	Normal operation
Port Number 1-8 LED		
1000	Illuminated	Link speed at 1000Mbps
	Off	Link speed at 10/100Mbps
	Illuminated	Ethernet link-up

LNK/ACT	Blinking	Activity (receiving or transmitting data)
	Off	Port disconnected or link failed

3.4 DIP Switches

DIP	Function Description
PWR	Primary power input from the terminal block ON Primary power alarm reporting is enabled OFF Primary power alarm reporting is disabled
RPS	Redundant power input from the terminal block ON Redundant power alarm reporting is enabled OFF Redundant power alarm reporting is disabled

Warning

⚠ Do not block air ventilation holes, as heat dissipated passes through them.

Attention

⚠ This device follows Part 15 of the FCC rules. Operation is subject to the following conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received including interference that may cause undesired operation.

Attention

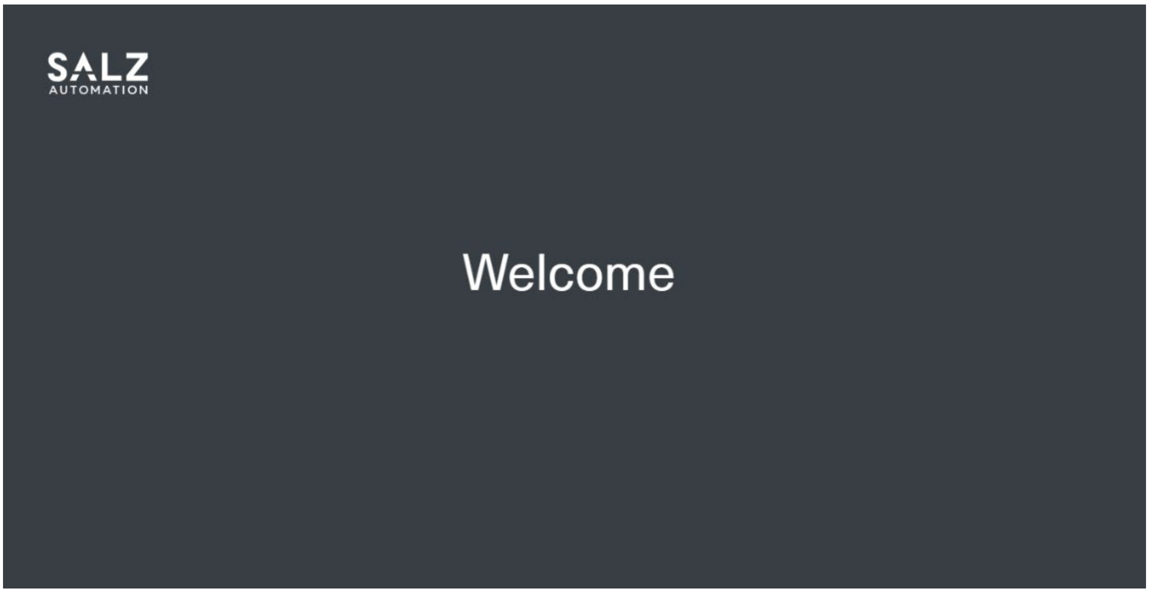
⚠ If the equipment is used in a manner not specified by the SALZ Automation GmbH, the protection provided by the equipment may be impaired.

4 Configuration

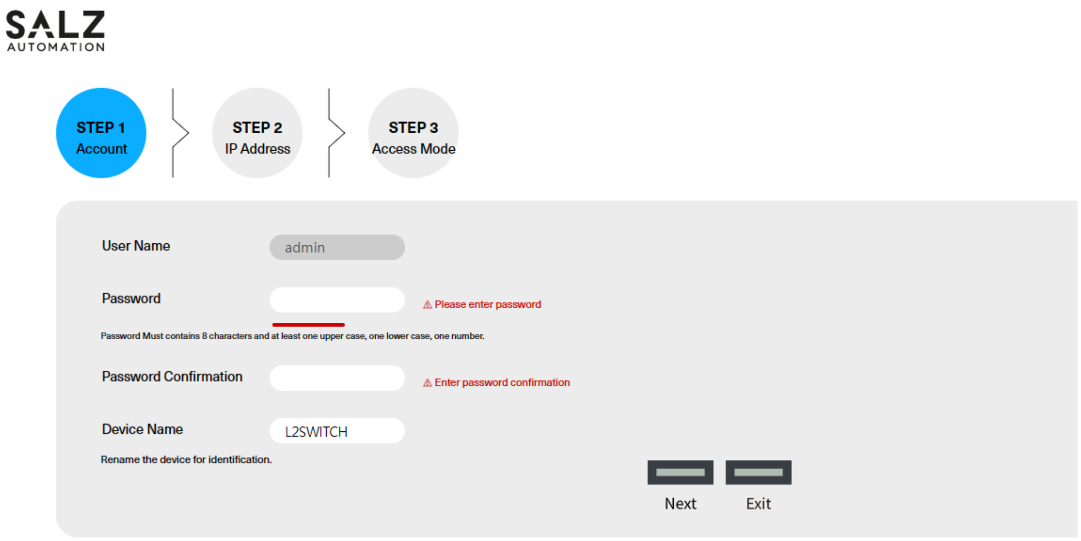
Initially, the new device connects the network using the default IP (192.168.0.254). Access the IP address to enter the Wizard. After three seconds the "Welcome" screen will switch to the set-up screen as shown below. The Wizard is only displayed when the device is switched on for the first time or after it has been reset. In addition, the wizard can be started via the corresponding menu item (Configuration -> Wizard Settings).

4.1 Wizard Settings

Wizard will be using full to configure basic settings in the device like switch User account with a host name, management IP, And access Mode. The Wizard-assisted interface covers the basic requirements for most end-users to set up the Ethernet switch in these three steps; 1) Account; 2) IP address; 3) Access Mode.



Welcome screen after logging in the first time or after resetting.



User Name: admin

Password: ⚠ Please enter password

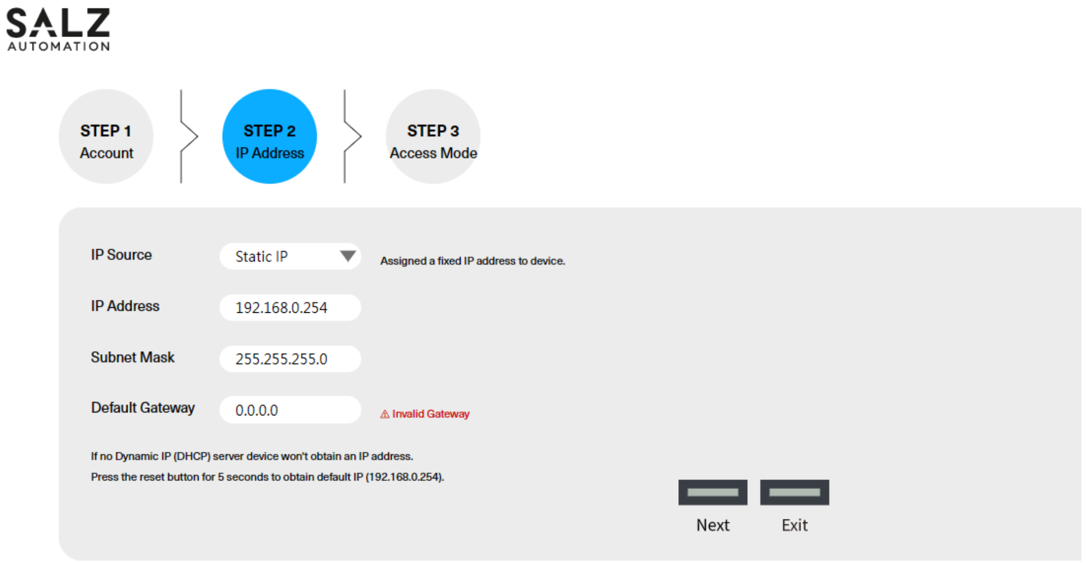
Password Must contains 8 characters and at least one upper case, one lower case, one number.

Password Confirmation: ⚠ Enter password confirmation

Device Name: L2SWITCH

Rename the device for identification.

Step 1: Account Settings to configure user credentials to access the device. The wizard will guide you through the strength of security.



IP Source: Static IP — Assigned a fixed IP address to device.

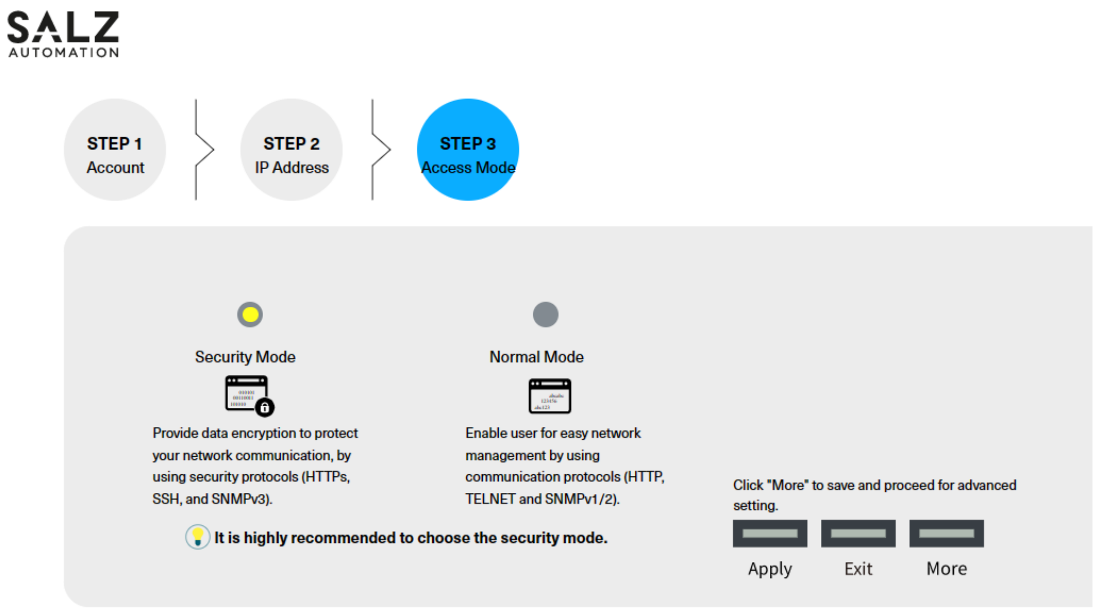
IP Address: 192.168.0.254

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0 ⚠ Invalid Gateway

If no Dynamic IP (DHCP) server device won't obtain an IP address.
Press the reset button for 5 seconds to obtain default IP (192.168.0.254).

Step 2: IP Address is to configure the management IP user can select DHCP mode or static mode to configure the switch IP as shown below.



○ Security Mode

Provide data encryption to protect your network communication, by using security protocols (HTTPs, SSH, and SNMPv3).

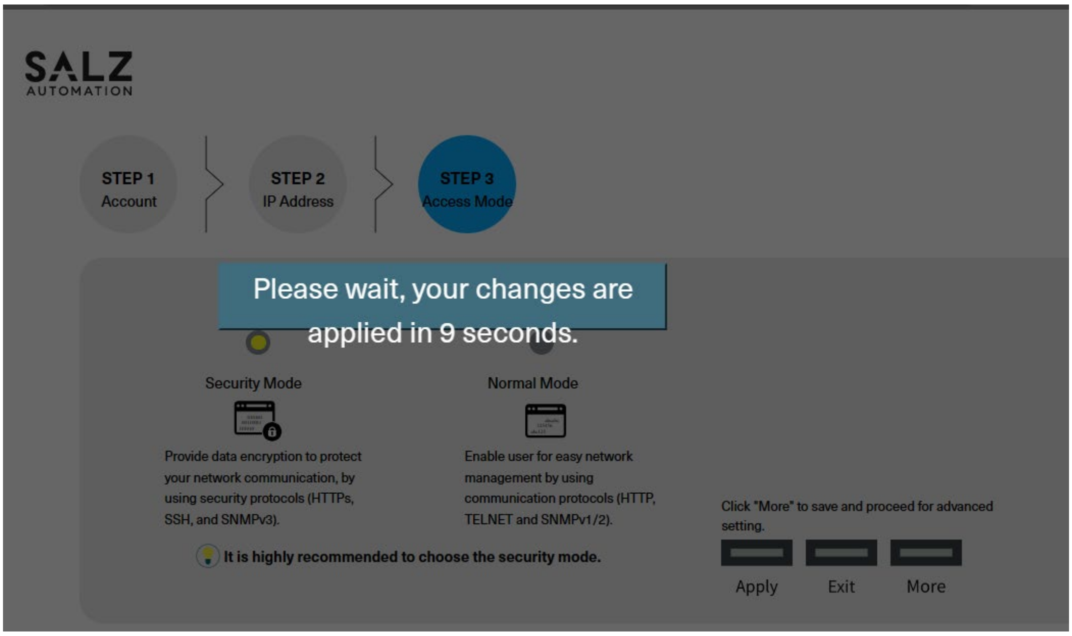
○ Normal Mode

Enable user for easy network management by using communication protocols (HTTP, TELNET and SNMPv1/2).

It is highly recommended to choose the security mode.

Click "More" to save and proceed for advanced setting.

Step 3: Access Mode is to access the device has 2 options Security mode (HHTTP SSH, and SNMPv3) and Normal mode (HTTP, TELNET, and SNMPv1/v2).



Please wait, your changes are applied in 9 seconds.

○ Security Mode

Provide data encryption to protect your network communication, by using security protocols (HTTPs, SSH, and SNMPv3).

○ Normal Mode

Enable user for easy network management by using communication protocols (HTTP, TELNET and SNMPv1/2).

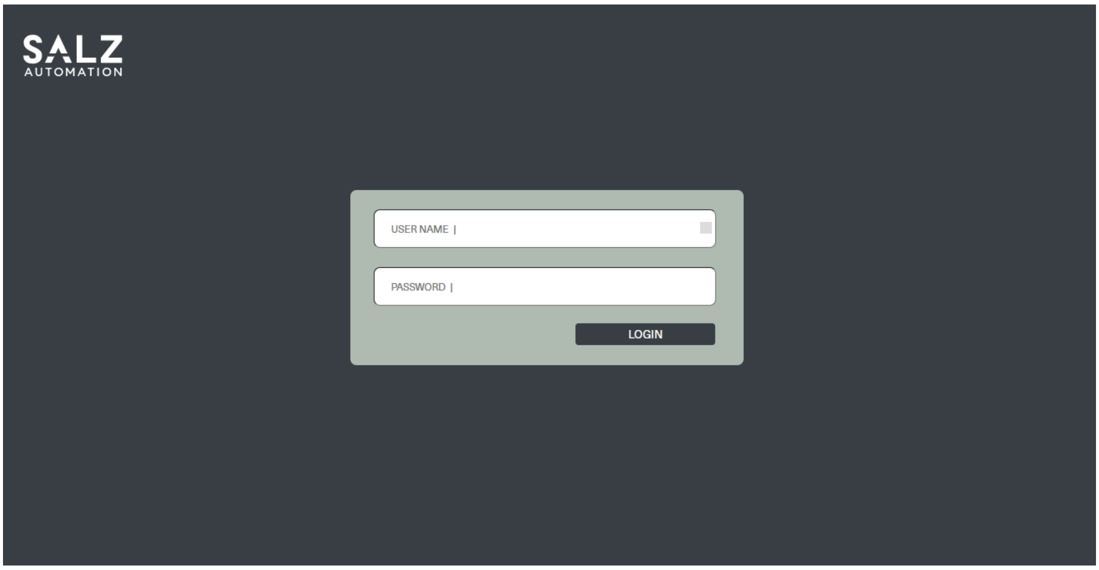
It is highly recommended to choose the security mode.

Click "More" to save and proceed for advanced setting.

Step 4: Restart the switch: The switch will be accessible under the new settings.

4.2 Lock in after the switch is configured.

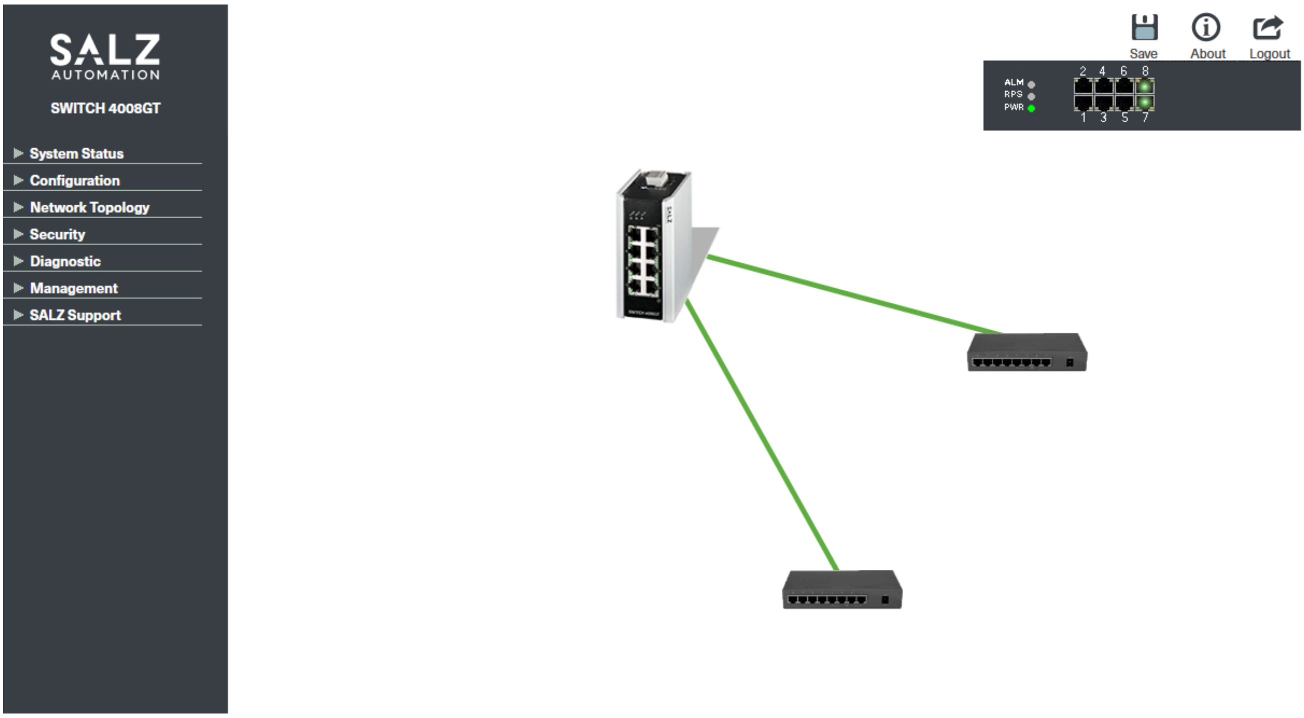
After the switch has been configured using the wizard, a login is required. The login screen appears when the device is selected and after several minutes of non-use.



Login screen for username and password

4.3 Overview

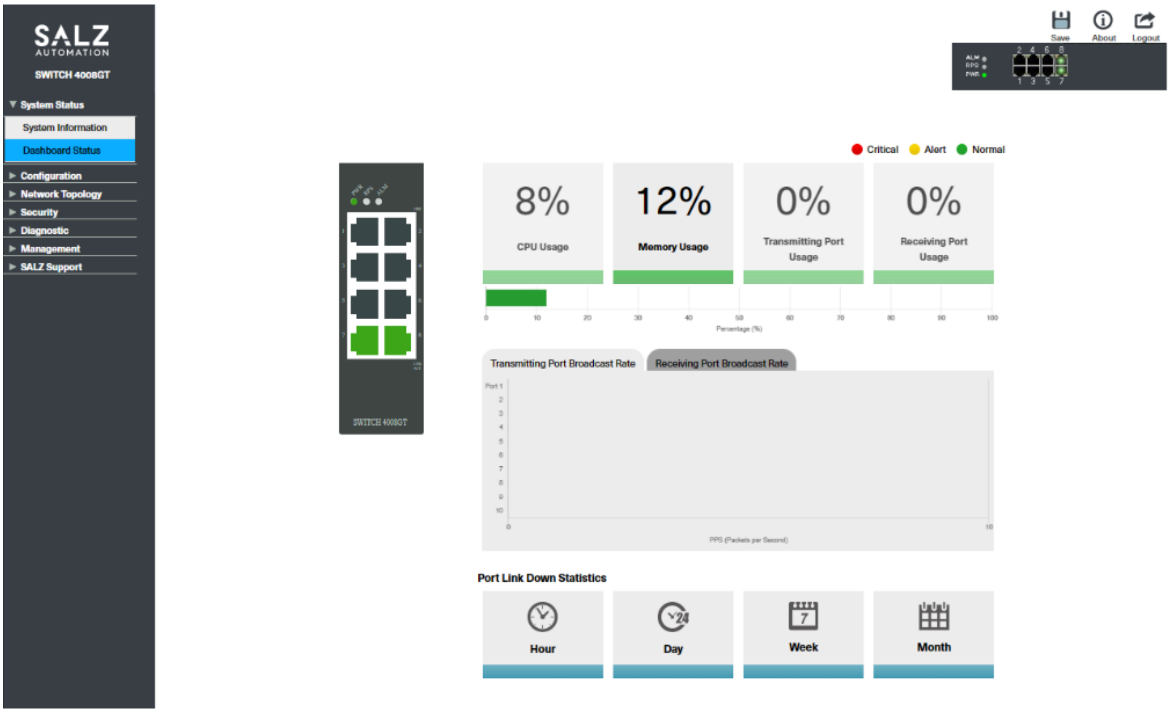
The switch informs about the general status on the receive screen. This includes information about the connected devices and diagnostic information.



Overview Screen for getting the first valuable information.

4.4 Dashboard status and Dashboard settings

The Dashboard is an intelligent system that provides real-time switch parameters including performance, link status, and data traffic information in an engaging, easy-view format for the end-users. The dashboard setting enables you to control the performance of the switch like CPU, Memory, Port Tx Usage, and Port Rx Usage. Learn the option to obtain port registration information.



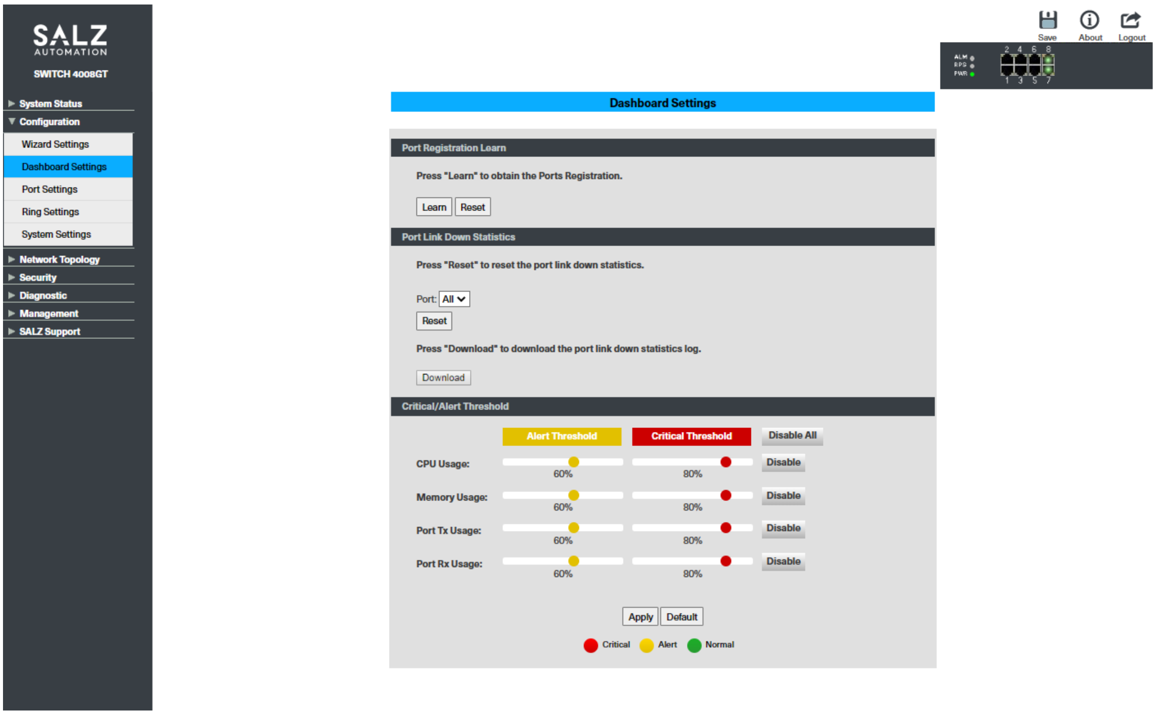
8% CPU Usage

12% Memory Usage

0% Transmitting Port Usage

0% Receiving Port Usage

Port Link Down Statistics



Dashboard Settings

Port Registration Learn

Press "Learn" to obtain the Ports Registration.

Learn | Reset

Port Link Down Statistics

Press "Reset" to reset the port link down statistics.

Port: All

Reset

Press "Download" to download the port link down statistics log.

Download

Critical/Alert Threshold

	Alert Threshold	Critical Threshold	Disable All
CPU Usage:	60%	80%	Disable
Memory Usage:	60%	80%	Disable
Port Tx Usage:	60%	80%	Disable
Port Rx Usage:	60%	80%	Disable

Apply | Default

● Critical ● Alert ● Normal

Dashboard Overview and Dashboard Settings

Parameter	Description
System Information	
Learn	This field is to obtain the port registration information.
Reset	Reset option to reset the port registration information
Port	User can select individual port or all ports information to reset to default on registration information
Download	This field will download the statistics of port-down information along with the date and time.
CPU Usage	User can configure threshold value to normal, alert, critical percentage, or disable the feature
Memory Usage	User can configure threshold value to normal, alert, critical percentage, or disable the feature
Port Tx Usage	User can configure threshold value to a normal, alert, critical percentage of the interface Tx usage or disable the feature
Port Rx Usage	User can configure threshold value to a normal, alert, critical percentage of the interface Rx usage or disable the feature
Apply	This field is used for applying the changes made
Default	This field will make the Switch to default values

4.5 Port Settings

4.5.1 Port Configuration

Introduction

In the port configuration, you can enable or disable the port. If the port is disabled, the port remains off without any operation. To keep it operating, place the port in enable state.

Speed

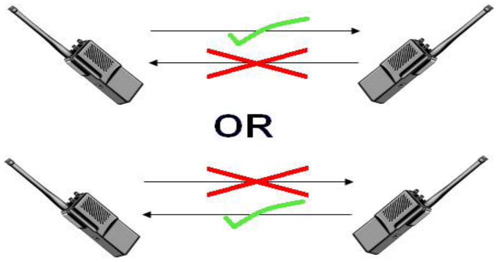
It defines at which speed the port should operate. The speeds that it can operate are 10/100/1000Mbps. And you can specify whether the port should operate and in what mode. The operating modes are half duplex and full duplex.

Duplex mode

A *duplex* communication system is a system composed of two connected parties or devices that can communicate with one another in both directions.

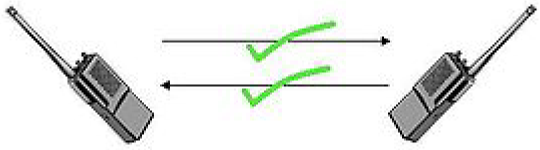
Half Duplex:

A *half-duplex* system provides for communication in both directions, but only one direction at a time (not simultaneously). Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting, before replying.



Full Duplex:

A *full-duplex*, or sometimes a *double-duplex* system, allows communication in both directions, and, unlike a half-duplex, allows this to happen simultaneously. Land-line telephone networks are full-duplex since they allow both callers to speak and be heard at the same time.



- Loopback Test

A loopback test is a test in which a signal is sent from a communications device and returned (looped back) to it to determine whether the device is working right or to pin down a failing node in a network. One type of loopback test is performed using a special plug, called a **wrap plug** which is inserted in a port on a communications device. The effect of a wrap plug is to cause transmitted (output) data to be returned as received (input) data, simulating a complete communications circuit using a single computer.

- Auto MDI-MDIX

Auto-MDIX (automatic medium-dependent interface crossover) is a computer networking technology that automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately, thereby removing the need for crossover cables to interconnect switches or connecting PCs peer-to-peer. When it is enabled, either type of cable can be used, or the interface automatically corrects any incorrect cabling. For Auto-MDIX to operate correctly, the speed on the interface and duplex setting must be set to "auto". Auto-MDIX was developed by HP engineers Dan Dove and Bruce Melvin.

- Auto-Negotiation

Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode.

If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using **half duplex** mode. When the Switch’s auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same to connect.

- Flow Control

The concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill and resend later.

The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half-duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half-duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.

Note: 1000 Base-T does not support force mode.

- Cable Test

This feature determines the quality of the cables, shorts, cable impedance mismatch, bad connectors, termination mismatch, and bad magnetics. The feature can work on the copper Ethernet cable only.

Default Settings

The default port Speed & Duplex is auto for all ports.

The default port Flow Control is Off for all ports.

4.5.1.1 CLI Configuration

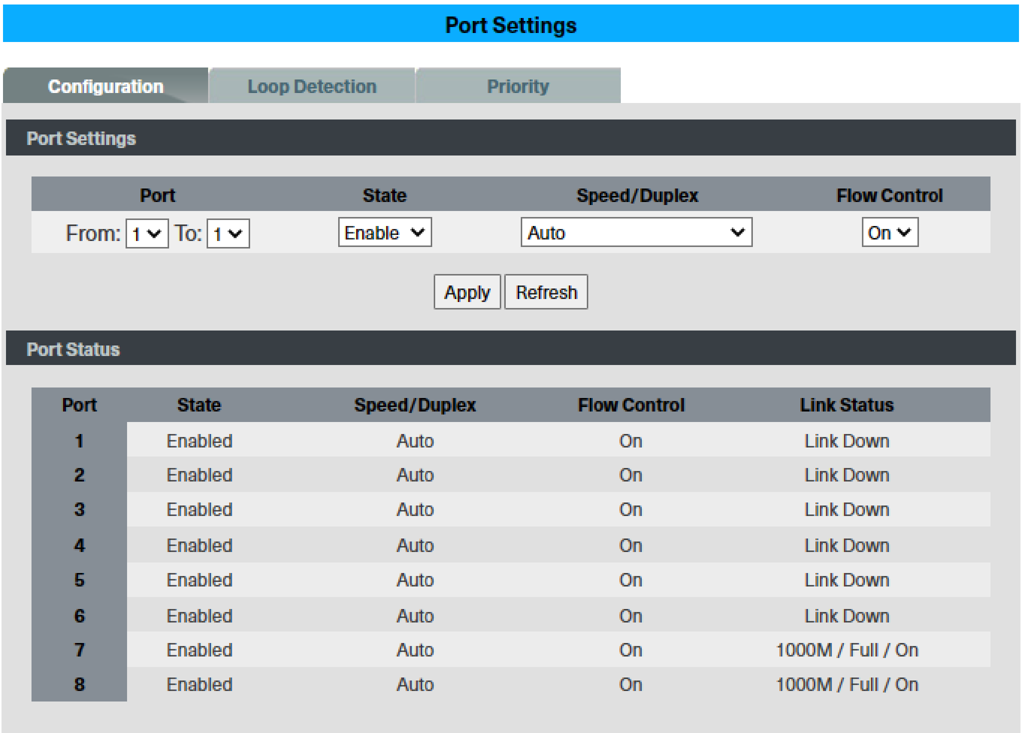
Node	Command	Description
enable	show interface IFNAME	This command displays the current port configurations.
configure	interface IFNAME	This command enters the interface configure node.
interface	show	This command displays the current port configurations.
interface	loopback (none | mac)	This command evaluates the loopback mode of operation for the specific port.
interface	flow control (off | on)	This command disables / enables the flow control for the port.
interface	speed (auto|10-full||10-half|100-full|100-half|1000-full)	This command configures the speed and duplex for the port.
interface	shutdown	This command disables the specific port.
interface	no shutdown	This command enables the specific port.
interface	Description STRINGs	This command configures a Description for the specific port.
interface	no Description	This command configures the default port Description.
interface	cable test	This command diagnostics the Ethernet cable and shows the broken distance.
interface	clean cable-test result	This command cleans the test

		result of the Ethernet cable test.
interface	show cable-test result	This command displays the test result of the Ethernet cable test.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	description STRINGs	This command configures a Description for the specific ports.
if-range	no description	This command configures the default port Description for the specific ports.
if-range	shutdown	This command disables the specific ports.
if-range	no shutdown	This command enables the specific ports.
if-range	speed (auto|10-full||10-half| 100-full|100-half|1000-full)	This command configures the speed and duplex for the port.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#interface gi1/0/1
L2SWITCH(config-if)#speed auto
```

4.5.1.2 Port Settings Web Configuration



Port	State	Speed/Duplex	Flow Control
From: 1 To: 1	Enable	Auto	On

Port	State	Speed/Duplex	Flow Control	Link Status
1	Enabled	Auto	On	Link Down
2	Enabled	Auto	On	Link Down
3	Enabled	Auto	On	Link Down
4	Enabled	Auto	On	Link Down
5	Enabled	Auto	On	Link Down
6	Enabled	Auto	On	Link Down
7	Enabled	Auto	On	1000M / Full / On
8	Enabled	Auto	On	1000M / Full / On

Parameter	**Description**
Port Settings	
Port	Selects a port or a range of ports on which to configure the port.
State	Select the option to enable/disable the port.
Speed/duplex	Select a speed/duplex for the port(s).
Flow Control	User can configure flow control on the interface on/off
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Port Status	
Port	This field displays the index number of a port.
State	This field displays the state of a port.
Speed/Duplex	This field displays the speed/duplex of a port.
Flow Control	Display the status of the flow control in the interface on/off

Link Status	This field displays the link status of a port.

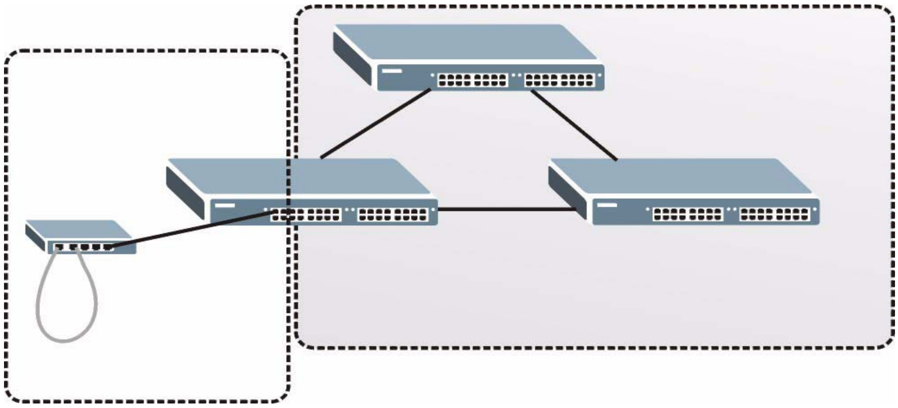
4.5.2 Loop Detection Configuration

Introduction

Loop detection is designed to manage loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in a loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast repeatedly causing a broadcast storm.

The difference between Loop Detection and STP:

Loop Detection **STP**



The Loop Detection function sends probe packets periodically to detect if the port connects to a network in a loop state. The Switch shuts down the port if the Switch detects that probe packets loop back to the Switch. This closes the port that was last connected in the loop.

Loop Recovery:

When the loop detection is enabled, the Switch will send one probe packet every two seconds and then wait for this packet. If it receives the packet at the same port, the Switch will disable this port. After the period ***recovery time,*** the Switch will enable this port and do loop detection again.

The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop detection feature.

For the access Switch, it may not enable the STP function. To guarantee the network topology is loop-free, the Loop detection function also needs to detect the below scenario.

If ports 1 and 2 are looped, and port 1’s loop detection is enabled, port 1 will be disabled. If both port 1’s and port 2’s loop detection is enabled, both port 1 and port 2 will be disabled.

Default Settings

- The default global Loop-Detection state is disabled.
- The default Loop Detection Destination MAC is **00:0b:04:AA:AA:AB**
- The default Port Loop-Detection state is disabled for all ports.

4.5.2.1 CLI Configuration

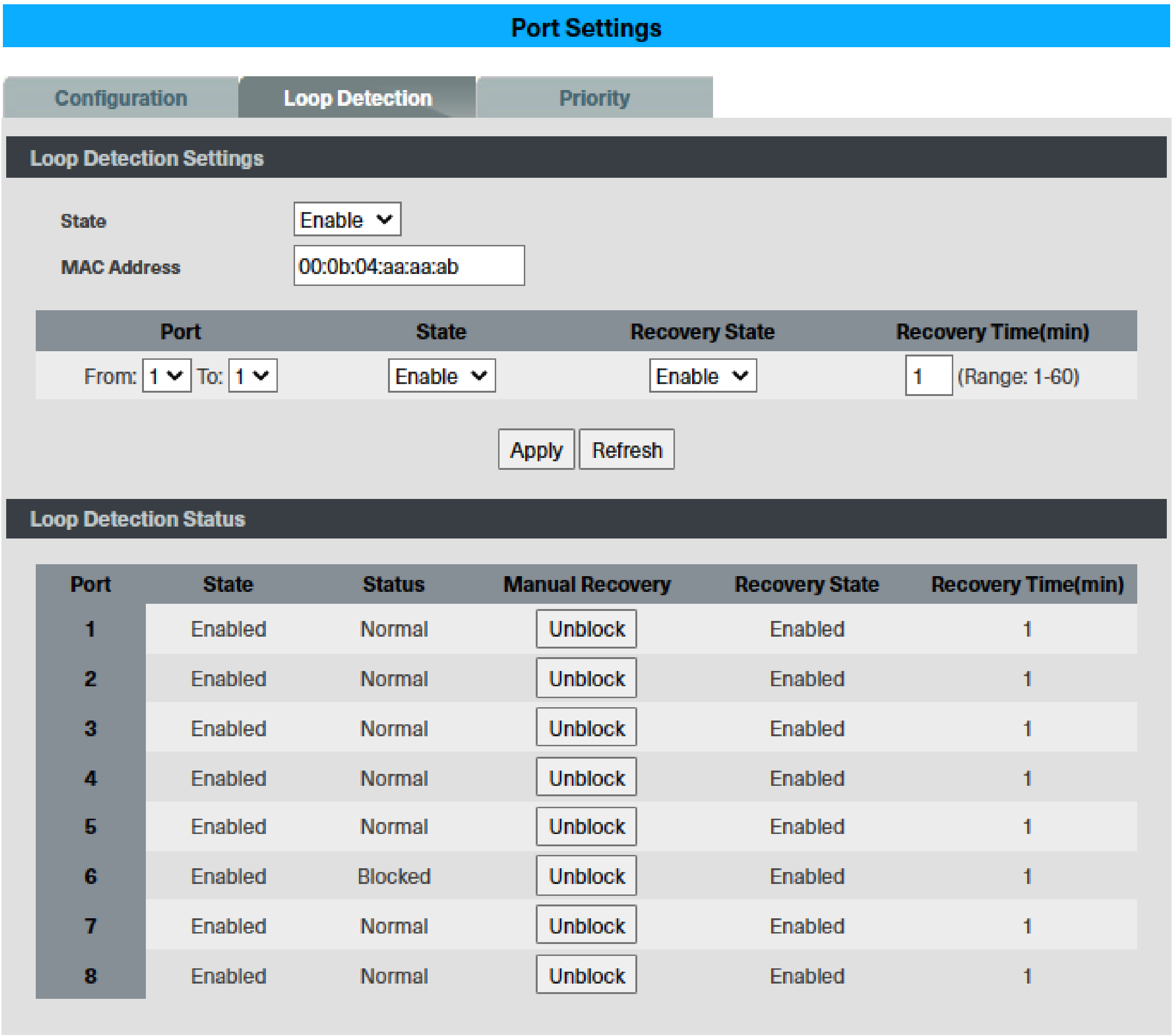
Node	Command	Description
enable	show loop-detection	This command displays the current loop detection configurations.
configure	loop-detection (disable | enable)	This command disables/enables the loop detection on the switch.
configure	loop-detection address macaddr	This command configures the destination MAC for the loop detection of special packets.
configure	no loop-detection address	This command configures the destination MAC to default (00:0b:04:AA:AA:AB).
interface	loop-detection (disable | enable)	This command disables/enables the loop detection on the port.
interface	no shutdown	This command enables the port. It can unblock ports blocked by loop detection.
interface	loop-detection recovery (disable | enable)	This command enables/disables the recovery function on the port.
interface	loop-detection recovery time VALUE	This command configures the recovery period time.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.

if-range	loop-detection (disable | enable)	This command disables/enables loop detection on the ports.
if-range	loop-detection recovery (disable | enable)	This command enables/disables the recovery function on the port.
if-range	loop-detection recovery time VALUE	This command configures the recovery period time.

Example:

```
L2SWITCH(config)#loop-detection enable
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#loop-detection enable
```

4.5.2.2 Loop Detection Web Configuration



Loop Detection Settings

State: Enable

MAC Address: 00:0b:04:aa:aa:ab

Port	State	Recovery State	Recovery Time(min)
From: 1 To: 1	Enable	Enable	1 (Range: 1-60)

Loop Detection Status

Port	State	Status	Manual Recovery	Recovery State	Recovery Time(min)
1	Enabled	Normal	Unblock	Enabled	1
2	Enabled	Normal	Unblock	Enabled	1
3	Enabled	Normal	Unblock	Enabled	1
4	Enabled	Normal	Unblock	Enabled	1
5	Enabled	Normal	Unblock	Enabled	1
6	Enabled	Blocked	Unblock	Enabled	1
7	Enabled	Normal	Unblock	Enabled	1
8	Enabled	Normal	Unblock	Enabled	1

Parameter	**Description**
State	User can configure loop-detection state enable/disable globally by default it is disabled.
MAC Address	Enter the destination MAC address, where the probe packets will be sent. If the port receives these same packets the port will be shut down.
Port	Select a port on which to configure loop guard protection.
State	Select **Enable** to use the loop guard feature on that particular port of the Switch.
Recovery State	Select **Enable** to reactivate the port automatically after the designated recovery time has passed.
Recovery Time (min)	Specify the recovery time in minutes that the Switch will wait before reactivating the port. This can be between 1 to 60 minutes.
Apply	Click **Apply** to save your changes to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Configuration Status	
Port	This field displays a port number.
State	This field displays if the loop guard feature is enabled.
Status	This field displays if the port is blocked.
Manual Recovery	Manual Recovery can be locked or unlocked by default it is unlocked
Recovery State	This field displays if the loop recovery feature is enabled.
Recovery Time (min)	This field displays the recovery time for the loop recovery feature.

4.5.3 Port Priority

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered promptly. When congestion occurs, all traffic has an equal chance of being dropped.

Using the Port Priority feature, you can select specific network traffic, and prioritize it according to its relative importance. Implementing Port Priority in your network makes network performance more predictable and bandwidth utilization more effective.

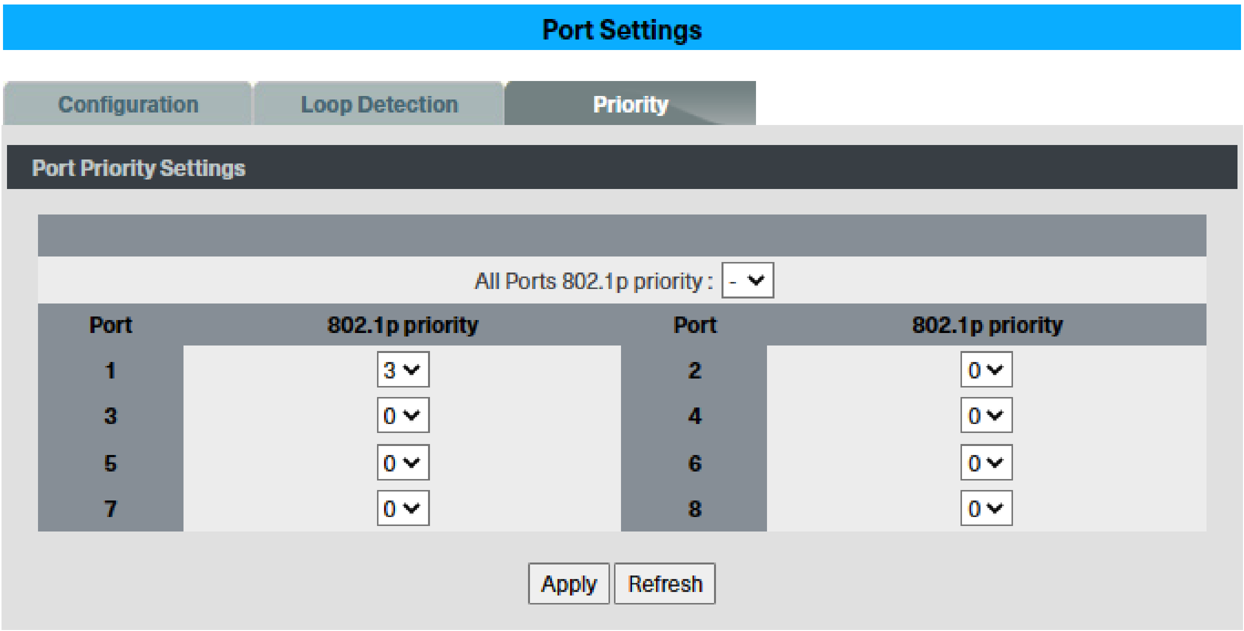
Eight different classes of priority are available, whereby the priority increases with ascending value. The way traffic is treated when assigned to any priority is undefined and left to the implementation. IEEE, however, has made some broad recommendations

4.5.3.1 CLI Configuration

Node	Command	Description
enable	show queue cos-map	This command displays the current 802.1p priority mapping to the service queue.
enable	show qos mode	This command displays the current QoS scheduling mode of IEEE 802.1p.
configure	queue cos-map PRIORITY QUEUE_ID	This command configures the 802.1p priority mapping to the service queue.
configure	no queue cos-map	This command configures the 802.1p priority mapping to the service queue to default.
configure	qos mode high-first	This command configures the QoS scheduling mode to high first, each hardware queue will transmit all the packets in its buffer before permitting the next lower priority to transmit its packets.
configure	qos mode wrr-queue weights VALUE	This command configures the QoS scheduling mode to Weighted Round Robin.
interface	default-priority	This command allows the user to specify a default priority handling of untagged packets received by the Switch. The priority value entered with this command will be used to

		determine which of the hardware priority queues the packet is forwarded to. Default: 0.
interface	no default-priority	This command configures the default priority for the specific port to default (0).
enable	show diffserv	This command displays DiffServ configurations.
configure	diffserv (disable | enable)	This command disables / enables the DiffServ function.
configure	diffserv dscp VALUE priority VALUE	This command sets the DSCP-to-IEEE 802.1q mappings.

4.5.3.2 Port Priority Web Configuration



All Ports 802.1p priority : -

Port	802.1p priority	Port	802.1p priority
1	3	2	0
3	0	4	0
5	0	6	0
7	0	8	0

Parameter	Description
Port Priority Settings	
Port	Selects a port or a range of ports on which to configure the priority.
Priority	Select a priority for packets received by the port. Only

	packets without 802.1p priority tagged will be applied the priority you set here.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Port Priority Status	
Port	This field displays a port number.
Priority	This field displays the priority for a port.

4.6 Ring Configuration

4.6.1 ERPS

Introduction

The ITU-T G.8032 **E**thernet **R**ing **P**rotection **S**witching feature implements protection switching mechanisms for Ethernet layer ring topologies. This feature uses the G.8032 **Ethernet Ring Protection (ERP)** protocol, defined in ITU-T G.8032, to protect Ethernet traffic in a ring topology, while ensuring that no loops are within the ring at the Ethernet layer. The loops are prevented by blocking traffic on either a predetermined link or a failed link.

The Ethernet ring protection functionality includes the following:

- Loop avoidance
- The use of learning, forwarding, and Filtering Database (FDB) mechanisms

Loop avoidance in an Ethernet ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This link is called the **ring protection link (RPL)** and under normal conditions, this ring link is blocked, i.e., not used for service traffic. One designated Ethernet ring node, the **RPL owner** node, is responsible to block traffic at one end of the RPL. Under an Ethernet ring failure condition, the RPL owner node is responsible for unblocking its end of the RPL, unless the RPL has failed, allowing the RPL to be used for traffic. The other Ethernet ring node adjacent to the RPL, the **RPL neighbor** node, may also participate in blocking or unblocking its end of the RPL.

The Ethernet rings could support a multi-ring/ladder network that consists of conjoined Ethernet rings by one or more interconnection points. The protection switching mechanisms and protocol defined in this Recommendation shall be applicable for a multi-ring/ladder network if the following principles are adhered to:

- R-APS channels are not shared across Ethernet ring interconnections.
- on each ring port, each traffic channel, and each R-APS channel are controlled (e.g., for blocking or flushing) by the Ethernet ring protection control process (ERP control process) of only one Ethernet ring.

- Each major ring or sub-ring must have its RPL.

In an Ethernet ring, without congestion, with all Ethernet ring nodes in the idle state (i.e., no detected failure, no active automatic or external command, and receiving only "NR, RB" R-APS messages), with less than 1200 km of ring fiber circumference and fewer than 16 Ethernet ring nodes, the switch completion time (transfer time as defined in [ITU-T G.808.1]) for a failure on a ring link shall be less than **50ms**.

The rings' protection architecture relies on the existence of an **APS protocol** to coordinate ring protection actions around an Ethernet ring.

The Switch supports up to **six** rings.

Guard timer -- All Ethernet Ring Nodes (ERN) use a guard timer. The guard timer prevents the possibility of forming a closed loop and prevents ERNs from applying outdated R-APS messages. The guard timer activates when an ERN receives information about a local switching request, such as after a switch fail (SF), manual switch (MS), or forced switch (FS). When this timer expires, the ERN begins to apply actions from the R-APS it receives. This timer cannot be manually stopped.

Wait to restore (WTR) timer -- The RPL owner uses the WTR timer. The WTR timer applies to the revertive mode to prevent frequent triggering of the protection switching due to port flapping or intermittent signal failure defects. When this timer expires, the RPL owner sends an R-APS (NR, RB) through the ring.

Wait to Block (WTB) timers -- This wait-to-block timer is activated on the RPL owner. The RPL owner uses WTB timers before initiating an RPL block and then reverting to the idle state after operator-initiated commands, such as for FS or MS conditions, are entered. Because multiple FS commands are allowed to co-exist in a ring, the WTB timer ensures that the clearing of a single FS command does not trigger the re-blocking of the RPL. The WTB timer is defined to be 5 seconds longer than the guard timer, which is enough time to allow a reporting ERN to transmit two R-APS messages and allow the ring to identify the latent condition. When clearing an MS command, the WTB timer prevents the formation of a closed loop due to the RPL owner node applying an outdated remote MS request during the recovery process.

Hold-off timer -- Each ERN uses a hold-off timer to delay reporting a port failure. When the timer expires, the ERN checks the port status. If the issue still exists, the failure is reported. If the issue does not exist, nothing is reported.

ERPS revertive and non-revertive switching -- ERPS considers revertive and non-revertive operations. In revertive operation, after the condition (s) causing a switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL. In the case of clearing a defect, the traffic channel reverts after the expiry of a WTR timer, which is used to avoid toggling protection states in case of intermittent defects. In non-revertive operation, the traffic channel continues to use the RPL, if it is not failed, after a switch condition has cleared.

Control VLAN:

The pure ERPS control packets domain only, no other packets are transmitted in this VLAN to guarantee no delay for the ERPS. So, when you configure a Control VLAN for a ring, the VLAN should be a new one. The ERPS will create this control VLAN and its member ports automatically. The member port should have the Left and Right ports only.

In ERPS, the control packets and data packets are separated into different VLANs.

The control packets are transmitted in a VLAN which is called the Control-VLAN.

Instance:

For ERPS version 2, the instance is a profile that specifies a control VLAN and a data VLAN or multiple data VLANs for the ERPS. In ERPS, it can separate the control packets and data packets in different VLANs. The control packets are in the Control-VLAN and the data packets can be in one or multiple VLANs, and then the user can assign an instance to an ERPS ring easily.

In ERPS version 1, if a port is blocked by ERPS, all packets are blocked.

In ERPS version 2, if a port is blocked by a ring of ERPS, only the packets belonging to the VLANs in the instance are blocked.

Control VLAN and Instance:

There are the Control VLAN and the Instance settings.

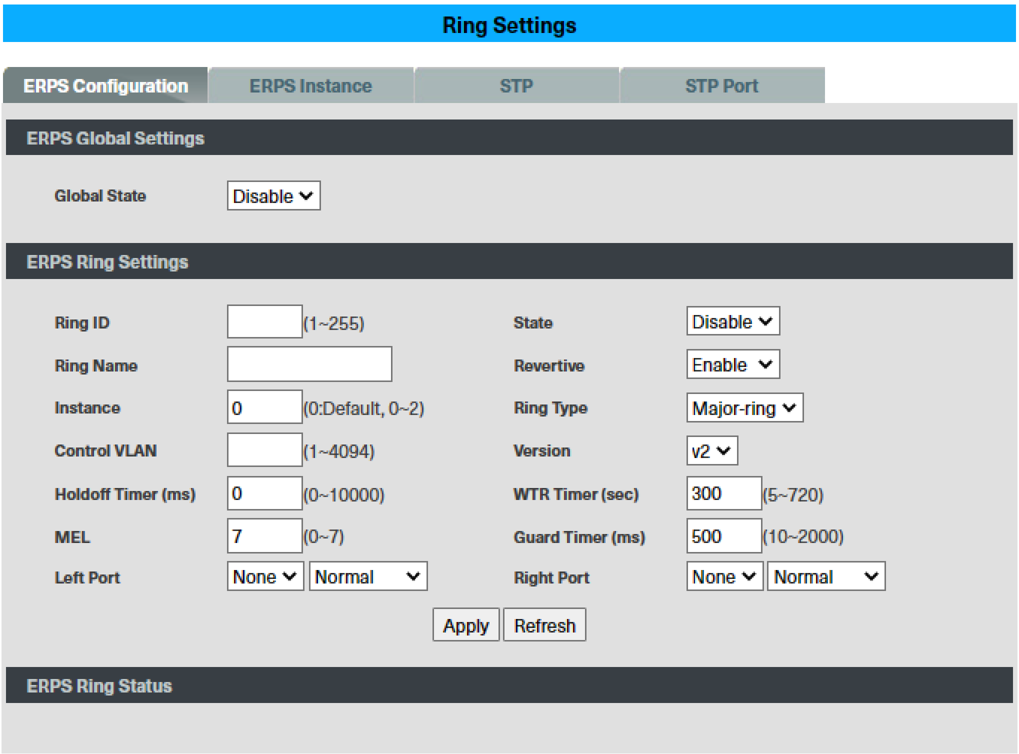
If the Control VLAN is configured for a ring and you want to configure an instance for the ring. The control VLAN of the instance must be the same as the Control-VLAN; otherwise, you will get an error. If you still want to use this instance, you can change the Control-VLAN to same as the Control-VLAN of the instance first. And then configures the instance.

4.6.1.1 CLI Configuration

Node	Command	Description
enable	show erps	This command displays the ERPS configurations.
enable	show erps instance	This command displays the ERPS instance configurations.
enable	show erps instance INSTANCE_ID	This command displays the specific ERPS instance configurations.
configure	erps enable	This command enables the global ERPS on the Switch.
configure	no erps enable	This command disables the global ERPS on the Switch.
configure	erps ring-id VALUE	This command creates an ERPS ring and its ID and enter ERPS node.
configure	erps instance	This command enters the instance configure the node.
configure	no erps ring-id VALUE	This command creates an ERPS ring and enters the ERPS node to configure detail ring configurations.
erps-ring	show	This command displays the configurations of the ring.
erps-ring	control-vlan	This command configures a control-VLAN for the ERPS ring.
erps-ring	guard-timer	This command configures the Guard Timer for the ERPS ring. (Default:500ms)
erps-ring	holdoff-timer	This command configures the Hold-off Timer for the ERPS ring. (Default: 0 ms)
erps-ring	left port PORTID type [owner|neighbor|normal]	This command configures the left port and type for the ERPS ring.
erps-ring	mel VALUE	This command configures a Control MEL for the ERPS ring.

erps-ring	name STRING	This command configures a name for the ERPS ring.
erps-ring	revertive	This command configures the revertive mode for the ERPS ring.
erps-ring	no revertive	This command configures the non-revertive mode for the ERPS ring.
erps-ring	right-port PORTID type [owner|neighbor|normal]	This command configures the right port and type for the ERPS ring.
erps-ring	ring enable	This command enables the ring.
erps-ring	no ring enables	This command disables the ring.
erps-ring	version	This command configures a version for the ERPS ring.
erps-ring	wtr-timer	This command configures the WTR Timer for the ERPS ring. (Default: 5 minutes)
config-erps-inst	instance INSTANCE_ID control-vlan VLAN_ID data-vlan VLAN_ID	This command configures a new instance and specifies its control VLAN and data VLAN.
config-erps-inst	no instance INSTANCE_ID	This command removes an instance.
config-erps-inst	show	This command displays all the instance configurations.

4.6.1.2 ERPS Global Web Configuration



ERPS Global Settings

Global State: Disable

ERPS Ring Settings

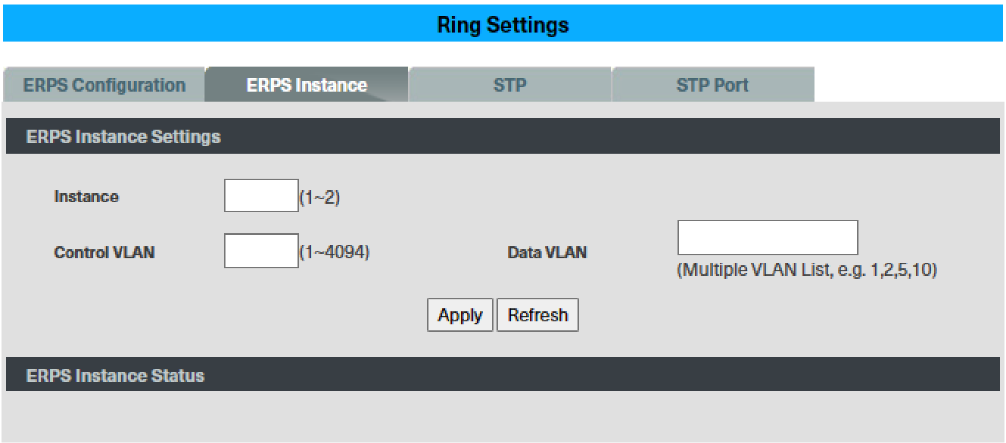
Ring ID	(1~255)	State	Disable
Ring Name		Revertive	Enable
Instance	0 (0:Default, 0~2)	Ring Type	Major-ring
Control VLAN	(1~4094)	Version	v2
Holdoff Timer (ms)	0 (0~10000)	WTR Timer (sec)	300 (5~720)
MEL	7 (0~7)	Guard Timer (ms)	500 (10~2000)
Left Port	None Normal	Right Port	None Normal

ERPS Ring Status

Parameter	Description
Global State	Enables/disables the global ERPS state.
Ring ID	Configures the ring ID. The Valid value is from 1 to 255.
State	Enables/disables the ring state.
Ring Name	Configures the ring name. (Up to 32 characters)
Revertive	Enables/disables the revertive mode.
Instance	Configures the instance for the ring. The Valid value is from 0 to 30. 0-Disable means the ERPS is running in version 1. The control VLAN of the instance should be the same as below Control VLAN.
Control VLAN	Configures the Control VLAN which is the ERPS control packets domain for the ring.
Version	Configures the version for the ring.
Hold-off Timer	Configures the Hold-off time for the ring. The Valid value is from 0 to 10000 (ms).
WTR Timer	Configures the WTR time for the ring. The Valid value is from 5

	to 12 (min).
MEL	Configures the Control MEL for the ring. The Valid value is from 0 to 7. The default is 7.
Guard Timer	Configures the Guard time for the ring. The Valid value is from 10 to 2000 (ms).
Left Port	Configures the left port and its type for the ring. The valid port type is one of Owner, Neighbor, or Normal.
Right Port	Configures the right port and its type for the ring. The valid port type is one of Owner, Neighbor, or Normal.
ERPS Status	
Ring ID	The ring ID.
Ring Name	The ring name.
State	The ring state.
Revertive	The ring revertive mode.
Control VLAN	The ring Control VLAN.
Version	The protocol version on the ring.
Hold off Timer	The Hold-off time.
WTR Timer	The WTR time.
MEL	The Control MEL.
Guard Timer	The Guard time.
Left Port	The left port.
Left Port Type	The left port types.
Right Port	The right port.
Right Port Type	The right port types.
WTB Timer	The WTB time.
Ring Status	The current ring status.
Left Port Status	The current left port status.
Right Port Status	The current right port status.

4.6.2 ERPS Instance Web Configuration



Ring Settings

ERPS Configuration | ERPS Instance | STP | STP Port

ERPS Instance Settings

Instance (1~2)

Control VLAN (1~4094)

Data VLAN (Multiple VLAN List, e.g. 1,2,5,10)

Apply Refresh

ERPS Instance Status

Parameter	Description
Instance Settings	
Instance	Configures the instance ID. The valid value is from 1 to 31.
Control VLAN	Configures the control VLAN for the instance. The valid value is from 1 to 4094.
Data VLAN	Configures the data VLAN for the instance. The valid value is from 1 to 4094. It can be one or multiple VLANs.
Instance Status	
Instance	The instance ID.
Control VLAN	The control VLAN of the instance.
Data VLAN	The data VLAN of the instance.

4.6.3 STP/RSTP

(R)STP detects, and breaks network loops and provides backup links between switches, bridges, or routers. It allows a Switch to interact with other (R)STP-compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch supports Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol

The Switch uses IEEE 802.1w RSTP that allows faster convergence of the spanning tree than STP (while also being backward compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge and then the root bridge notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database.

In STP, the port states are Blocking, Listening, Learning, and Forwarding.

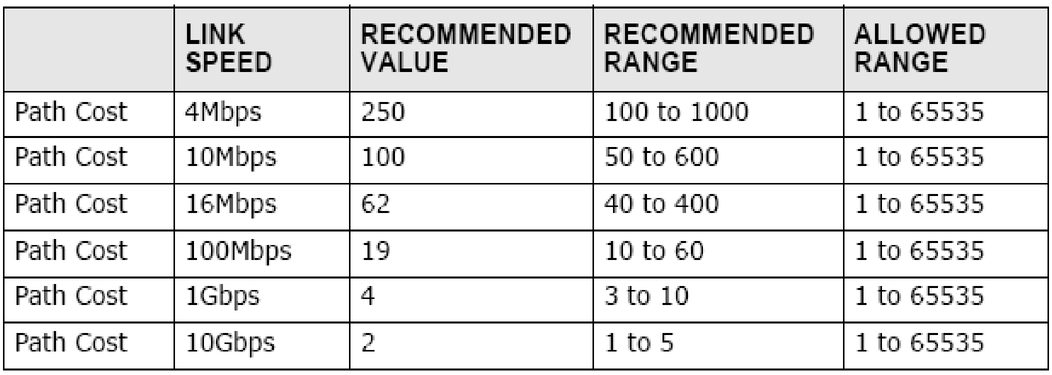
In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this document, “STP” refers to both STP and RSTP.

STP Terminology

The root bridge is the base of the spanning tree. Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 27 STP Path Costs



	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the bridge communicates with the root through the root port. The root port is the port on this Switch with the lowest path cost to the root (the root path cost). If there is no root port, then this Switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

Forward Time (Forward Delay): -- This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.

Max Age: -- This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.

Hello Time: -- This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

Path Cost: -- Path cost is the cost of transmitting a frame onto a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.

How STP Works:

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed. Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

802.1D STP

The Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. It is based on an algorithm invented by Radia Perlman while working for Digital Equipment Corporation. In the OSI model for computer networking, STP falls under layer 2. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loops must be avoided because they result in flooding the network.

The Spanning Tree Protocol (STP) is defined in the IEEE Standard 802.1D. As the name suggests, it creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches) and disables those links that are not part of the tree, leaving a single active path between any two network nodes.

STP switch port states:

- Blocking - A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail, and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in the blocking state.
- Listening - The switch processes BPDUs and awaits possible added information that would cause it to return to the blocking state.
- Learning - While the port does not yet forward frames (packets) it does learn source addresses from frames received and adds them to the filtering database (switching database)
- Forwarding - A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate they should return to the blocking state to prevent a loop.
- Disabled - Not strictly part of STP, a network administrator can manually disable a port

802.1w RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP), which provides for faster-spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP. While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a second.

RSTP bridge port roles:

- Root - A forwarding port that is the best port from the non-Root bridge to the Root bridge
- Designated - A forwarding port for every LAN segment
- Alternate - An alternate path to the root bridge. This path is different from using the root port.
- Backup - A backup/redundant path to a segment where another bridge port already connects.

- Disabled - Not strictly part of STP, a network administrator can manually disable a port

Edge Port:

They are attached to a LAN that has no other bridges attached. These edge ports transition directly to the forwarding state. RSTP continues to monitor the port for BPDUs in case a bridge is connected. RSTP can also be configured to automatically detect edge ports. As soon as the bridge detects a BPDU coming to an edge port, the port becomes a non-edge port.

Forward Delay:

The range is from 4 to 30 seconds. This is the maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forward).

Transmission Limit:

This is used to configure the minimum interval between the transmission of consecutive RSTP BPDUs. This function can only be enabled in RSTP mode. The range is from 1 to 10 seconds.

Hello Time:

Set the time at which the root switch transmits a configuration message. The range is from 1 to 10 seconds.

Bridge priority:

The bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will become the root device.

Port Priority:

Set the port priority in the switch. A low numeric value indicates a high priority. A port with lower priority is more likely to be blocked by STP if a network loop is detected. The valid value is from 0 to 240.

Path Cost:

The valid value is from 1 to 200000000. Higher-cost paths are more likely to be blocked by STP if a network loop is detected.

BPDU Guard

This is a per-port setting. If the port is enabled in the BPDU guard receives any BPDU, the port will be set to disable to avoid the error environments. The user must enable it manually

BPDU Filter

It is a feature to filter sending or receiving BPDUs on a switch port. If the port receives any BPDUs, the BPDUs will be dropped.

Notice:

If both the BPDU filter and BPDU guard are enabled, the BPDU filter has high priority.

Root Guard

The Root Guard feature forces an interface to become a designated port to prevent surrounding switches from becoming root switches. In other words, Root Guard provides a way to enforce the root bridge placement in the network. The Root Guard feature prevents a Designated Port from becoming a Root Port. If a port on which the Root Guard feature receives a superior BPDU, it moves the port into a root-inconsistent state (effectively equal to a listening state), thus maintaining the current Root Bridge status. The port can be moved to the forwarding state if no superior BPDU is received by this port for three hello time.

Default Settings

STP/RSTP	disabled.
STP/RSTP mode	RSTP.
Forward Time	15 seconds.
Hello Time	2 seconds.
Maximum Age	20 seconds.
System Priority	32768.
Transmission Limit	3 seconds.

Per port STP state	enabled.
Per port Priority	128.
Per port Edge port	disabled.
Per port BPDU filter	disabled.
Per port BPDU guard	disabled.
Per port BPDU Root guard	disabled.
Per port Path Cost	depend on port link speed.

Example: Bandwidth -> STP Path Cost Value

10 Mbps-> 100

100 Mbps-> 19

1 Gbps -> 4

0 Gbps -> 2

4.6.3.1 CLI Configuration

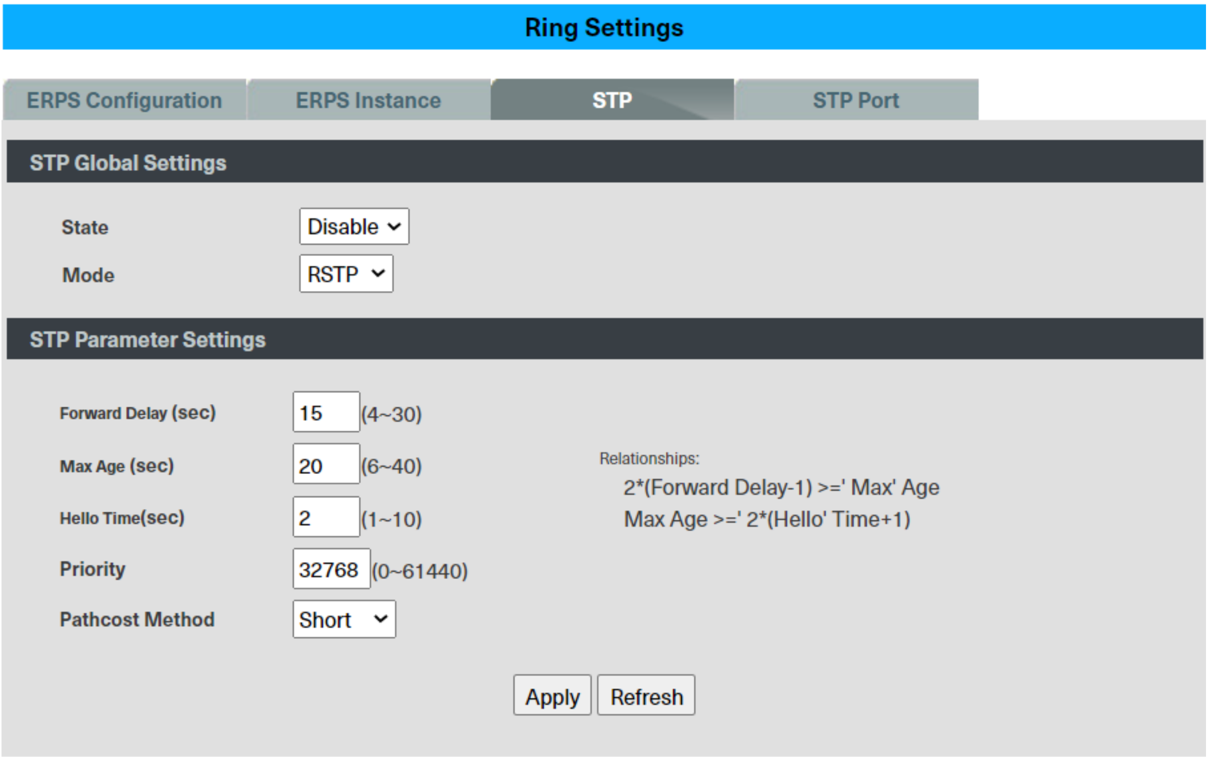
Node	Command	Description
enable	show spanningtree active	This command displays the spanning tree information for only active port(s)
enable	show spanning treeblocked ports	This command displays the spanning tree information for only blocked port(s)
enable	show spanningtree port detail PORT_ID	This command displays the spanning tree information for the interface port.
enable	show spanningtreestatistics PORT_ID	This command displays the spanning tree information for the interface port.
enable	show spanning treesummary	This command displays the summary of port states and configurations
enable	clear spanning treecounters	This command clears spanning treestatistics for all ports.
enable	clear spanning treecounters PORT_ID	This command clears spanning treestatistics for a specific port.
configure	spanning tree (disable | enable)	This command disables / enables the spanning tree function for the system.
configure	spanning treealgorithm-timer	This command configures the bridge times (forward-delay, max-age, hello-time).

	forward-time TIME max-age TIME hello-time TIME	
configure	no spanning treealgorithm-timer	This command configures the default values for forward-time & max-age & hello-time.
configure	spanning treeforward-time <4-30>	This command configures the bridge forward delay time (sec).
configure	no spanning treeforward-time	This command configures the default values for forward-time.
configure	spanning treehello-time <1-10>	This command configures the bridge hello time(sec).
configure	no spanning treehello-time	This command configures the default values for hello-time.
configure	spanning treemax-age <6-40>	This command configures the bridge message max-age time(sec).
configure	no spanning treemax-age	This command configures the default values for max-age time.
configure	spanning treemode (rstp|stp)	This command configures the spanning mode.
configure	spanning treepath cost method (short|long)	This command configures the path cost method.
configure	spanning treepriority <0-61440>	This command configures the priority for the system.
configure	no spanning treepriority	This command configures the default values for the system priority.
interface	spanning tree (disable|enable)	This command configures enables/disables the STP function for the specific port.
interface	spanning tree bpdu filter (disable|enable)	This command configures enables/disables the bpdu filter function for the specific port.
interface	spanning tree bpdu guard (disable|enable)	This command configures enables/disables the bpdu guard function for the specific port.
interface	spanning tree root guard (disable|enable)	This command enables/disables the BPDU Root guard port setting for the specific port.

interface	spanning treeedge-port (disable|enable)	This command enables/disables the edge port setting for the specific port.
interface	spanning treecost VALUE	This command configures the cost for the specific port. Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-200000000.
interface	no spanning treecost	This command configures the path cost to default for the specific port.
interface	spanning tree port-priority <0-240>	This command configures the port priority for the specific port. Default: 128.
interface	no spanning tree port-priority	This command configures the port priority to default for the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	spanning tree(disable|enable)	This command configures enables/disables the STP function for the specific port.
if-range	spanning tree bpdu filter (disable|enable)	This command configures enables/disables the bpdu filter function for the specific port.
if-range	spanning tree bpdu guard (disable|enable)	This command configures enables/disables the bpdu guard function for the specific port.
if-range	spanning tree root guard (disable|enable)	This command enables/disables the BPDU Root guard port setting for the specific port.
if-range	spanning tree edge-port (disable|enable)	This command enables/disables the edge port setting for the specific port.
if-range	spanning tree cost VALUE	This command configures the cost for the specific port. Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-200000000.

if-range	no spanning tree cost	This command configures the path cost to default for the specific port.
if-range	spanning tree port-priority <0-240>	This command configures the port priority for the specific port. Default: 128.
if-range	no spanning tree port-priority	This command configures the port priority to default for the specific port.

4.6.3.2 STP/RSTP Web Configuration



State: Disable
Mode: RSTP

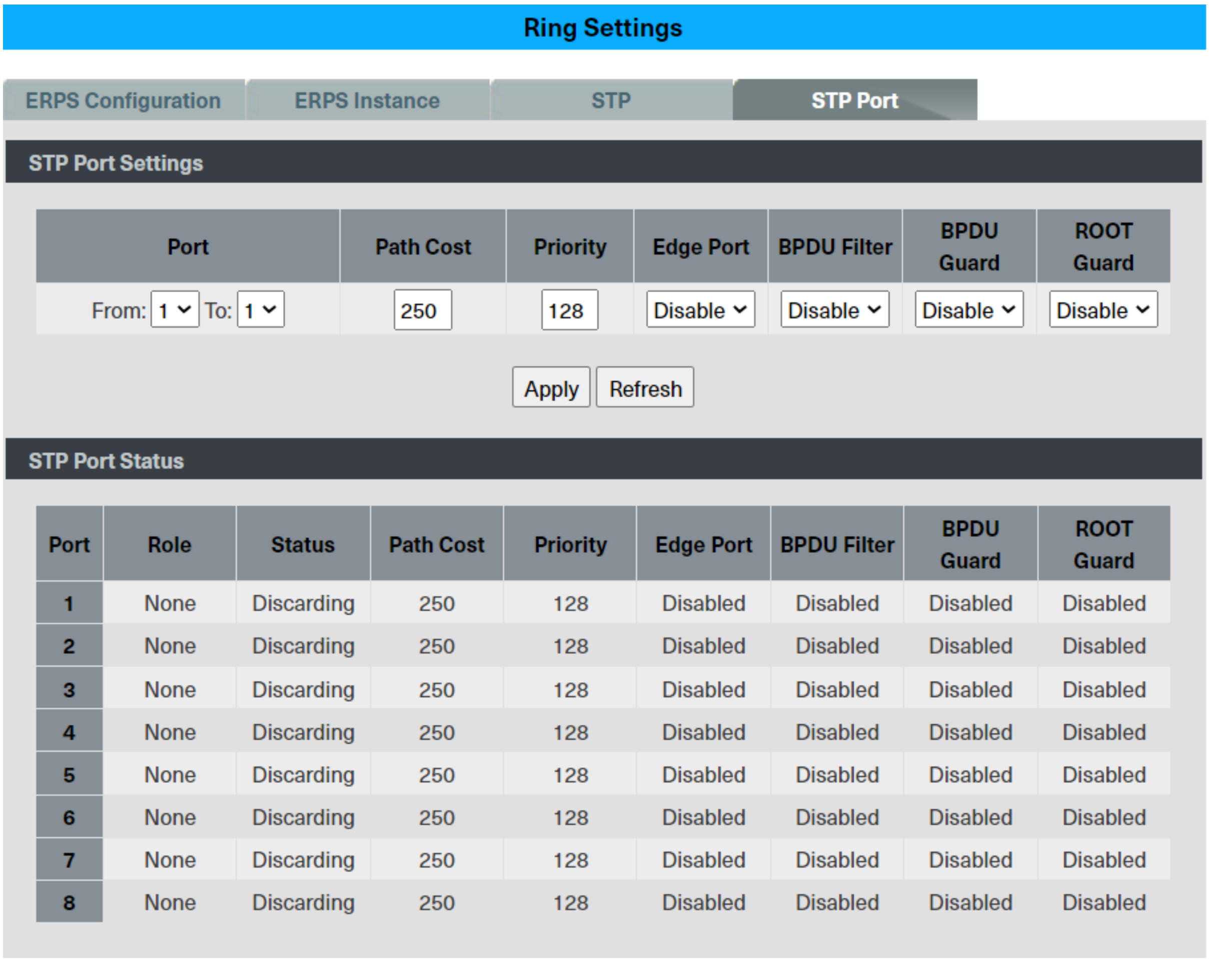
Forward Delay (sec): 15 (4~30)
Max Age (sec): 20 (6~40)
Hello Time(sec): 2 (1~10)
Priority: 32768 (0~61440)
Pathcost Method: Short

Relationships:
2*(Forward Delay-1) >=' Max' Age
Max Age >=' 2*(Hello' Time+1)

Parameter	**Description**
State	Select **Enabled** to use Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).
Mode	Select to use either Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).
Forward Delay	This is the maximum delay time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting

	information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Priority	Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Enter a value from 0~61440. The lower the numeric value you assign, the higher the priority for this bridge. Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age, and Root Forwarding Delay.
Pathcost Method	Path cost is the cost of transmitting a frame onto a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.

4.6.3.3 STP/RSTP Port Settings Web Configuration



Port	Path Cost	Priority	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
From: 1 To: 1	250	128	Disable	Disable	Disable	Disable

Port	Role	Status	Path Cost	Priority	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
1	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
2	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
3	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
4	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
5	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
6	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
7	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
8	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled

Parameter	Description
Port	Selects a port that you want to configure.
Active	Enables/Disables the spanning tree function for the specific port.
Path Cost	Configures the path cost for the specific port.
Priority	Configures the priority for the specific port.
Edge Port	Configures the port type for the specific port. Edge or Non-Edge.
BPDU Filter	Enables/Disables the BPDU filter function for the specific port.
BPDU Guard	Enables/Disables the BPDU guard function for the specific port.
ROOT Guard	Enables/Disables the BPDU root guard function for the specific port.

Port Status	
Active	The state of the STP function.
Role	The port role. Should be one of the Alternated / Designated / Root / Backup / None.
Status	The port's status. Should be one of the Discarding / Blocking / Listening / Learning / Forwarding / Disabled.
Path Cost	The port's path cost.
Priority	The port's priority.
Edge Port	The state of the edge function.
BPDU Filter	The state of the BPDU filter function.
BPDU Guard	The state of the BPDU guard function.
ROOT Guard	The state of the BPDU Root guard function.

4.7 System Settings

4.7.1 System Settings

Host Name

The **hostname** is the same as the SNMP system name. Its length is up to 64 characters.

Management VLAN

The **Management VLAN** is used to configure the switch management VLAN

4.7.1.1 CLI Configuration

Node	**Command**	**Description**
configure	hostname STRINGS	This command sets the system's network name.
eth0	management vlan VLANID	This command configures the management VLAN.

4.7.2 Modbus TCP Settings

MODBUS TCP supports diverse types of data formats for reading. The primary four types of them are:

Data Access Type		Function Code	Function Name	Note
Bit access	Physical Discrete Inputs	2	Read Discrete Inputs	Not support now
	Internal Bits or Physical Coils	1	Read Coils	Not support now
Word access (16-bit access)	Physical Input Registers	4	Read Input Registers	
	Physical Output Registers	3	Read Holding Registers	Not support now

4.7.2.1 CLI Configuration

Node	Command	Description
enable	show modbus	This command displays the current Modbus configurations.
configure	modbus (disable|enable)	This command disables / enables the Modbus on the switch.

4.8 IGMP Settings

IGMP Snooping

The IGMP snooping is for multicast traffic. The Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

The Switch can perform IGMP snooping on up to 4094 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs.

Switch then performs IGMP snooping on the first VLANs that send IGMP packets. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

Configurations

Users can enable/disable the IGMP Snooping on the Switch. Users also can enable/disable the IGMP Snooping on a specific VLAN. If the IGMP Snooping on the Switch is disabled, the IGMP Snooping is disabled on all VLANs even some of the VLAN IGMP Snooping are enabled.

Default Settings

If received packets are not received after 400 seconds, all multicast entries will be deleted.

The default global IGMP snooping state is disabled.

The default VLAN IGMP snooping state is disabled for all VLANs.

The unknown multicast packets will be dropped.

The default port Immediate Leave state is disabled for all ports.

The default port Querier Mode state is auto for all ports.

The IGMP snooping Report Suppression is disabled.

Notices: There are a global state and per VLAN states. When the global state is disabled, the IGMP snooping on the Switch is disabled even per VLAN states are enabled. When the global state is enabled, the user must enable per VLAN states to enable the IGMP Snooping on the specific VLAN

4.8.1 General Settings

4.8.1.1 CLI Configuration

Node	Command	Description

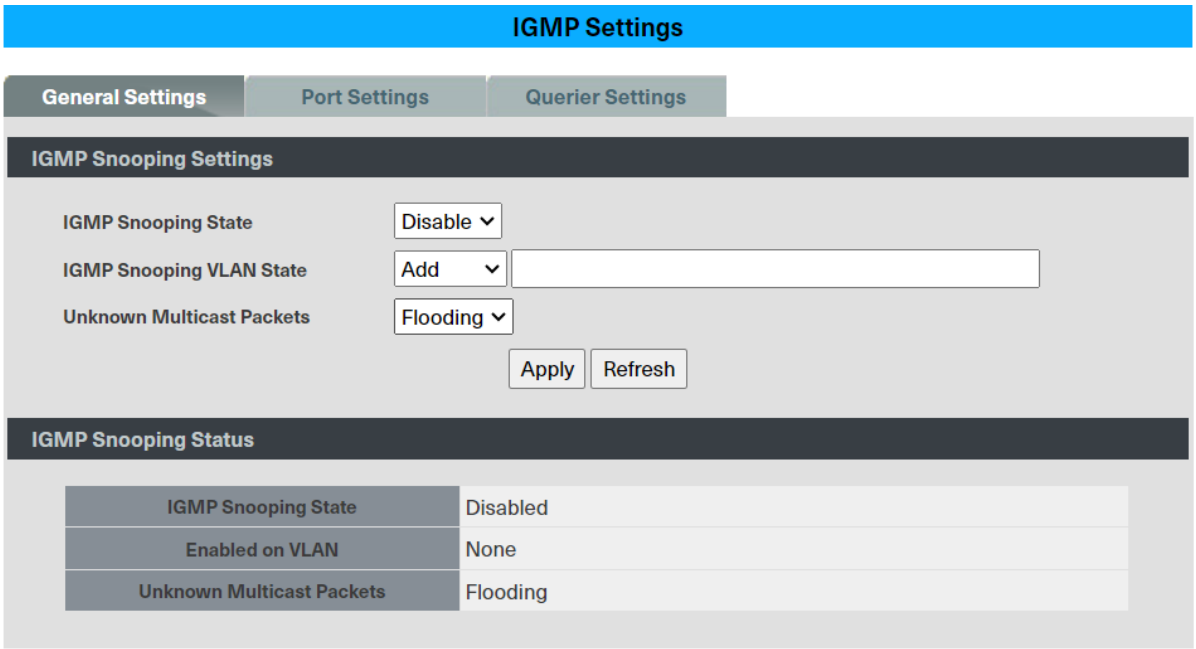
enable	show igmp-snooping	This command displays the current IGMP snooping configurations.
enable	configure terminal	This command changes the node to configure node.
configure	igmp-snooping (disable|enable)	This command **disables** / **enables** the IGMP snooping on the switch.
configure	igmp-snooping vlan VLANLISTS	This command enables the IGMP snooping function on a VLAN or range of VLANs.
configure	no igmp-snooping vlan VLANLISTS	This command disables the IGMP snooping function on a VLAN or range of VLANs.
configure	igmp-snooping unknown-multicast (drop|flooding)	This command configures the process for unknown multicast packets when the IGMP snooping function is enabled. **drop**: Drop all of the unknown multicast packets. **flooding**: Flooding the unknown multicast packets to all ports.

Example:

```
L2SWITCH(config)#igmp-snooping enable

L2SWITCH(config)#igmp-snooping vlan 1
```

4.8.1.2 Web Configuration



IGMP Snooping State: Disable
IGMP Snooping VLAN State: Add
Unknown Multicast Packets: Flooding

IGMP Snooping State	Disabled
Enabled on VLAN	None
Unknown Multicast Packets	Flooding

Parameter	Description
IGMP Snooping Settings	
IGMP Snooping State	Select **Enable** to activate IGMP Snooping to forward group multicast traffic only to ports that are members of that group. Select **Disable** to deactivate the feature.
IGMP Snooping VLAN State	Select **Add** and enter VLANs upon which the Switch is to perform IGMP snooping. The valid range of VLAN IDs is between 1 and 4094. Use a comma (,) or hyphen (-) to specify more than one VLANs. Select **Delete** and enter VLANs on which to have the Switch not perform IGMP snooping.
Unknown Multicast Packets	Specify the action to perform when the Switch receives an unknown multicast frame. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

IGMP Snooping Status	
IGMP Snooping State	This field displays whether IGMP snooping is globally enabled or disabled.
Enable on VLAN	This field displays VLANs on which the Switch is to perform IGMP snooping. None displays if you have not enabled IGMP snooping on any VLAN yet.
Unknown Multicast Packets	This field displays whether the Switch is set to **drop** or **flooding** unknown multicast packets.

4.8.2 Port Settings

Immediate Leave

When you enable IGMP Immediate-Leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN. (Immediate Leave is only supported on IGMP Version 2 hosts).

The switch uses IGMP snooping Immediate Leave to remove from the forwarding table an interface that sends a leave message without the switch sending 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. Immediate

Leave ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

Without Immediate Leave, when the switch receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP specific query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership.

Port IGMP Querier Mode

- ✓ **Auto:** The Switch uses the port as an IGMP query port if the port receives IGMP query packets.
- ✓ **Fixed:** The Switch always treats the port(s) as IGMP query port(s). This is for connecting an IGMP multicast server to the port(s). The Switch always forwards the client's report/leave packets to the port.
- ✓ Normally, the port is connected to an IGMP server.
- ✓ **Edge:** The Switch does not use the port as an IGMP query port. The IGMP query packets received by this port will be dropped.

Normally, the port is connected to an IGMP client.

Note: The Switch will forward the IGMP join and leave packets to the query port.

4.7.1.1. CLI Configuration

Node	Command	Description
enable	show igmp-snooping	This command displays the current IGMP snooping configurations.
enable	configure terminal	This command changes the node to configure node.
configure	interface IFNAME	This command enters the interface configure node.
interface	igmp-immediate-leave	This command enables the IGMP Snooping immediate leave function for the specific port.
interface	no igmp-immediate-leave	This command disables the IGMP Snooping immediate leave function for the specific port.

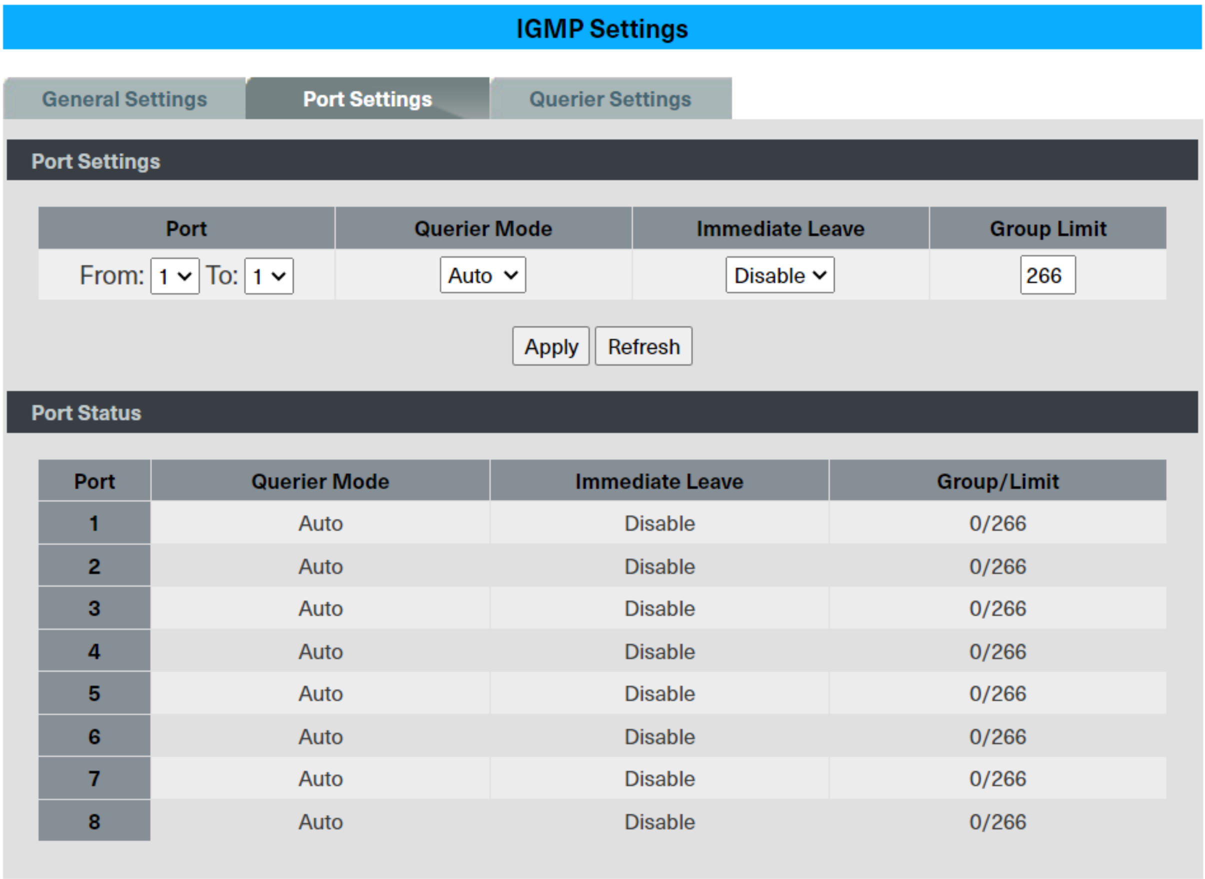
interface	igmp-group-limit VALUE	This command configures the maximum groups for the specific port.
interface	no igmp-group-limit	This command configures the default value for the limitation of the maximum groups for the specific port.
interface	igmp-querier-mode (auto|fixed|edge)	This command specifies whether or not and under what conditions the port(s) is (are) IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. (Default: auto)
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the if-range configure node.
if-range	igmp-immediate-leave	This command enables the IGMP Snooping immediate leave function for the specific ports.
if-range	no igmp-immediate-leave	This command disables the IGMP Snooping immediate leave function for the specific ports.
if-range	igmp-group-limit VALUE	This command configures the maximum groups for the specific port.
if-range	no igmp-group-limit	This command configures the default value for the limitation of the maximum groups for the specific port.

if-range	igmp-querier-mode (auto|fixed|edge)	This command specifies whether or not and under what conditions the ports is (are) IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. (Default: auto)

Example:

```
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#igmp-immediate-leave
L2SWITCH(config-if)#igmp-querier-mode fixed
L2SWITCH(config-if)#igmp-snooping group-limit 20
```

4.8.2.1 Web Configuration



Port Settings

Port	Querier Mode	Immediate Leave	Group Limit
From: 1 To: 1	Auto	Disable	266

Port Status

Port	Querier Mode	Immediate Leave	Group/Limit
1	Auto	Disable	0/266
2	Auto	Disable	0/266
3	Auto	Disable	0/266
4	Auto	Disable	0/266
5	Auto	Disable	0/266
6	Auto	Disable	0/266
7	Auto	Disable	0/266
8	Auto	Disable	0/266

Parameter	**Description**
Port Settings	
Querier Mode	Select the desired setting, **Auto**, **Fixed**, or **Edge**. **Auto** means the Switch uses the port as an IGMP query port if the port receives IGMP query packets. **Fixed** means the Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). **Edge** means the Switch does not use the port as an IGMP query port. In this case, the Switch does not keep a record of an IGMP router being connected to this port and the Switch does not forward IGMP join or leave packets to this port.
Immediate Leave	Select individual ports on which to enable immediate leave.
Group Limit	Configures the maximum group for the port or a range of ports.

Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Port Status	
Port	The port ID.
Querier Mode	The Querier mode setting for the specific port.
Immediate Leave	The Immediate Leave setting for the specific port.
Group / Limit	The current joining group count and the maximum group count.

4.8.3 Querier Settings

IGMP Querier

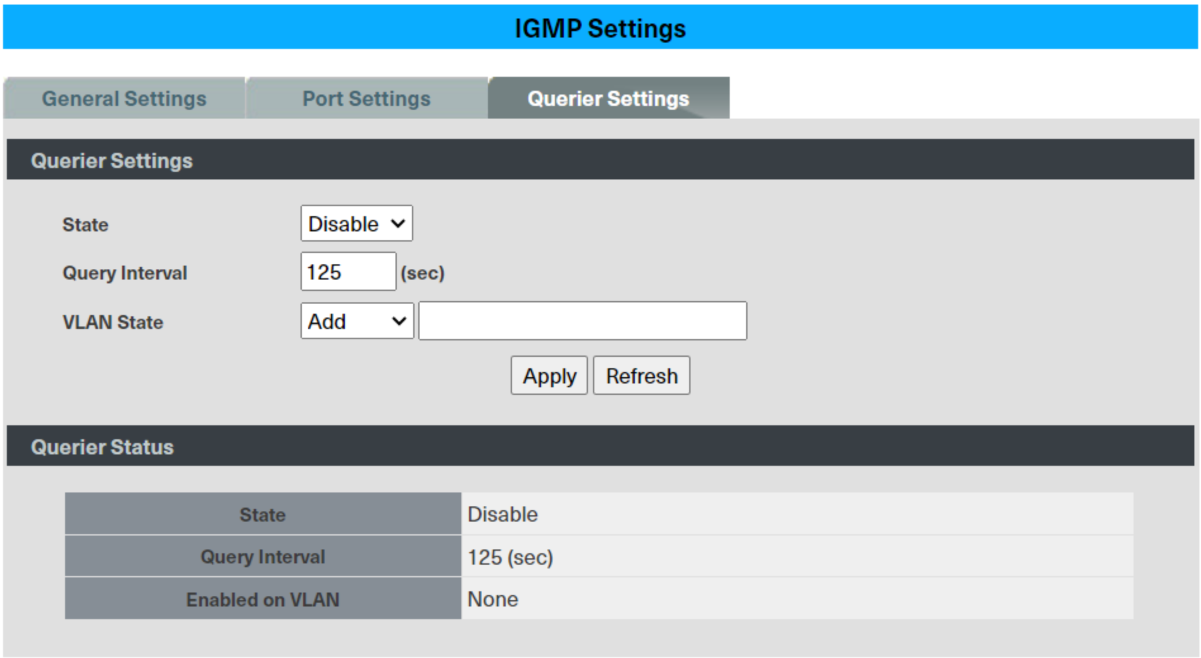
There is normally only one Querier per physical network. All multicast routers start up as a Querier on each attached network. If a multicast router hears a Query message from a router with a lower IP address, it MUST become a non-Querier on that network. If a router has not heard a Query message from another router for [Other Querier Present Interval], it resumes the role of Querier. Routers periodically [Query Interval] send a General Query on each attached network for which this router is the Querier, to solicit membership information. On startup, a router SHOULD send [Startup Query Count] General Queries spaced closely together [Startup Query Interval] to determine membership information quickly and reliably. A General Query is addressed to the all-systems multicast group (224.0.0.1), has a Group Address field of 0, and has a Max. Response Time of [Query Response Interval].

4.8.3.1 CLI Configuration

Node	Command	Description
enable	show igmp-snooping querier	This command displays the current IGMP Queriers and the querier configurations.

enable	configure terminal	This command changes the node to configure node.
configure	igmp-snooping querier (disable|enable)	This command disables / enables the IGMP snooping querier on the switch.
configure	igmp-snooping querier vlan VLANLISTS	This command enables the IGMP snooping querier function on a VLAN or range of VLANs.
configure	no igmp-snooping querier vlan VLANLISTS	This command disables the IGMP snooping querier function on a VLAN or range of VLANs.
configure	igmp-snooping query interval <2-300>	This command configures the query interval for the Querier. Unit: second.

4.8.3.2 Web Configuration



Querier Settings

State: Disable

Query Interval: 125 (sec)

VLAN State: Add

Querier Status

State	Disable
Query Interval	125 (sec)
Enabled on VLAN	None

Parameter	Description
Querier Settings	
State	This field configures the global Querier state.
Query Interval	This field configures the interval which Querier send query packet periodically.
VLAN State	This field enables the Querier state in a vlan or a range of vlan.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Querier Status	
State	This filed indicates the current global Querier status.
Query Interval	This field indicates the interval which Querier send query packet periodically.
Enable on VLAN	This field displays VLANs on which the Switch is to perform IGMP querier. None displays if you have not enabled IGMP querier on any VLAN yet.

4.8.4 IPV4 Settings

IPV4 Settings is used to configure the switch management IP by static or DHCP Client

Default Settings

The default DHCP client is disabled.
The default Static IP is 192.168.0.254
Subnet Mask is 255.255.255.0
Default Gateway is 0.0.0.0

4.8.4.1 CLI Configuration

Node	Command	Description
enable	ping IPADDR [–c COUNT]	This command sends an echo request to the destination host. The –c parameter allow the user to specific the packet count. The default count is 4.

enable	ping IPADDR [–s SIZE]	This command sends an echo request to the destination host. The –s parameter allows the user to specify the packet size. Valid range: 0 ~ 1047 bytes.
enable	ping IPADDR [–c COUNT –s SIZE]	This command sends an echo request to the destination host. The –c parameter allows the user to specify the packet count. The default count is 4. The –s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
enable	ping IPADDR [-s SIZE –c COUNT]	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4. The –s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
configure	reboot	This command reboots the system.
configure	interface eth0	This command enters the eth0 interface node to configure the system IP.
configure	configure terminal	This command changes the mode to config mode.
configure	interface eth0	This command changes the mode to eth0 mode.
eth0	show	This command displays the eth0 configurations.
eth0	IP address A.B.C.D/M	This command configures a static IP and subnet mask for the system.
eth0	IP address default-gateway A.B.C.D	This command configures the system's default gateway.
eth0	IP DHCP client (disable|enable|renew)	This command configures DHCP client function for the system. Disable: Use a static IP address on the switch. Enable & Renew: Use the DHCP client to get an IP address from DHCP server.

Example: The procedures to configure an IP address for the Switch.

To enter the configure node.

```
L2SWITCH#configure terminal
L2SWITCH(config)#
```

To enter the ETH0 interface node.

```
L2SWITCH(config)#interface eth0
L2SWITCH(config-if)#
```

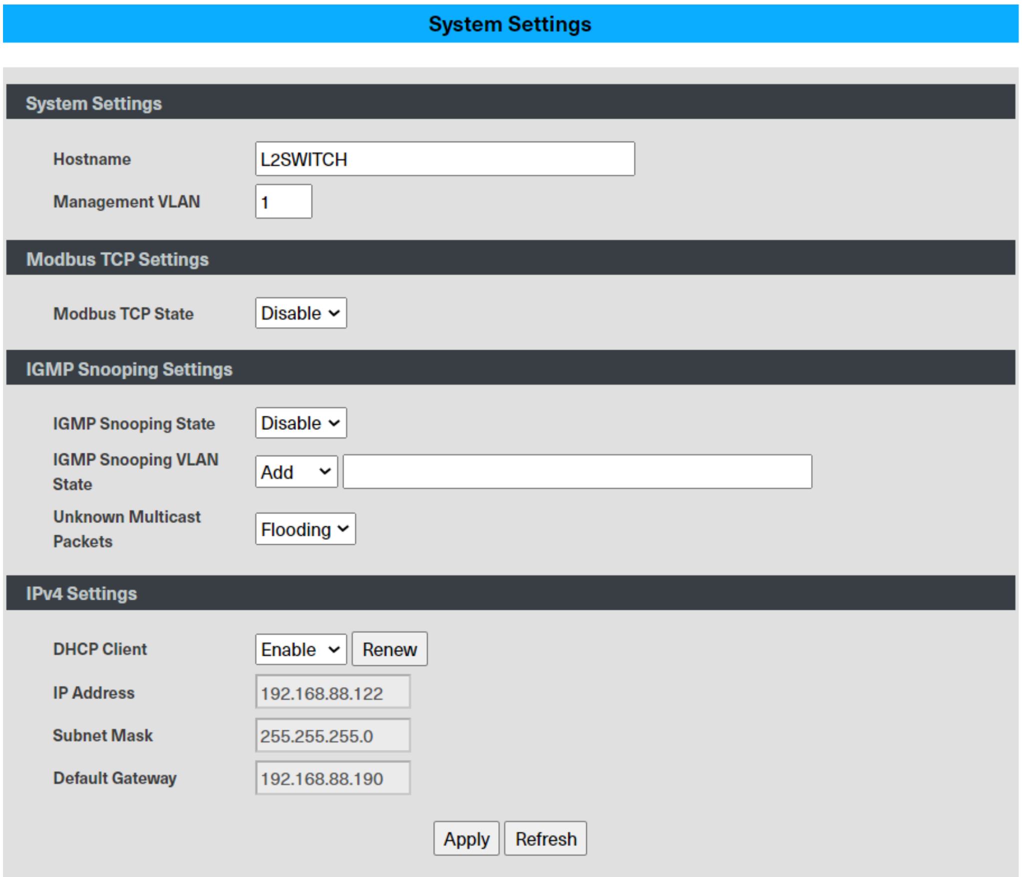
To get an IP address from a DHCP server.

```
L2SWITCH(config-if)#IP DHCP client enables
```

To configure a static IP address and a gateway for the Switch.

```
L2SWITCH(config-if)#IP address 192.168.202.111/24
L2SWITCH(config-if)#IP address default-gateway 192.168.202.1
```

4.8.4.2 Web Configuration of System Settings



System Settings

System Settings

Hostname	L2SWITCH
Management VLAN	1

Modbus TCP Settings

Modbus TCP State	Disable

IGMP Snooping Settings

IGMP Snooping State	Disable
IGMP Snooping VLAN State	Add
Unknown Multicast Packets	Flooding

IPv4 Settings

DHCP Client	Enable Renew
IP Address	192.168.88.122
Subnet Mask	255.255.255.0
Default Gateway	192.168.88.190

Parameter	Description
System Settings	
Hostname	Enter up to 64 alphanumeric characters for the name of your Switch. The hostname should be the combination of the digit or the alphabet or hyphens (-) or underscores (_).
Management VLAN	This field is to configure Management VLAN
Modbus TCP Settings	
Modbus TCP State	Select the option to enable/disable the Modbus TCP on the Switch.
IGMP Snooping Settings	
IGMP Snooping State	Select **Enable** to activate IGMP Snooping to forward group multicast traffic only to ports that are members of that group. Select **Disable** to deactivate the feature
IGMP Snooping VLAN state	Select **Add** and enter VLANs upon which the Switch is to perform IGMP snooping. The valid range of VLAN IDs is between 1 and 4094. Use a comma (,) or hyphen (-) to specify more than one VLAN. Select **Delete** and enter VLANs on which to have the Switch not perform IGMP snooping
Unknown Multicast Packets	Specify the action to perform when the Switch receives an unknown multicast frame. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
IPv4 Settings	
DHCP Client	Select **Enable** to allow the Switch to automatically get an IP address from a DHCP server. Click **Renew** to have the Switch re-get an IP address from the DHCP server. Select **Disable** if you want to configure the Switch's IP address manually.
IP Address	Configures an IPv4 address for your Switch in dotted decimal notation. For example, 192.168.0.254.
Subnet Mask	Enter the IP subnet mask of your Switch in dotted

	decimal notation for example, 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example, 192.168.1.1.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

5 Network Topology

5.1 MAP Settings

Introduction

The Topology Map is a feature to check neighbor devices' information or to configure them easily. Click the Topology Map, the system will display the topology as below.

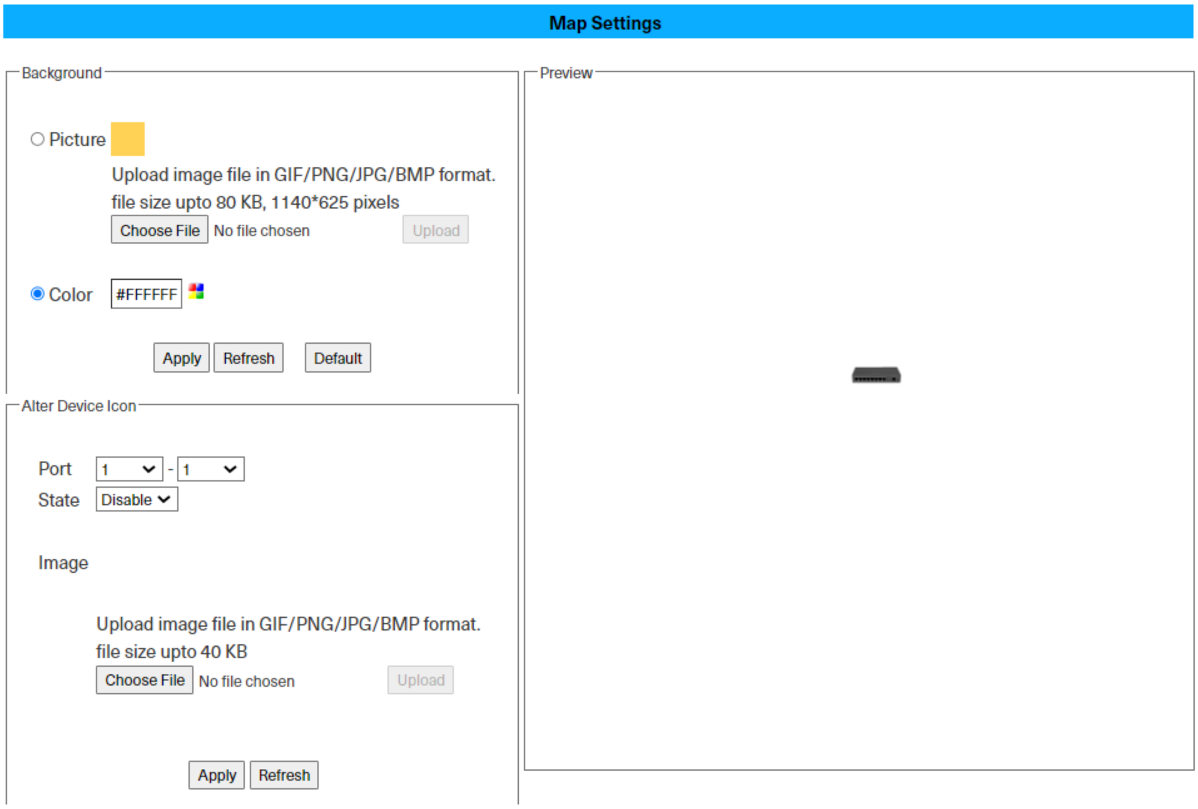
All devices connect to the Switch directly and support LLDP will be displayed on the screen. Such as the below figure, the Switch is its neighbor device. When move the mouse indicator on the Device icon, it will display a piece of information about the connected device. If the neighbor device is a Switch that supports the Lamungan Management function, click the right key of the mouse. The menu will be displayed on the screen. And then you can click an item which you want to configure the Switch.

NOTE: Topology map can be viewed on Google Chrome, Microsoft Edge, or Firefox browsers, IE will not be supportive as it does not have long time support from Microsoft for update.

5.1.1 CLI Configuration

Node	Command	Description
configure	lamungan-device background-type (picture|color)	This command is used to configure manual registration of lamungan device background-type (picture|color).

5.1.2 Map Settings Web Configuration



Map Settings

Background

○ Picture

Upload image file in GIF/PNG/JPG/BMP format.
file size upto 80 KB, 1140*625 pixels

Choose File No file chosen Upload

● Color #FFFFFF

Apply Refresh Default

Alter Device Icon

Port 1 - 1
State Disable

Image

Upload image file in GIF/PNG/JPG/BMP format.
file size upto 40 KB

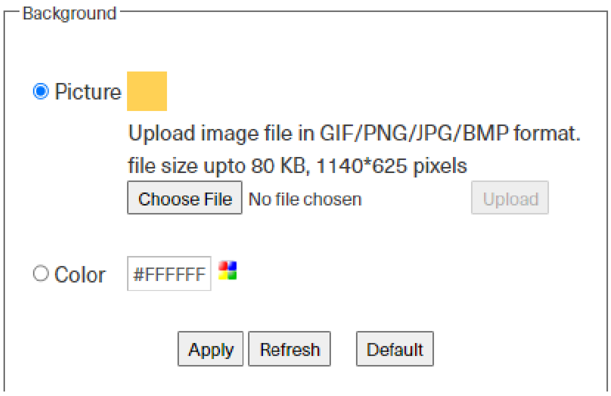
Choose File No file chosen Upload

Apply Refresh

Preview

Background Settings

You can upload your company floor layout plan picture into the background image so that you can identify easily where the switch has been placed.



Background

● Picture

Upload image file in GIF/PNG/JPG/BMP format.
file size upto 80 KB, 1140*625 pixels

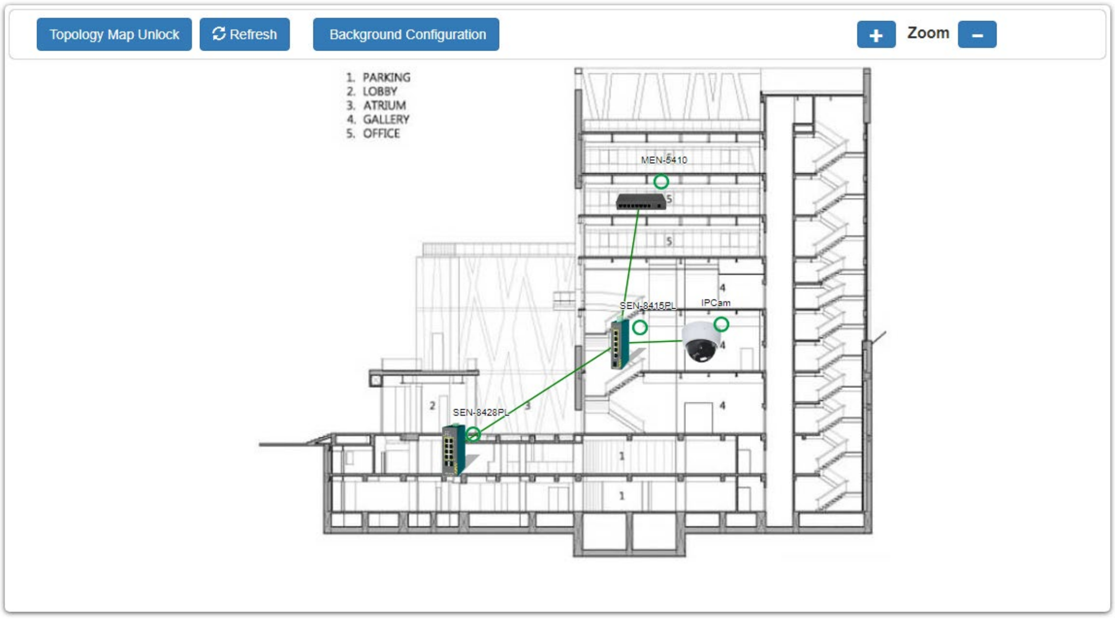
Choose File No file chosen Upload

○ Color #FFFFFF

Apply Refresh Default

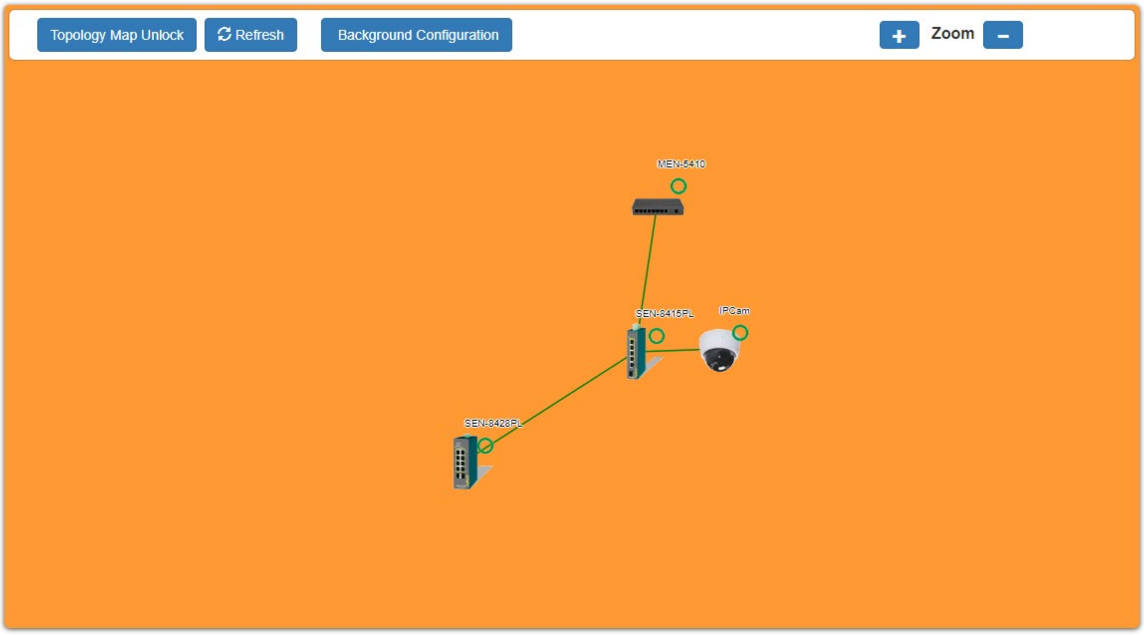
- **Picture**

  To choose a file which you want to display it in the background and the Preview window will display your select immediately. If you click the “Upgrade” button, the file will be download to the Switch and it will be applied on next reboot.



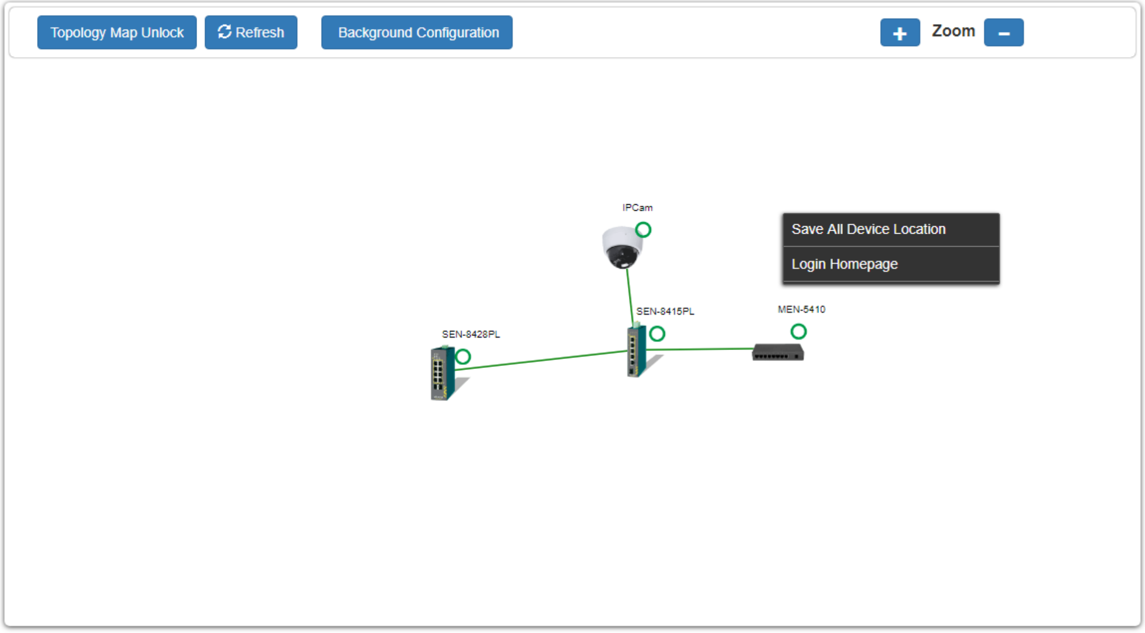
- **Color**

  Allow user to select standard color for the background and the Preview window will display your select immediately.



Client Switch Management

By Right clicking on the neighbor non-lite Switch, you get this menu, and you can configure as shown below.



Non-lite Switch menu:

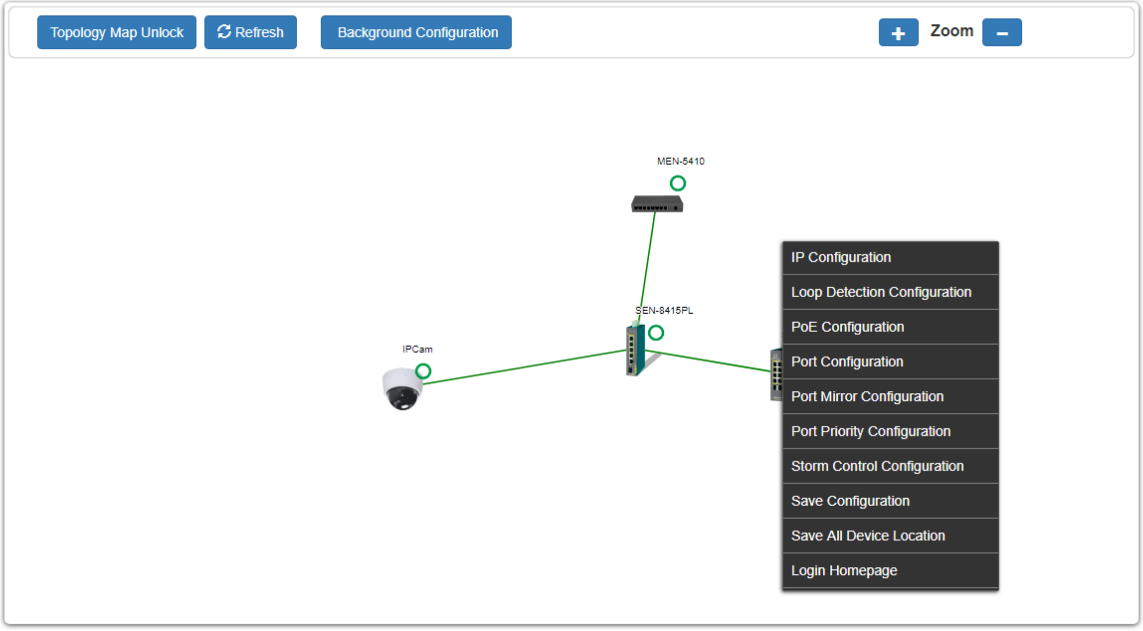
- Save All Device Location

  To fix the location of all devices on the map, so that it restores its places after refresh.

- Login Web GUI

  To log in to the client device web GUI and make necessary changes.

By Right clicking on the neighbor lite switch (SEN-8428PL) you get this menu, and you can configure as shown below.



5.2 Neighbor Devises

5.2.1 LLDP

Introduction

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 station's 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).

Default Settings

The LLDP on the Switch is enabled.

Tx Interval: 30 seconds.

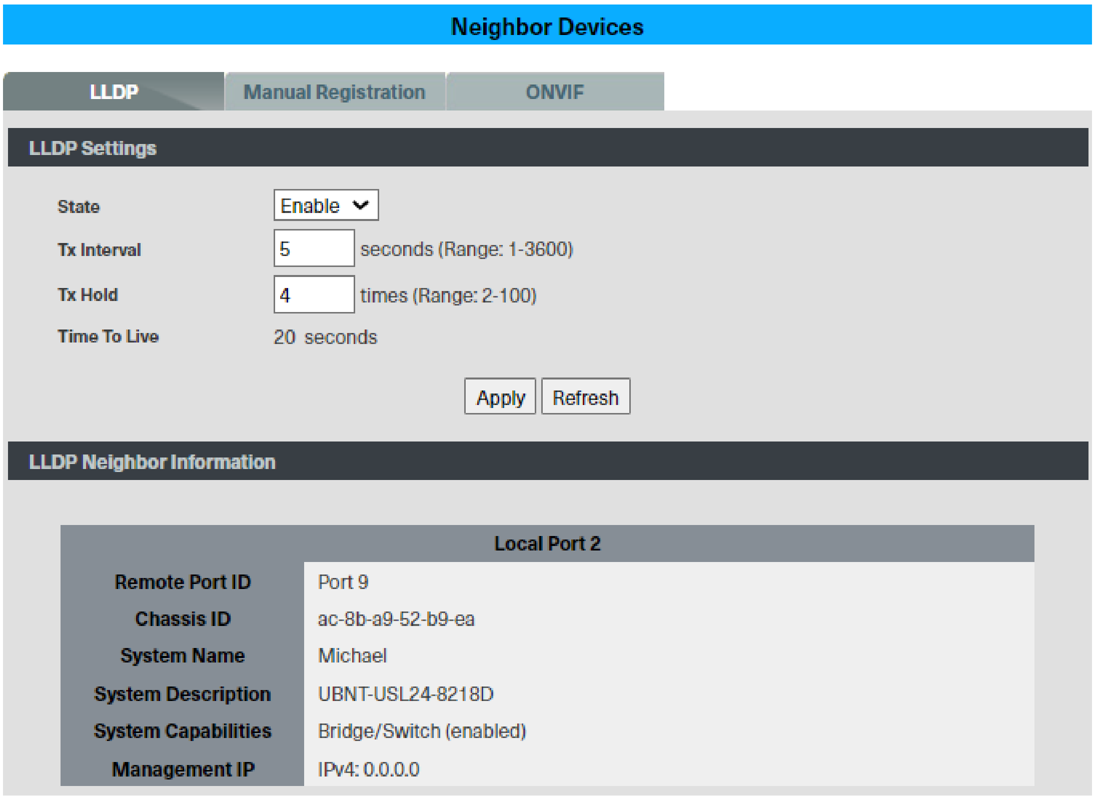
Tx Hold: 4 times.

Time To Live: 120 seconds.

5.2.1.1 CLI Configuration

Node	Command	Description
enable	show LLDP	This command displays the LLDP configurations.
enable	show LLDP neighbor	This command displays all the ports' neighbor information.
configure	LLDP (disable|enable)	This command globally enables / disables the LLDP function on the Switch.
configure	LLDP tx-interval	This command configures the interval to transmit the LLDP packets.
configure	LLDP tx-hold	This command configures the tx-hold time which determines the TTL of the Switch's message. (TTL=tx-hold * tx-interval)
interface	LLDP-agent (disable|enable|rx-only|tx-only)	This command configures the LLDP agent function. disable – Disable the LLDP on the specific port. enable – Transmit and Receive the LLDP packet on the specific port. tx-only – Transmit the LLDP packet on the specific port only. rx-only – Receive the LLDP packet on the specific port.
configure	interface range gigabitethernet1/0 / PORTLISTS	This command enters the interface configure node.
if-range	LLDP-agent (disable|enable|rx-only|tx-only)	This command configures the LLDP agent function. disable – Disable the LLDP on the specific port. enable – Transmit and Receive the LLDP packet on the specific port. tx-only – Transmit the LLDP packet on the specific port only. rx-only – Receive the LLDP packet on the specific port.

5.2.1.2 LLDP Web configuration



State: Enable

Tx Interval: 5 seconds (Range: 1-3600)

Tx Hold: 4 times (Range: 2-100)

Time To Live: 20 seconds

Local Port 2	
Remote Port ID	Port 9
Chassis ID	ac-8b-a9-52-b9-ea
System Name	Michael
System Description	UBNT-USL24-8218D
System Capabilities	Bridge/Switch (enabled)
Management IP	IPv4: 0.0.0.0

Parameter	Description
LLDP Settings	
State	Globally enables / disables the LLDP on the Switch.
Apply	Click **Apply** to take effect the settings.
LLDP Neighbor Information	
Local Port	The local port ID.
Remote Port ID	The connected port ID.
Chassis ID	The neighbor’s chassis ID.
System Name	The neighbor’s system name.
System Description	The neighbor’s system Description.
System Capabilities	The neighbor’s capability.
Management IP	The neighbor’s management address.

5.2.2 Manual Registration

Introduction

If devices do not support LLDP and ONVIF, user must enter the details of it by manually under manual registration. The function support four types, IP-Cam, PLC, Switch, and PC.

5.2.2.1 CLI Configuration

Node	Command	Description
enable	show lamungan-device	This command displays the current manual registration configuration of lamungan device.
configure	lamungan-device type (IPcam|plc|switch|pc)	This command is used to configure manual registration of lamungan device type like ((IPcam|plc|switch|pc) .
configure	no lamungan-device mac	This command is deleted configure of manual registration lamungan device using mac of ((IPcam|plc|switch|pc) .
configure	lamungan-device background-type (picture|color)	This command is used to configure manual registration of lamungan device background-type (picture|color).

Example:

```
L2SWITCH(config)#lamungan-device type pc mac F8:28:19:5C:64:A3 IP 192.168.0.200 product-name maddy system-name PC
```

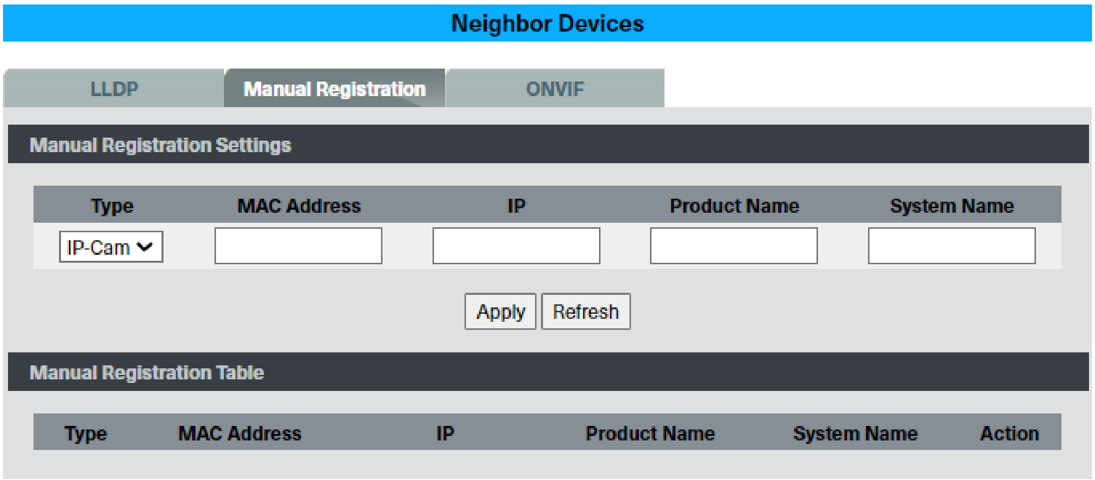
```
L2SWITCH#show lamungan-device
```

```
L2SWITCH(config)#lamungan-device background-type picture picture-value ems_custom_bg.cfg color-value ffff
```

```
L2SWITCH(config)#lamungan-device background-type color picture-value custom.cfg color-value ffff
```

5.2.2.2 Manual Registration Web Configuration

For devices which do not support ONVIF or LLDP, User can input the device's MAC address and then the Switch will discover the device and display it on the Lamungan Map.



Manual Registration Settings

Type	MAC Address	IP	Product Name	System Name
IP-Cam				

Manual Registration Table

Type	MAC Address	IP	Product Name	System Name	Action

Parameter	Description
Manual Registration Settings	
Type (IPcam|plc|switch|pc)	User can select the type of the device for manual registration like (IPcam|plc|switch|pc) connected as neighbor device to switch.
MAC Address	The MAC address of the device selected for manual registration.
IP	User can configure IP address of the manual registration device connected
Product Name	User can configure name of the product selected for manual registration
System Name	User can configure the system name for the manual registration
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Manual Registration Table	
Type	The kind of devices connected to switch.
MAC Address	Display The MAC address of the configured device.
IP	Display the IP address of the configured device

Product Name	Display the name of the product configured.
System Name	Display the system name assigned manually
Action	Whether to delete entered device or not.

5.2.3 ONVIF

ONVIF is an open industry forum that provides and promotes standardized interfaces for effective interoperability of IP-based physical security products.

The Switch use ONVIF to discovery if there is ONVIF device connected to the Switch.

ONVIF settings and ONVIF Neighbor

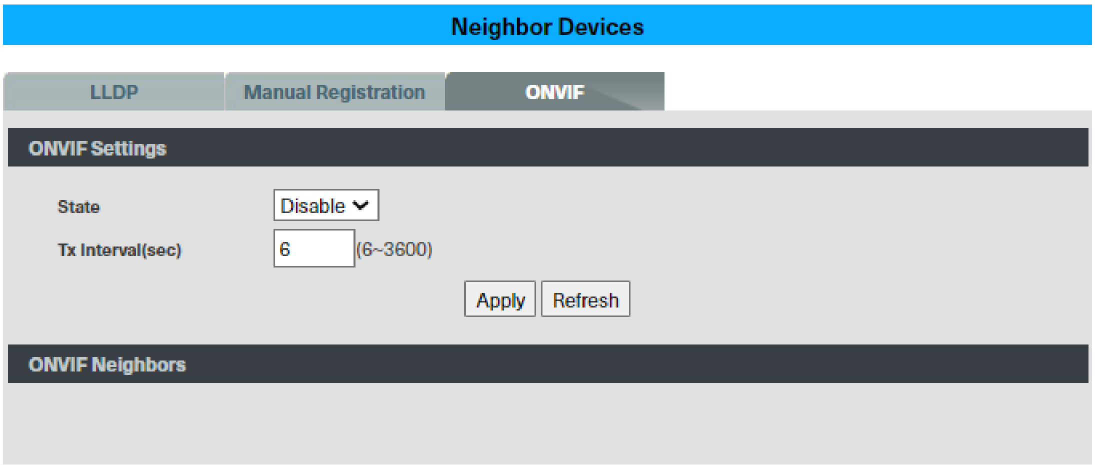
The page shows the detail information about ONVIF settings and ONVIF devices connected to the Switch. The Switch displays ONVIF devices up to total port count, SEN-8428PL shows upto 10 ONVIF devices connected to it. If one or more ONVIF devices are connected to the same port it displays the last ONVIF device gets connect to it.

5.2.3.1 CLI Configuration

Node	Command	Description
enable	show onvif neighbors	This command displays the onvif neighbor discovery.
configure	onvif enable	This command is used to enable onvif service on device .
configure	onvif disable	This command is used to disable onvif service on device .
configure	onvif binding-ports	This command is used to configure onvif binding ports .
configure	no onvif binding-ports	This command is used to delete onvif binding ports .
configure	onvif tx-interval <6-3600> Unit: second. (Default: 6)	This command is used to configure onvif tx-interval discovery time from the range of 6-3600 seconds default time is 6 seconds

configure	no onvif tx-interval	This command is used to delete onvif tx-interval discovery time from the range of 6-3600 seconds default time is 6 seconds

5.2.3.2 ONVIF Web Configuration



State: Disable

Tx Interval(sec): 6 (6~3600)

Parameter	**Description**
ONVIF Settings	
State	Select option to enable / disable the ONVIF feature on the Switch.
Tx Interval	Configures the sending ONVIF discovery packet interval. Valid range is 6 ~ 3600 seconds.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
ONVIF Neighbor Information	
Port	The connected port of the ONVIF device.
IP Address	The IP address of the ONVIF device.
MAC Address	The MAC address on the ONVIF device.
VLAN ID	The VLAN ID of the ONVIF device join.
Product Name	Name of the product added
Product Type	What kind of product that is added
Model	Model of the product

Location	Location where it is placed
Web Service Address	Address of the web service of that camera

5.3 Topology Map

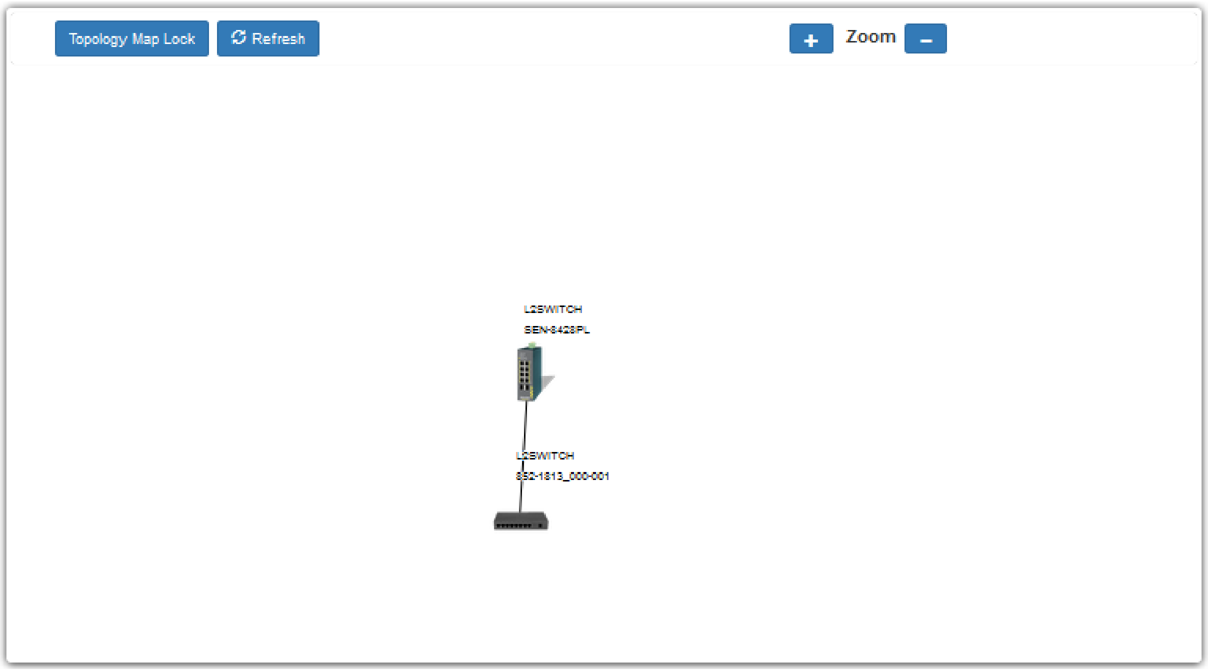
Introduction

The Topology Map is a feature to check neighbor devices' information or to configure them easily. Click the Topology Map, the system will display topology as below.

All devices connect to the Switch directly and support LLDP will be displayed on the screen. Such as below figure, the MEN-5410 is its neighbor device. When move the mouse indicator on the MEN-5410 icon, it will display a few information about the MEN-5410. If the neighbor device is a Switch which supports Lamungan server function, click the right key of the mouse. The menu will be displayed on the screen. And then you can click an item which you want to configure the Switch.

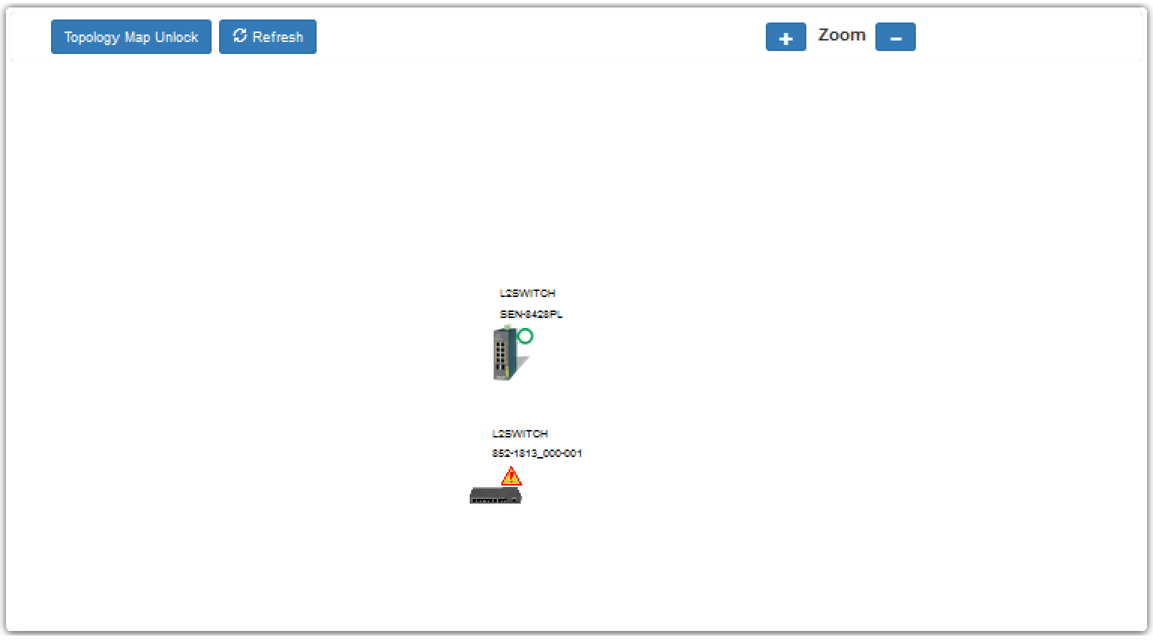
NOTE: Topology map can be viewed only on Google or Firefox browsers.

Web Configuration of Topology MAP

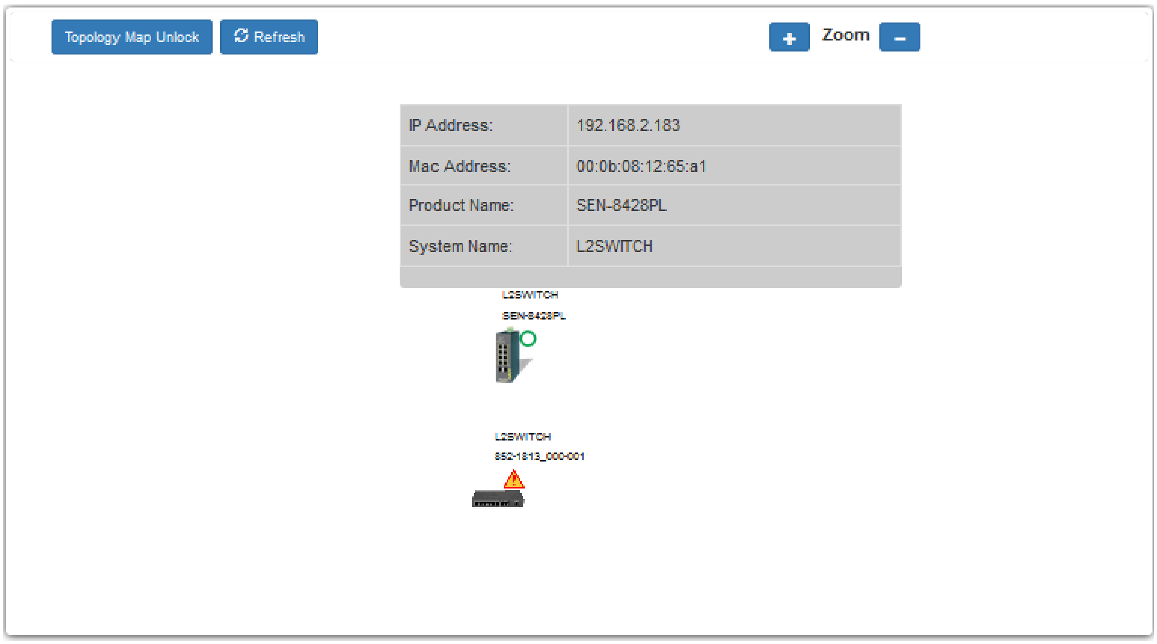


When you click the "Topology Map Lock," the screen will appear as below:

The green circle on the devices indicates they are working normally.



You can view the basic details of the devices connected to the host, by placing the cursor on it.



IP Address:	192.168.2.183
Mac Address:	00:0b:08:12:65:a1
Product Name:	SEN-8428PL
System Name:	L2SWITCH

When there is something wrong with the device (SEN-8428PL), the screen will appear as below. So that you can find the details of events that have gone wrong and correct it.

6 Security

6.1 802.1x

Introduction

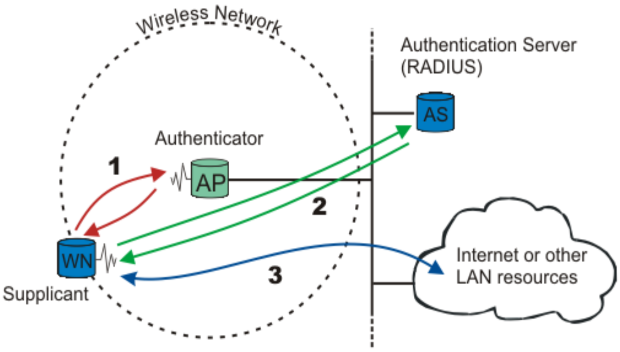
IEEE 802.1X is an IEEE Standard for port-based Network Access Control ("port" meaning a single point of attachment to the LAN infrastructure). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN, either establishing a point-to-point connection or preventing it if authentication fails. It is used for most wireless 802.11 access points and is based on the Extensible Authentication Protocol (EAP).

802.1X provides port-based authentication, which involves communications between a supplicant, authenticator, and authentication server. The supplicant is often software on a client device, such as a laptop, the authenticator is a wired Ethernet switch or wireless access point, and an authentication server is generally a RADIUS database. The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity is authorized. An analogy to this is providing a valid passport at an airport before being allowed to pass through security to the terminal. With 802.1X port-based authentication, the supplicant provides credentials, such as Username/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the credentials are valid (in the authentication server database), the supplicant (client device) is allowed to access resources located on the protected side of the network.

Upon detection of the new client (supplicant), the port on the switch (authenticator) is enabled and set to the "**unauthorized**" state. In this state, only 802.1X traffic is allowed; other traffic, such as DHCP and HTTP, is blocked at the network layer (Layer 3). The authenticator sends out the EAP-Request identity to the supplicant, the supplicant responds with the EAP-response packet that the authenticator forwards to the authenticating server. If the authenticating server accepts the request, the authenticator sets the port to the "authorized" mode and normal traffic is allowed. When the supplicant logs off, it sends an EAP-logoff message to the authenticator. The authenticator then sets the port to the "unauthorized" state, once again blocking all non-EAP traffic.

The following figure illustrates how a client connecting to an IEEE

802.1xauthentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a Username and password.



When the client provides the login credentials, the Switch sends an authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

Local User Accounts

By storing user profiles locally on the Switch, your Switch can authenticate users without interacting with a network authentication server. However, there is a limit on the number of users you may authenticate in this way.

Guest VLAN:

The Guest VLAN in IEEE 802.1x port authentication on the switch to provide limited services to clients, such as downloading the IEEE 802.1x client. These clients might be upgrading their system for IEEE 802.1x authentication.

When you enable a guest VLAN on an IEEE 802.1x port, the switch assigns clients to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.

Port Parameters:

- **Admin Control Direction:**

  both - drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication.

  in - drop only incoming packets on the port when a user has notpassed802.1x port authentication.

- **Re-authentication:**
  Specify if a subscriber must periodically re-enter his or her Username and password to stay connected to the port.

- **Reauth-period:**
  Specify how often a client must re-enter his or her username and password to stay connected to the port. The acceptable range for this field is 0 to 65535 seconds.

- **Port Control Mode:**
  Auto : Users can access network after authenticating.

  Force-authorized : Users can access network without authentication.

  Force-unauthorized: Users cannot access network.

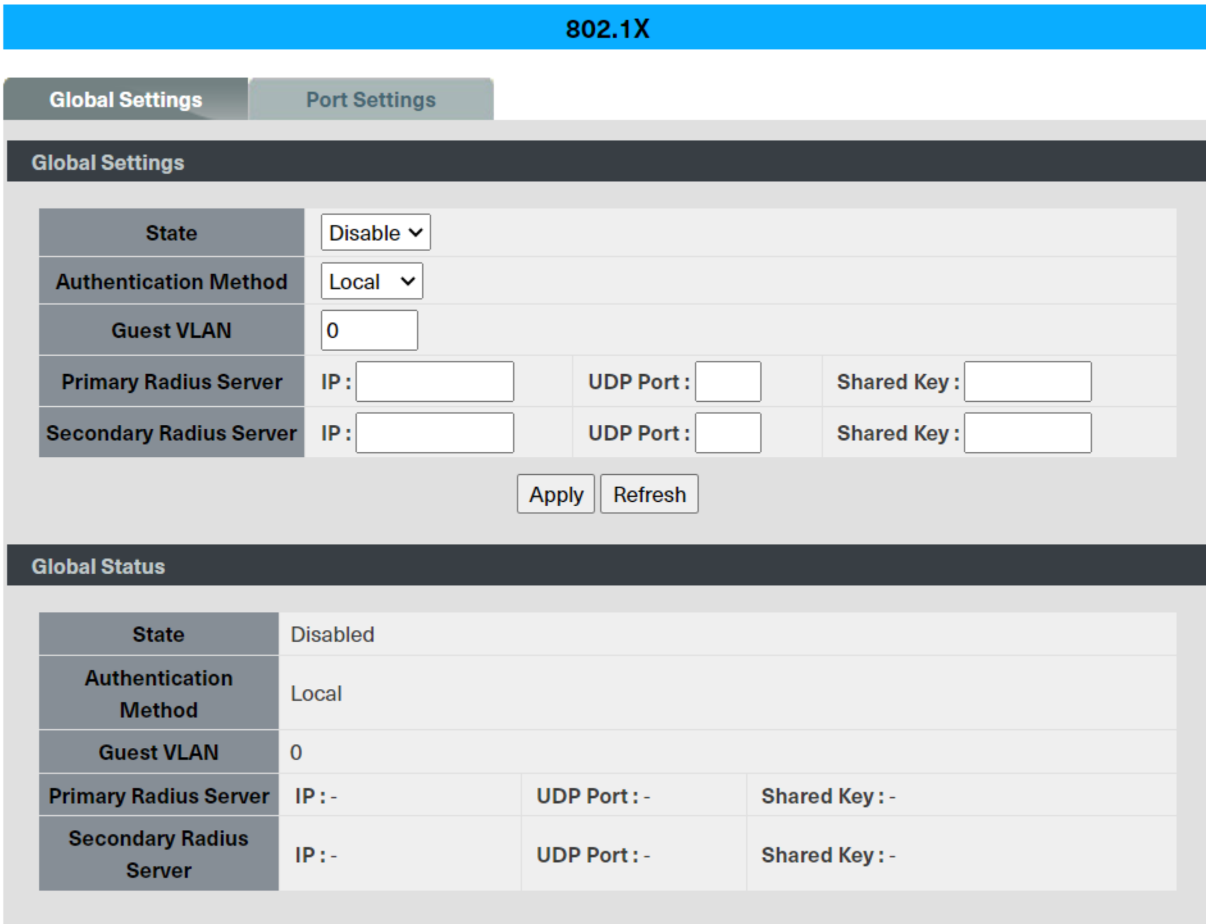
- **Quiet Period:**
  Specify a period of the time the client must wait before the next re-authentication attempt. This will prevent the Switch from becoming overloaded with continuous re-authentication attempts from the client. The acceptable range for this field is 0 to 65535 seconds.

- **Server Timeout:**
  The server-timeout value is used for timing out the Authentication Server.

- **Supp-Timeout:**
  The supp-timeout value is the initialization value used for timing out a Supplicant.

- **Max-req Time:**
  Specify the number of times the Switch will try to connect to the authentication server before determining the server is down. The acceptable range for this field is 1 to 10 times.

6.1.1 Global Settings 802.1X



802.1X

Global Settings | Port Settings

Global Settings

State	Disable		
Authentication Method	Local		
Guest VLAN	0		
Primary Radius Server	IP :	UDP Port :	Shared Key :
Secondary Radius Server	IP :	UDP Port :	Shared Key :

Apply Refresh

Global Status

State	Disabled		
Authentication Method	Local		
Guest VLAN	0		
Primary Radius Server	IP : -	UDP Port : -	Shared Key : -
Secondary Radius Server	IP : -	UDP Port : -	Shared Key : -

Parameter	Description
State	Select **Enable** to permit 802.1 x authentications on the Switch. Note: You must first enable 802.1 x authentications on the Switch before configuring it on each port.
Authentication Method	Select whether to use **Local** or **RADIUS** as the authentication method. The **Local** method of authentication uses the “guest” and “user” user groups of the user account database on the Switch itself to authenticate. However, only a certain number of accounts can exist at one time. **RADIUS** is a security protocol used to authenticate users by means of an external server instead of an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS allows you to validate an unlimited number of

	users from a central location.
Guest VLAN	Configure the guest vlan.
Primary Radius Server	When **RADIUS** is selected as the 802.1x authentication method, the **Primary Radius Server** will be used for all authentication attempts.
IP Address	Enter the IP address of an external RADIUS server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for authentication is **1812**.
Share Key	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.
Second Radius Server	This is the backup server used only when the **Primary Radius Server** is down.
Global Status	
State	This field displays if 802.1x authentication is **Enabled** or **Disabled**.
Authentication Method	This field displays if the authentication method is **Local** or **RADIUS**.
Guest VLAN	The field displays the guest vlan.
Primary Radius Server	This field displays the IP address, UDP port and shared key for the **Primary Radius Server**. This will be blank if nothing has been set.
Secondary Radius Server	This is the backup server used only when the **Primary Radius Server** is down.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

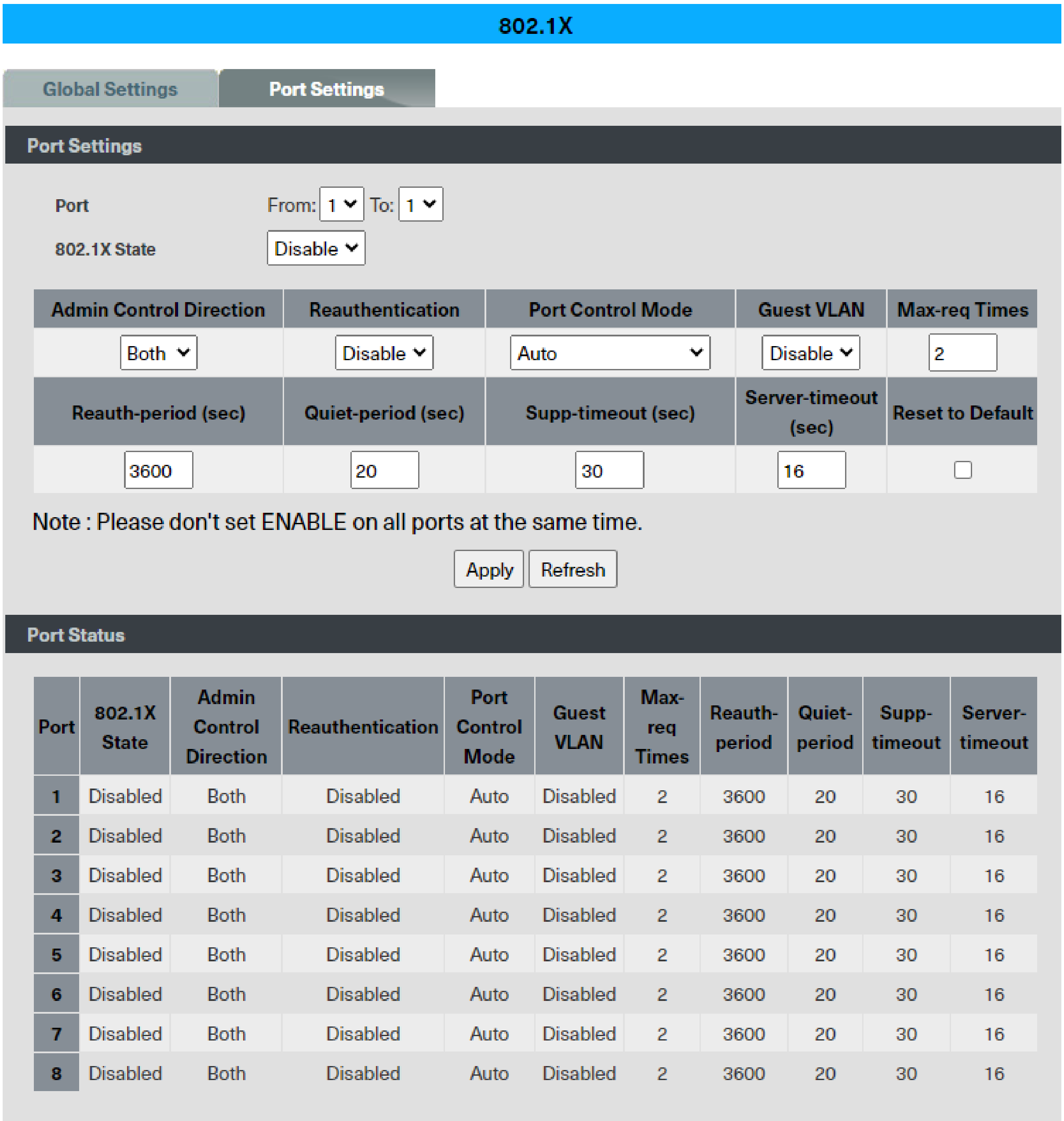
6.1.1.1 CLI Configuration

Node	Command	Description
enable	show dot1x	This command displays the current 802.1x configurations.

enable	show dot1x username	This command displays the current user accounts for the local authentication.
enable	show dot1x accounting-record	This command displays the local accounting records.
configure	dot1x authentication (disable|enable)	This command enables/disables the 802.1x authentication on the switch.
configure	dot1x authentic-method (local|radius)	This command configures the authentic method of 802.1x.
configure	no dot1x authentic-method	This command configures the authentic method of 802.1x to default.
configure	dot1x radius primary-server-IP <IP> port PORTID	This command configures the primary radius server.
configure	dot1x radius primary-server-IP <IP> port PORTID key KEY	This command configures the primary radius server.
configure	dot1x radius secondary-server-IP <IP> port PORTID	This command configures the secondary radius server.
configure	dot1x radius secondary-server-IP <IP> port PORTID key KEY	This command configures the secondary radius server.
configure	no dot1x radius secondary-server-IP	This command removes the secondary radius server.
configure	dot1x username <STRING> passwd <STRING>	This command configures the user account for local authentication.
configure	no dot1x username <STRING>	This command deletes the user account for local authentication.
configure	dot1x accounting (disable|enable)	This command enables/disables the dot1x local accounting records.

configure	dot1x guest-vlan VLANID	This command configures the guest vlan.
configure	no dot1x guest-vlan	This command removes the guest vlan.
interface	dot1x admin-control-direction (both|in)	This command configures the control direction for blocking packets.
interface	dot1x default	This command sets the port configuration to default settings.
interface	dot1x max-req <1-10>	This command sets the max-req times of a port. (1~10).
interface	dot1x port-control (auto | force-authorized | force-unauthorized)	This command configures the port control mode on the port.
interface	dot1x authentication (disable|enable)	This command enables/disables the 802.1x on the port.
interface	dot1x reauthentication (disable|enable)	This command enables/disables re-authentication on the port.
interface	dot1x timeout quiet-period	This command configures the quiet-period value on the port.
interface	dot1x timeout server-timeout	This command configures the server-timeout value on the port.
interface	dot1x timeout reauth-period	This command configures the re-auth-period value on the port.
interface	dot1x timeout supp-timeout	This command configures the supp-timeout value on the port.
interface	dot1x guest-vlan (disable|enable)	This command configures the 802.1x state on the port.

6.1.2 Web Configuration 802.1X Port Settings



802.1X

Global Settings | Port Settings

Port Settings

Port From: 1 To: 1

802.1X State: Disable

Admin Control Direction	Reauthentication	Port Control Mode	Guest VLAN	Max-req Times
Both	Disable	Auto	Disable	2
Reauth-period (sec)	**Quiet-period (sec)**	**Supp-timeout (sec)**	**Server-timeout (sec)**	**Reset to Default**
3600	20	30	16	□

Note : Please don't set ENABLE on all ports at the same time.

Apply | Refresh

Port Status

Port	802.1X State	Admin Control Direction	Reauthentication	Port Control Mode	Guest VLAN	Max-req Times	Reauth-period	Quiet-period	Supp-timeout	Server-timeout
1	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
2	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
3	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
4	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
5	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
6	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
7	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16
8	Disabled	Both	Disabled	Auto	Disabled	2	3600	20	30	16

Parameter	**Description**
Port	Select a port number to configure.
802.1x State	Select **Enable** to permit 802.1 x authentications on the port. You must first enable 802.1 x authentications on the Switch before configuring it on each port.
Admin Control Direction	Select **Both** to drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication.

	Select **In** to drop only incoming packets on the port when a user has not passed 802.1x port authentication.
Re-authentication	Specify if a subscriber must periodically re-enter his or her Username and password to stay connected to the port.
Port Control Mode	Select **Auto** to require authentication on the port. Select **Force Authorized** to always force this port to be authorized. Select **Force Unauthorized** to always force this port to be unauthorized. No packets can pass through this port.
Guest VLAN	Select **Disable** to disable Guest VLAN on the port. Select **Enable** to enable Guest VLAN on the port.
Max-req Time	Specify the number of times the Switch will try to connect to the authentication server before determining the server is down. The acceptable range for this field is 1 to 10 times.
Reauth period	Specify how often a client must re-enter his or her username and password to stay connected to the port. The acceptable range for this field is 0 to 65535 seconds.
Quiet period	Specify a period of the time the client must wait before the next re-authentication attempt. This will prevent the Switch from becoming overloaded with continuous re-authentication attempts from the client. The acceptable range for this field is 0 to 65535 seconds.
Supp timeout	Specify how long the Switch will wait before communicating with the server. The acceptable range for this field is 0 to 65535 seconds.
Server timeout	Specify how long the Switch to time out the Authentication Server. The acceptable range for this field is 0 to 65535 seconds.
Reset to Default	Select this and click **Apply** to reset the custom 802.1x port authentication settings back to default.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Port Status	
Port	This field displays the port number.

802.1x State	This field displays if 802.1 x authentications is **Enabled** or **Disabled** on the port.
Admin Control Direction	This field displays the Admin Control Direction. **Both** will drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication. **In** will drop only incoming packets on the port when a user has not passed 802.1x port authentication.
Re-authentication	This field displays if the subscriber must periodically re-enter his or her username and password to stay connected to the port.
Port Control Mode	This field displays the port control mode. **Auto** requires authentication on the port. **Force Authorized** forces the port to be authorized. **Force Unauthorized** forces the port to be unauthorized. No packets can Pass through the port.
Guest VLAN	This field displays the Guest VLAN setting for hosts that have not passed authentication.
Max-req Time	This field displays the number of times the Switch will try to connect to the authentication server before determining the server is down.
Reauth period	This field displays how often a client must re-enter his or her username and password to stay connected to the port.
Quiet period	This field displays the period of the time the client must wait before the next re-authentication attempt.
Supp timeout	This field displays how long the Switch will wait before communicating with the server.
Server timeout	This field displays how long the Switch will wait before communicating with the client.

6.2 ACL

Introduction

L2 Access control list (**ACL**) is a list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

L2 ACL function allows user to configure a few rules to reject packets from the specific ingress ports or all ports. These rules will check the packets' source MAC address and destination MAC address. If packets match these rules, the system will do the actions "deny." "deny" means rejecting these packets.

The Action Resolution engine collects the information (action and metering results) from the hit entries: if more than one rule matches, the actions and meter/counters are taken from the policy associated with the matched rule with highest priority.

Default Settings

Maximum profile: 64.

Maximum profile name length: 16.

Notices

The ACL name should be the combination of the digit or the alphabet.

6.2.1 CLI configuration

Node	Command	Description
enable	show access-list	This command displays all the access control profiles.
configure	no access-list STRING	This command deletes an access control profile.
acl	show	This command displays the current access control profile.
acl	action (disable|drop|permit)	This command actives this profile. disable – disable the profile. drop – If packets match the profile, the packets will be dropped. permit – If packets match the profile, the packets will be forwarded.
acl	action dscp remarking <0-63>	This command actives this profile and specify that it is for DSCP remark. And configures the new DSCP value which will be override to all packets matched this profile.

acl	action 802.1p remarking <0-7>	This command actives this profile and specify that it is for 802.1p remark. And configures the new 802.1p value which will be override to all packets matched this profile.
acl	802.1p VALUE	This command configures the 802.1p value for the profile.
acl	dscp VALUE	This command configures the DSCP value for the profile.
acl	destination mac host MACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC and mask for the profile. The second MACADDR parameter is the mask for the profile.
acl	no destination mac	This command removes the destination MAC from the profile.
acl	ethertype STRING	This command configures the ether type for the profile. Where the STRING is a hex-decimal value. e.g.: 08AA.
acl	no ethertype	This command removes the limitation of the ether type from the profile.
acl	source mac host MACADDR	This command configures the source MAC and mask for the profile.
acl	source mac MACADDR MACADDR	This command configures the source AMC and mask for the profile.
acl	no source mac	This command removes the source MAC and mask from the profile.
acl	source IP host IPADDR	This command configures the source IP address for the profile.
acl	source IP IPADDR IPMASK	This command configures the source IP address and mask for the profile.

acl	no source IP	This command removes the source IP address from the profile.
acl	destination IP host IPADDR	This command configures a specific destination IP address for the profile.
acl	destination IP IPADDR IPMASK	This command configures the destination IP address and mask for the profile.
acl	no destination IP	This command removes the destination IP address from the profile.
acl	l4-source-port IPADDR	This command configures UDP/TCP source port for the profile.
acl	no l4-source-port IPADDR	This command removes the UDP/TCP source port from the profile.
acl	L4-destination-port PORT	This command configures the UDP/TCP destination port for the profile.
acl	no l4-destination-port	This command removes the UDP/TCP destination port from the profile.
acl	vlan VLANID	This command configures the VLAN for the profile.
acl	no vlan	This command removes the limitation of the VLAN from the profile.
acl	source interface PORT_ID	This command configures the source interface for the profile.
acl	no source interface PORT_ID	This command removes the source interface from the profile.

Where the MAC mask allows users to filter a range of MAC in the packets' source MAC or destination MAC.

For example:

```
source mac 00:01:02:03:04:05 ff:ff:ff:ff:00
```

The command will filter source MAC range from 00:01:02:03:00:00 to 00:01:02:03:ff:ff

Where the IPMASK mask allows users to filter a range of IP in the packets' source IP or destination IP.

For example:

```
source IP 172.20.1.1 255.255.0.0
```

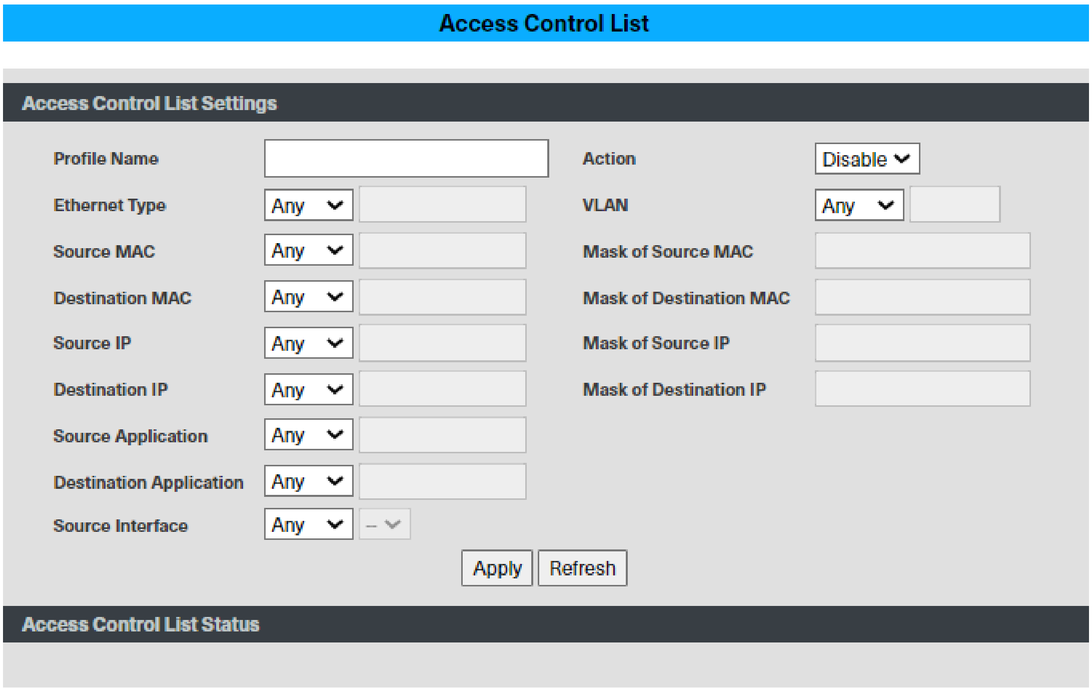
The command will filter source IP range from 172.20.0.0 to 172.20.255.255

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#access-list 111
L2SWITCH(config-acl)#vlan 2
L2SWITCH(config-acl)#source interface 1
L2SWITCH(config-acl)#show
Profile Name: 111
Activate: disabled
VLAN: 2
Source Interface: 1
Destination MAC Address: any
Source MAC Address: any
Ethernet Type: any
Source IP Address: any
Destination IP Address: any
Source Application: any
Destination Application: any
```

Note: Any: Do not care.

6.2.2 ACL Web Configuration



Access Control List

Access Control List Settings

Profile Name		Action	Disable
Ethernet Type	Any	VLAN	Any
Source MAC	Any	Mask of Source MAC	
Destination MAC	Any	Mask of Destination MAC	
Source IP	Any	Mask of Source IP	
Destination IP	Any	Mask of Destination IP	
Source Application	Any		
Destination Application	Any		
Source Interface	Any		

Access Control List Status

Parameter	Description
Profile Name	The access control profile name.
State	Selects Disables / Drop / Permits/ DSCP action for the profile.
Ethernet Type	Configures the Ethernet type of the packets that you want to filter.
VLAN	Configures the VLAN of the packets that you want to filter.
Source MAC	Configures the source MAC of the packets that you want to filter.
Mask of Source MAC	Configures the bitmap mask of the source MAC of the packets that you want to filter. If the Source MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured in Source MAC field.
Destination MAC	Configures the destination MAC of the packets that you want to filter.
Mask of Destination MAC	Configures the bitmap mask of the destination MAC of the packets that you want to filter. If the Destination MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured

	in Destination MAC field.
Source IP	Configures the source IP of the packets that you want to filter.
Mask of Source IP	Configures the bitmap mask of the source IP of the packets that you want to filter. If the Source IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Source IP field.
Destination IP	Configures the destination IP of the packets that you want to filter.
Mask of Destination IP	Configures the bitmap mask of the destination IP of the packets that you want to filter. If the Destination IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Destination IP field.
Source Application	Configures the source UDP/TCP ports of the packets that you want to filter.
Destination Application	Configures the destination UDP/TCP ports of the packets that you want to filter.
Source Interface(s)	Configures one or a rage of the source interfaces of the packets that you want to filter.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

6.3 Port Security

Introduction

The Switch will learn the MAC address of the device directly connected to a particular port and allow traffic through. We will ask the question: “How do we control who and how many can connect to a switch port?” This is where port security can assist us. The Switch allow us to control which devices can connect to a switch port or how many of them can connect to it (such as when a hub or another switch is connected to the port).

Let us say we have only one switch port left free, and we need to connect five hosts to it. What can we do? Connect a hub or switch to the free port! Connecting a switch or a hub to a port has implications. It means that the network will have more traffic. If a switch or a hub is connected by a user instead of an administrator, then there are chances that loops will be created. So, it is best that number of hosts allowed to connect is restricted at the switch level. This can be done using the “port-security limit” command. This command configures the maximum number of MAC addresses that can source traffic through a port.

Port security can set maximum number of MAC addresses allowed per interface. When the limit is exceeded, incoming packets with new MAC addresses are dropped. It can be use MAC table to check it. The static MAC addresses are included for the limit.

Note: If you configure a port of the Switch from disabled to enabled, all the MAC learned by this port will be clear.

Default Settings

The port security on the Switch is disabled.

The Maximum MAC per port is 5.

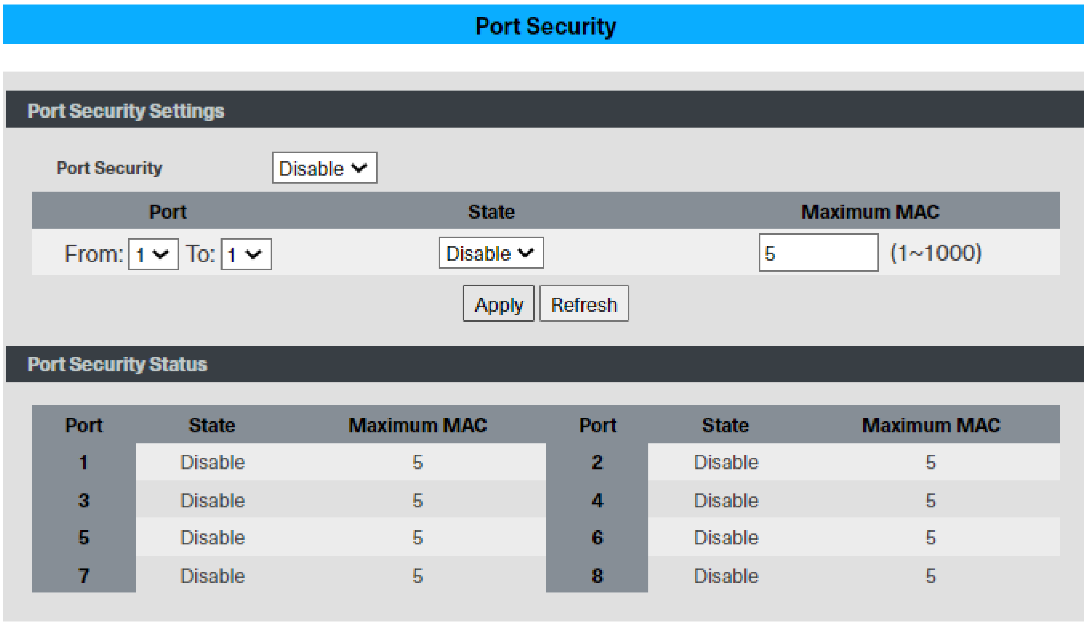
The port state of the port security is disabled.

6.3.1 CLI Configuration

Node	Command	Description
enable	show port-security	This command displays the current port security configurations.
configure	port-security (disable|enable)	This command enables / disables the global port security function.
interface	port-security (disable|enable)	This command enables / disables the port security function on the specific port.
interface	port-security limit VALUE	This command configures the maximum MAC entries on the specific port.
configure	interface range gigabitethernet1/0/PORTLISTS	This command enters the interface configure node.

if-range	port-security (disable|enable)	This command enables / disables the port security function for the specified ports
if-range	port-security limit VALUE	This command configures the maximum MAC entries for the specified ports.

6.3.2 Web Configuration



Port Security

Port Security Settings

Port Security: Disable

Port	State	Maximum MAC
From: 1 To: 1	Disable	5 (1~1000)

Port Security Status

Port	State	Maximum MAC	Port	State	Maximum MAC
1	Disable	5	2	Disable	5
3	Disable	5	4	Disable	5
5	Disable	5	6	Disable	5
7	Disable	5	8	Disable	5

Parameter	**Description**
Port Security Settings	
Port Security	Select **Enable/Disable** to permit Port Security on the Switch.
Port	Select a port number to configure.
State	Select **Enable/Disable** to permit Port Security on the port.
Maximum MAC	The maximum number of MAC addresses allowed per interface. The acceptable range is 1 to 1000.
Port Security Status	
Port	This field displays a port number.
State	This field displays if Port Security is **Enabled** or **Disabled**
Maximum MAC	This field displays the maximum number of MAC addresses

6.4 Server Control

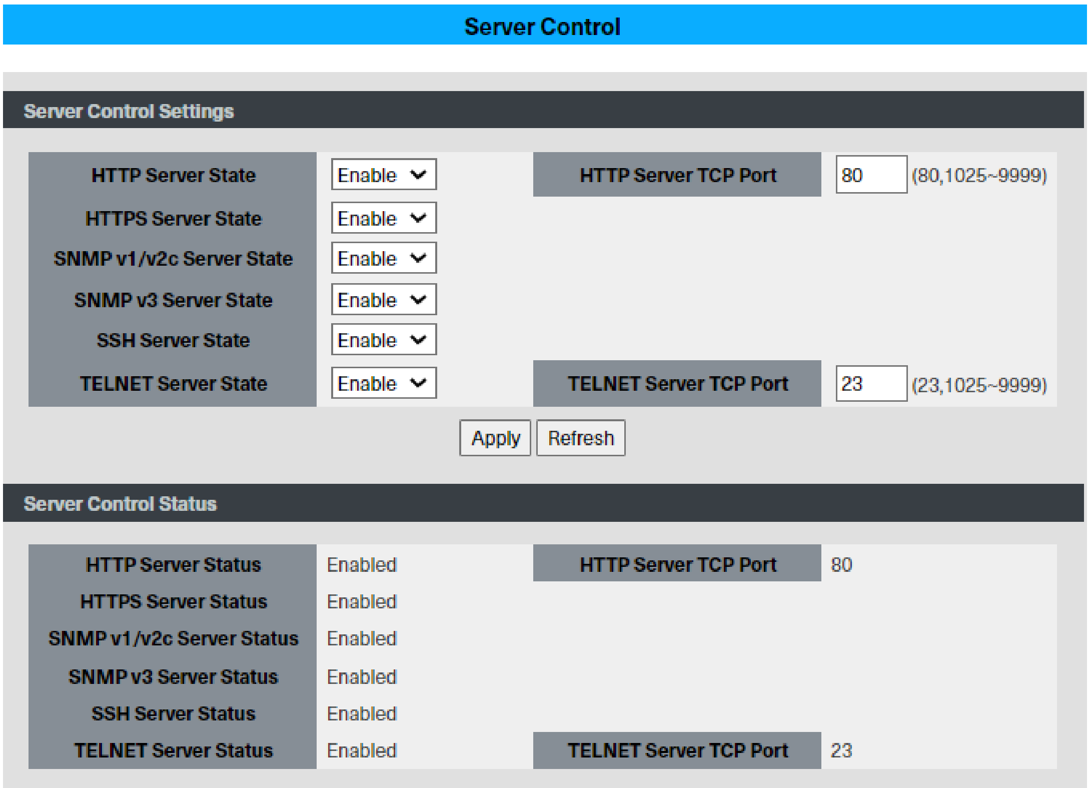
Introduction

The function allows users to enable or disable the HTTP, HTTPS, SNMPv1/v2c, SNMPv3, SSH, Telnet, service individually.

6.4.1 CLI Configuration

Node	Command	Description
enable	show server status	This command displays the current server status.
configure	ssh server	This command enables the ssh on the Switch.
configure	no ssh server	This command disables the ssh on the Switch.
configure	telnet server	This command enables the telnet on the Switch.
configure	no telnet server	This command disables the telnet on the Switch.
configure	SNMPv1/v2c	This command enables the SNMPv1/v2c on the Switch
configure	SNMPv1/v2c	This command disables the SNMPv1/v2c on the Switch.
configure	SNMPv3	This command enables the SNMPv3 on the Switch
configure	SNMPv3	This command disables the SNMPv3 on the Switch.
configure	web server	This command enables the web on the Switch.
configure	no web server	This command disables the web on the Switch.

6.4.2 Sever Settings Web Configuration



Server Control

Server Control Settings

HTTP Server State	Enable	HTTP Server TCP Port	80	(80,1025~9999)
HTTPS Server State	Enable			
SNMP v1/v2c Server State	Enable			
SNMP v3 Server State	Enable			
SSH Server State	Enable			
TELNET Server State	Enable	TELNET Server TCP Port	23	(23,1025~9999)

Server Control Status

HTTP Server Status	Enabled	HTTP Server TCP Port	80
HTTPS Server Status	Enabled		
SNMP v1/v2c Server Status	Enabled		
SNMP v3 Server Status	Enabled		
SSH Server Status	Enabled		
TELNET Server Status	Enabled	TELNET Server TCP Port	23

Parameter	Description
Server Settings	
HTTP Server State	Selects Enable or Disable to enable or disable the HTTP service.
HTTPS Server State	Selects Enable or Disable to enable or disable the HTTPS service.
SNMPv1/v2c Server State	Selects Enable or Disable to enable or disable the SNMPv1/v2c service.
SNMPv3 Server State	Selects Enable or Disable to enable or disable the SNMPv3 service.
SSH Server State	Selects Enable or Disable to enable or disable the SSH service.
Telnet Server State	Selects Enable or Disable to enable or disable the Telnet service.
Apply	Click Apply to configure the settings.
Refresh	Click this button to reset the fields to the last setting.

Server Status	
HTTP Server Status	Displays the current HTTP service status.
HTTPS Server Status	Displays the current HTTPS service status.
SNMPv1/v2c Server Status	Displays the current SNMPv1/v2c service status
SNMPv3 Server Status	Displays the current SNMPv3 service status
SSH Server Status	Displays the current SSH service status.
Telnet Server Status	Displays the current Telnet service status.

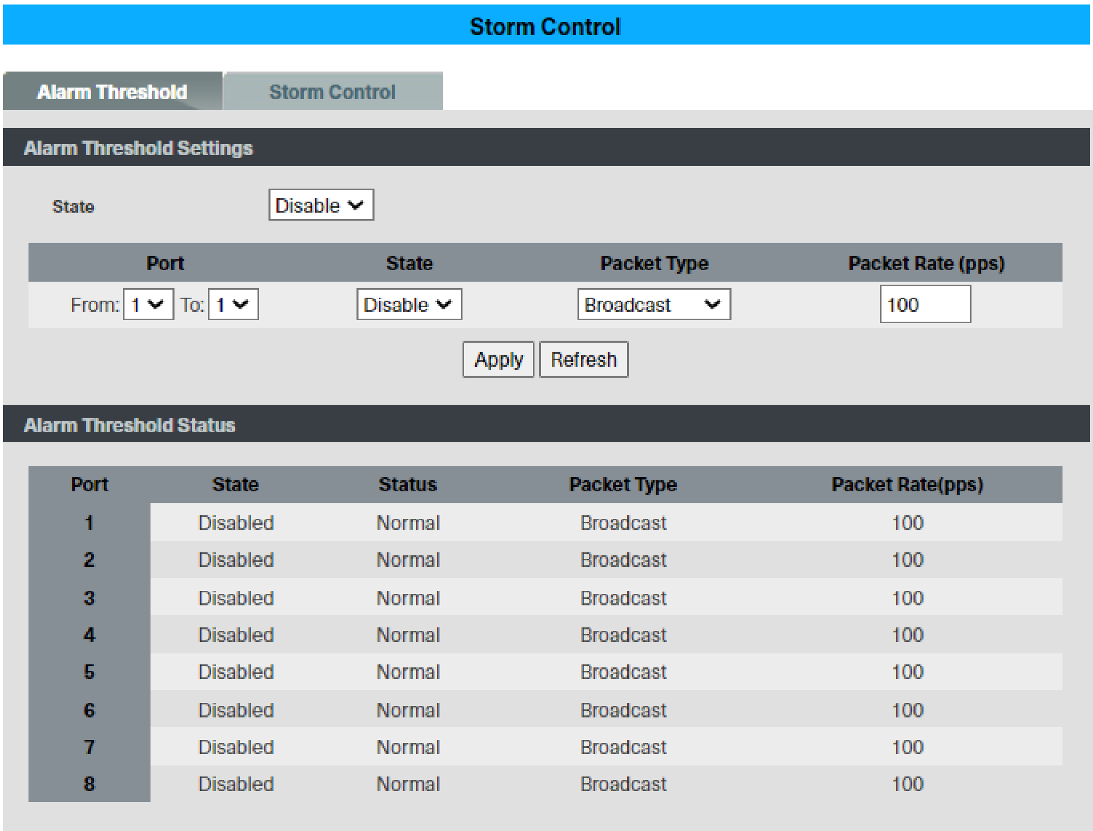
6.5 Storm control

6.5.1 Alarm Threshold

Introduction

When the selected packet rate is over the alarm threshold, the Switch will send syslog alarm to syslog server.

6.5.1.1 Alarm Threshold Web Configuration



State: Disable

Port	State	Packet Type	Packet Rate (pps)
From: 1 To: 1	Disable	Broadcast	100

Port	State	Status	Packet Type	Packet Rate(pps)
1	Disabled	Normal	Broadcast	100
2	Disabled	Normal	Broadcast	100
3	Disabled	Normal	Broadcast	100
4	Disabled	Normal	Broadcast	100
5	Disabled	Normal	Broadcast	100
6	Disabled	Normal	Broadcast	100
7	Disabled	Normal	Broadcast	100
8	Disabled	Normal	Broadcast	100

Parameter	Description
Alarm Threshold Settings	
State	Select option to enable / disable the alarm threshold feature on the Switch.
Port	Selects a port or a range of ports on which to configure the alarm threshold.
State	Selects **Enable** / **Disable** the alarm threshold for the port(s).
Packet Type	Selects packet type one of Broadcast / Multicast / Broadcast and Multicast.
Packet Rate	Select the alarm threshold packet rate in pps.
Alarm Threshold Status	
	The table display the current settings and port status.

6.5.2 Port Settings

Introduction

A broadcast storm means that your network is overwhelmed with constant broadcast or multicast traffic. Broadcast storms can eventually lead to a complete loss of network connectivity as the packets proliferate.

Storm Control protects the Switch bandwidth from flooding packets, including broadcast packets, multicast packets, and destination lookup failure (DLF).

Broadcast storm control limits the number of broadcasts, multicast and unknown unicast (also referred to as Destination Lookup Failure or DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and unknown unicast packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast, and unknown unicast packets in your network.

The default rate is 300pps for Broadcast and DLF. You can set to maximum rate of 5000pps for multicast, broadcast or DLF

6.5.2.1 CLI Configuration

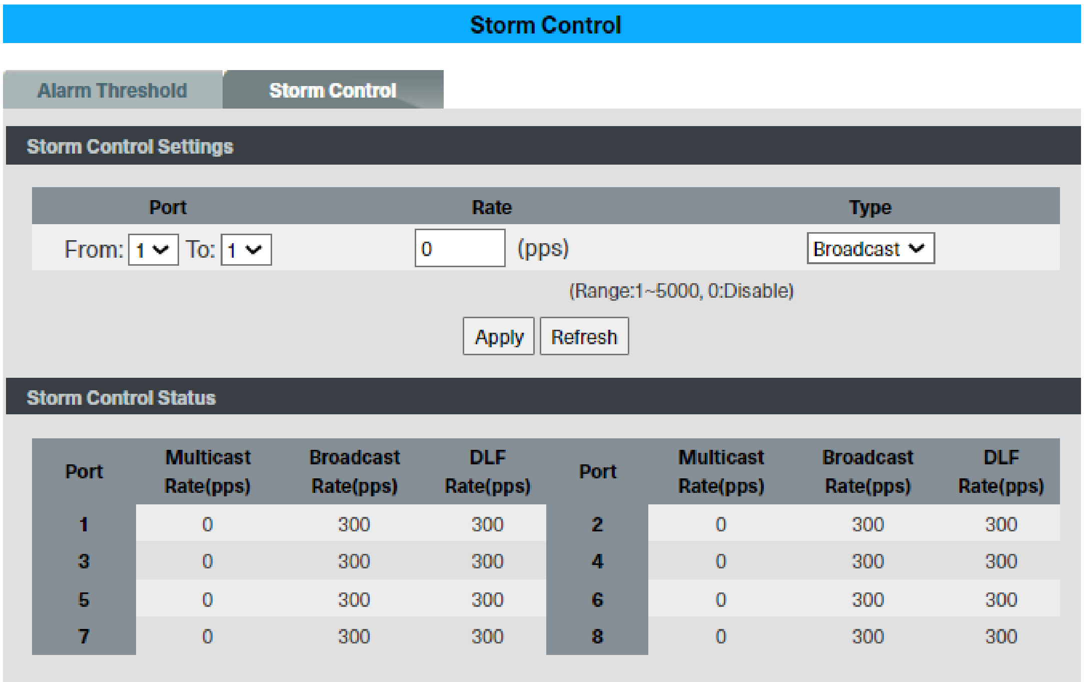
Node	Command	Description
enable	show storm-control	This command displays the current storm control configurations.
configure	storm-control rate RATE_LIMIT type (bcast | mcast | DLF) ports PORTLISTS	This command enables the bandwidth limit for broadcast or multicast or DLF packets and set the limitation.
configure	no storm-control type (bcast | mcast | DLF) ports PORTLISTS	This command disables the bandwidth limit for broadcast or multicast or DLF packets.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#storm-control rate 1 type broadcast ports 1-6
L2SWITCH(config)#storm-control rate 1 type multicast ports 1-6
```

```
L2SWITCH(config)#storm-control rate 1 type DLF ports 1-6
```

6.5.2.2 Storm Control Web configuration



Port	Rate	Type
From: 1 To: 1	0 (pps)	Broadcast

(Range:1~5000, 0:Disable)

Port	Multicast Rate(pps)	Broadcast Rate(pps)	DLF Rate(pps)	Port	Multicast Rate(pps)	Broadcast Rate(pps)	DLF Rate(pps)
1	0	300	300	2	0	300	300
3	0	300	300	4	0	300	300
5	0	300	300	6	0	300	300
7	0	300	300	8	0	300	300

Parameter	**Description**
Storm Control Settings	
Port	Select individual port number or range for which you want to configure storm control settings.
Rate	Configure the packet rate in pps to allow on interfaces. Disable for 0 and ranges 1 ~ 5000. .
Type	Click the check box to select Multicast / Broadcast / DLF storm control.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Storm Control Status	
Port	This field displays a port number.
Multicast Rate(pps)	This field displays the multicast storm control state along with configured rate of pps on the port.
Broadcast Rate(pps)	This field displays the broadcast storm control state along with configured rate of pps on the port.

DLF Rate(pps)	This field displays the DLF storm control state along with configured rate of pps on the port.

6.6 VLAN

6.6.1 Port Isolation

The port isolation is a port-based virtual LAN feature. It partitions the switching ports into virtual private domains designated on a per port basis. Data switching outside of the port's private domain is not allowed. It will ignore the packets' tag VLAN information.

This feature is a per port setting to configure the egress port(s) for the specific port to forward its received packets. If the CPU port (port 0) is not an egress port for a specific port, the host connected to the specific port cannot manage the Switch.

If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. CPU refers to the Switch management port. By default, it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port, then the Switch cannot be managed from that port.

6.6.1.1 CLI Configuration

Node	Command	Description
enable	show port-isolation	This command displays the current port isolation configurations. "V" indicates the port's packets can be sent to that port. "-" indicates the port's packets cannot be sent to that port.
interface	port-isolation ports PORTLISTS	This command configures a port or a range of ports to egress traffic from the specific port.
interface	no port-isolation	This command configures all ports to egress traffic from the specific port.

Example: If you want to allow port-1 and port-3 to talk to each other, you must configure as below:

```
L2SWITCH(config)#interface 1/0/1
```

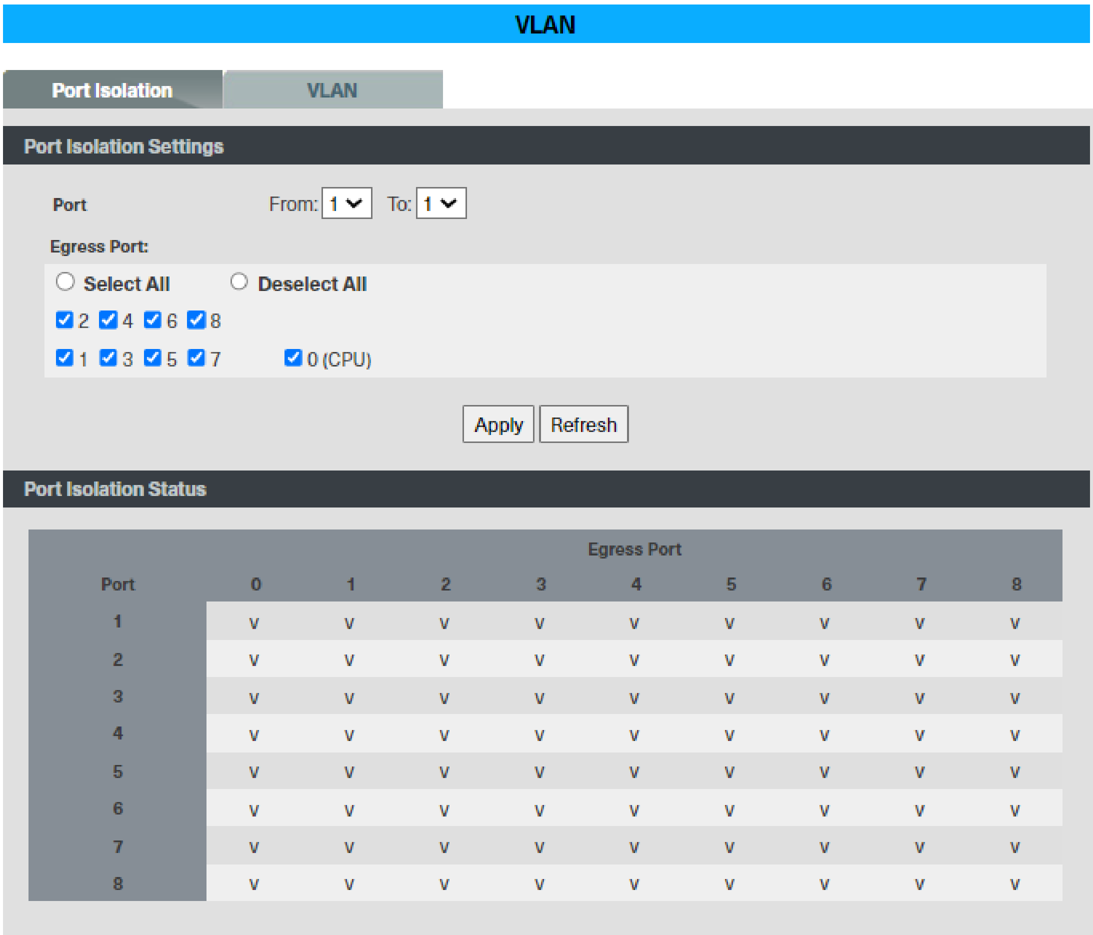
```
L2SWITCH(config-if)#port-isolation ports 3
L2SWITCH(config-if)#exit
```

Allow the port-1 to send its ingress packets to port-3.

```
L2SWITCH(config)#interface 1/0/3
L2SWITCH(config-if)#port-isolation ports 1
L2SWITCH(config-if)#exit
```

Allow the port-3 to send its ingress packets to port-1

6.6.1.2 Port Isolation Web Configuration



Port Isolation Settings

Port From: 1 To: 1

Egress Port:

○ Select All ○ Deselect All

☑ 2 ☑ 4 ☑ 6 ☑ 8

☑ 1 ☑ 3 ☑ 5 ☑ 7 ☑ 0 (CPU)

Port Isolation Status

	Egress Port								
Port	0	1	2	3	4	5	6	7	8
1	v	v	v	v	v	v	v	v	v
2	v	v	v	v	v	v	v	v	v
3	v	v	v	v	v	v	v	v	v
4	v	v	v	v	v	v	v	v	v
5	v	v	v	v	v	v	v	v	v
6	v	v	v	v	v	v	v	v	v
7	v	v	v	v	v	v	v	v	v
8	v	v	v	v	v	v	v	v	v

Parameter	Description
Port	Select a port number to configure its port isolation settings. Select **All Ports** to configure the port isolation settings for all ports on the Switch.

Egress Port	An egress port is an outgoing port, that is, a port through which a data packet leaves. Selecting a port as an outgoing port means it will communicate with the port currently being configured.
Select All/ Deselect All	Click **Select All** to mark all ports as egress ports and permit traffic. Click **Deselect All** to unmark all ports and isolate them. Deselecting all ports means the port being configured cannot communicate with any other port.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last setting.
Port Isolation Status	"V" indicates the port's packets can be sent to that port. "-" indicates the port's packets cannot be sent to that port.

6.6.2 VLAN Settings

802.1Q VLAN

Introduction

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. In Lite Managed switches, user can configure maximum of 5 VLAN's on each interface in the format 1,3,7,10,25. Network reconfiguration can be done through software instead of physically relocating devices.

VID- VLAN ID is the identification of the VLAN, which is basically used by the standard 802.1Q. It has 12 bits and allow the identification of 4096 (2^12) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant, and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 bytes	3 bits	1 bit	12 bits

- Forwarding Tagged and Untagged Frames

Each port on the Switch can pass tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strIPs off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1QVLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

- 802.1QPort base VLAN

With port based VLAN membership, the port is assigned to a specific VLAN independent of the user or system attached to the port. This means all users attached to the port should be members of the same VLAN. The network administrator typically performs the VLAN assignment. The port configuration is static and cannot be automatically changed to another VLAN without manual reconfiguration.

As with other VLAN approaches, the packets forwarded using this method do not leak into other VLAN domains on the network. After a port has been assigned to a VLAN, the port cannot send to or receive from devices in another VLAN without the intervention of a Layer 3 device.

The device that is attached to the port likely has no understanding that a VLAN exists. The device simply knows that it is a member of a subnet, and that the device should be able to talk to all other members of the subnet by simply sending information to the cable segment. The switch is responsible for identifying that the information came from a specific VLAN and for ensuring that the information gets to all other members of the VLAN. The switch is further responsible for ensuring that ports in a different VLAN do not receive the information.

This approach is quite simple, fast, and easy to manage in that there are no complex lookup tables required for VLAN segmentation. If port-to-VLAN association is done with an application-specific integrated circuit (ASIC), the performance is exceptionally good. An ASIC allows the port-to-VLAN mapping to be done at the hardware level.

The port isolation is a port-based virtual LAN feature. It partitions the switching ports into virtual private domains designated on a per port basis. Data switching outside of the port’s private domain is not allowed. It will ignore the packets’ tag VLAN information.

This feature is a per port setting to configure the egress port(s) for the specific port to forward its received packets. If the CPU port (port 0) is not an egress port for a specific port, the host connected to the specific port cannot manage the Switch.

If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the Switch management port. By default, it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port, then the Switch cannot be managed from that port.

Notice:

Maximum allowable VLAN's to configure on the device are 5.

Access port:

Allows one VLAN only which is untagged port and PVID (particular VLAN id) should be configured on interface by default VLAN 1 is PVID for all the interfaces. The port should be connected to PC device.

Trunk port:

Allows the user to configure up to 5 VLAN's maximum on the interface and always tagged where its PVID is 1 (System configure them automatically). The port should be connected to another switch.

Default Settings

All ports join in the VLAN 1.

6.6.3 CLI Configuration

Node	Command	Description
enable	show vlan VLANID	This command displays the VLAN configurations.
configure	vlan <1~4094>	This command enables a VLAN and enters the VLAN node.
configure	no vlan <1~4094>	This command deletes a VLAN.
vlan	show	This command displays the current VLAN configurations.
vlan	name STRING	This command assigns a name for the specific VLAN. The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_). The maximum length of the name is 16 characters.
vlan	no name	This command configures the vlan name to default. Note: The default vlan name is "VLAN"+

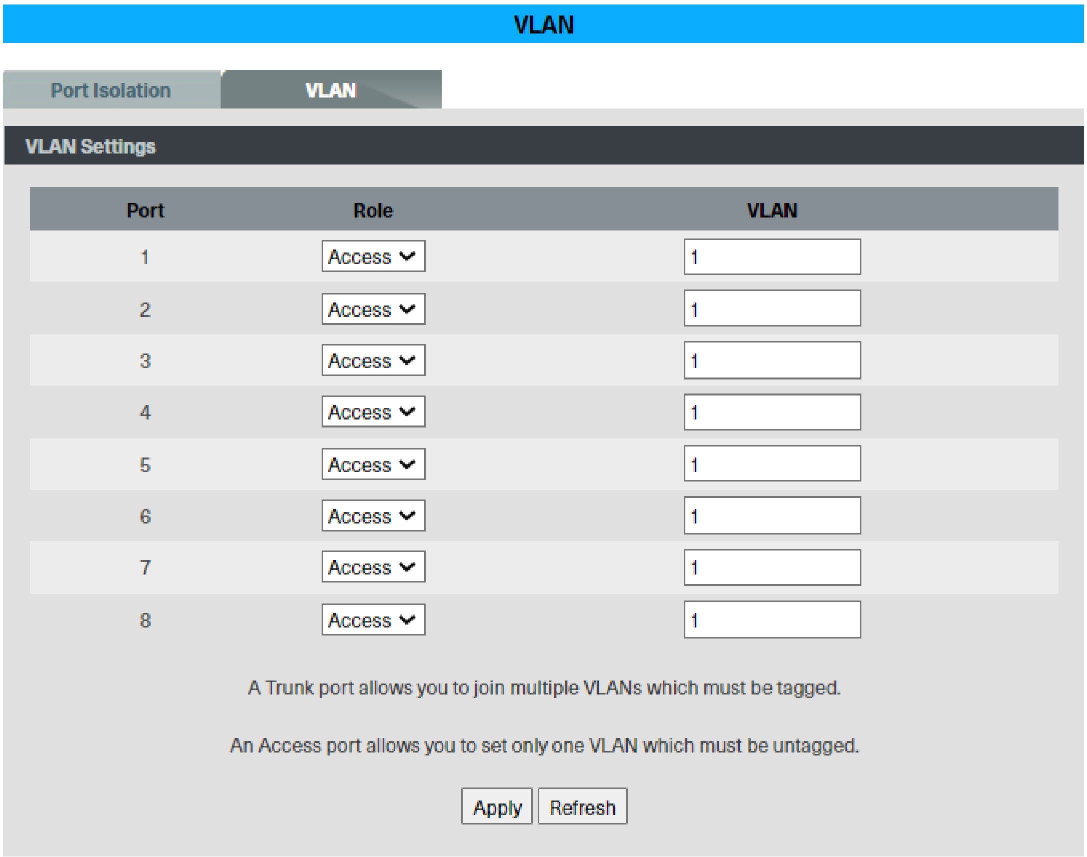
		VLAN_ID, VLAN1, VLAN2, ...
vlan	add PORTLISTS	This command adds a port or a range of ports to the vlan.
vlan	fixed PORTLISTS	This command assigns ports for permanent member of the vlan.
vlan	no fixed PORTLISTS	This command removes all fixed member from the vlan.
vlan	tagged PORTLISTS	This command assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the vlan.
vlan	no tagged PORTLISTS	This command removes all tagged member from the vlan.
vlan	untagged PORTLISTS	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the vlan.
vlan	no untagged PORTLISTS	This command removes all untagged member from the vlan.
interface	acceptable frame type (all|tagged|untagged)	This command configures the acceptable frame type. all - acceptable all frame types. tagged - acceptable tagged frame only. untagged – acceptable untagged frame only.
interface	PVID VLANID	This command configures a VLAN ID for the port default VLAN ID.
interface	no PVID	This command configures 1 for the port default VLAN ID.
config	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	PVID VLANID	This command configures a VLAN ID for the port default VLAN ID.
if-range	no PVID	This command configures 1 for the port

		default VLAN ID.
configure	vlan range STRINGS	This command configures a range of VLAN's and Maximum allowed VLAN's are 5.
configure	no vlan range STRINGS	This command removes a range of VLAN's and Maximum removable VLAN's are 5.
vlan-range	1-4	This command will allow user to create VLAN range maximum allowed VLAN's are 5
vlan-range	add PORTLISTS	This command adds a port or a range of ports to the VLANs.
vlan-range	fixed PORTLISTS	This command assigns ports for permanent member of the VLAN group.
vlan-range	no fixed PORTLISTS	This command removes all fixed member from the VLANs.
vlan-range	tagged PORTLISTS	This command assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the VLANs.
vlan-range	no tagged PORTLISTS	This command removes all tagged member from the VLANs.
vlan-range	untagged PORTLISTS	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the VLANs.
vlan-range	no untagged PORTLISTS	This command removes all untagged member from the VLANs.

Example:

- L2SWITCH#configure terminal
- L2SWITCH(config)#vlan 2
- L2SWITCH(config-vlan)#fixed 1-5
- L2SWITCH(config-vlan)#untagged 1-3
- L2SWITCH(config)#vlan range 10-14
- L2SWITCH(config-vlan-range)# fixed 1-5
- L2SWITCH(config-vlan-range)# tagged 5

6.6.4 Web Configuration VLAN Settings



Port	Role	VLAN
1	Access	1
2	Access	1
3	Access	1
4	Access	1
5	Access	1
6	Access	1
7	Access	1
8	Access	1

A Trunk port allows you to join multiple VLANs which must be tagged.

An Access port allows you to set only one VLAN which must be untagged.

Parameter	Description
Port	Select a port number to configure from the drop-down box. Select **All** to configure all ports at the same time.
Role	Select role on interface as access or trunk.
VLAN	User can configure maximum of 5 VLAN's on each interface in the format 1,3,7,10,25
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.

7 Diagnosis

7.1 Alarm Information

Introduction

The feature displays if there are any abnormal situation need process immediately.

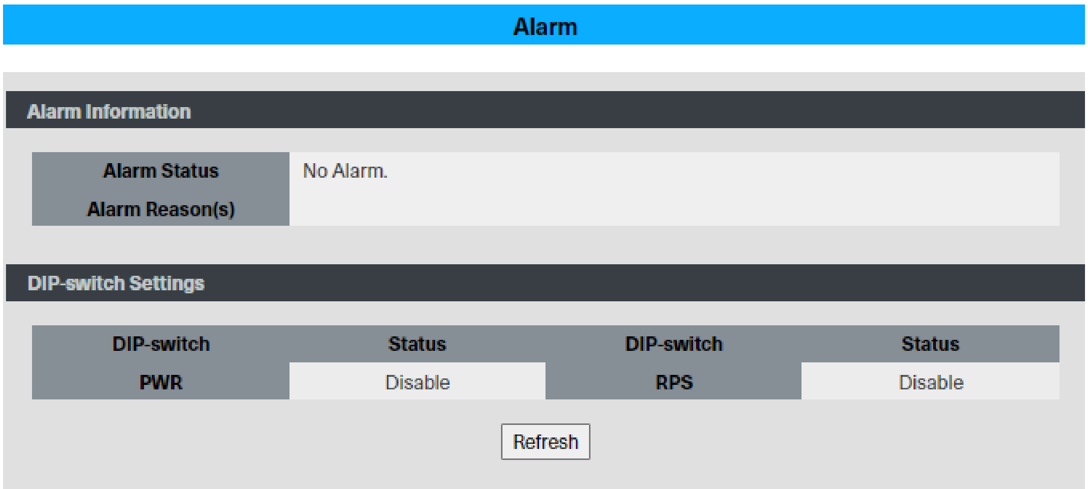
Alarm LED: On - When any alarm events happen.

The web pages show you the detail alarm reason.

7.1.1.1 CLI Command

Node	Command	Description
enable	show alarm-info	This command displays alarm information.

7.1.1.2 Alarm Information Web



Alarm

Alarm Information

Alarm Status Alarm Reason(s)	No Alarm.

DIP-switch Settings

DIP-switch	Status	DIP-switch	Status
PWR	Disable	RPS	Disable

Parameter	Description
Alarm Information	
Alarm Status	This field indicates if there are any alarm events.
Alarm Reason(s)	This field displays all the detail alarm events.
Function DIP Switch Settings:	
Storm	The field display the current Storm Control DIP settings. Disable – Storm Control controlled by user configurations. Enable – Broadcast and DLF Storm control is enabled.

	And the packet rate is 300 pps.
QoS	The field display the current QoS DIP settings. Disable – Port priority controlled by user configurations. Enable – port 1 & 2 have higher priority.
P9 100Fx	The field display the current port 9 100M-Full DIP settings. Disable – port 9 speed controlled by user configurations. Enable – port 9 speed is 100M-Full.
P10 100Fx	The field displays the current port 10 100M-Full settings. Disable – port 10 speed controlled by user configurations. Enable – port 10 speed is 100M-Full.

7.2 Port Mirror

Introduction

The Port-Based Mirroring is used on a network switch to send a copy of network packets sent/received on one switch ports to a network monitoring connection on another switch port (Destination Port). This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system.

Port Mirroring, together with a network traffic analyzer, helps to monitor network traffic.

Default Settings

Mirror Configurations:

State	: Disable
Monitor port	: 1
Ingress port(s)	: None
Egress port(s)	: None

7.2.1 CLI Configuration

Node	Command	Description
enable	show mirror	This command displays the current port mirroring configurations.
configure	mirror (disable|enable)	This command disables / enables the port mirroring on the switch.
configure	mirror destination port PORT_ID	This command specifies the **monitor port** for the port mirroring.
configure	mirror source ports PORT_LIST mode *(both|ingress|egress)*	This command **adds** a port or a range of ports as the source ports of the port mirroring.
configure	no mirror source ports PORT_LIST	This command **removes** a port or a range of ports from the source ports of the port mirroring.

The procedures to configure the port mirror.

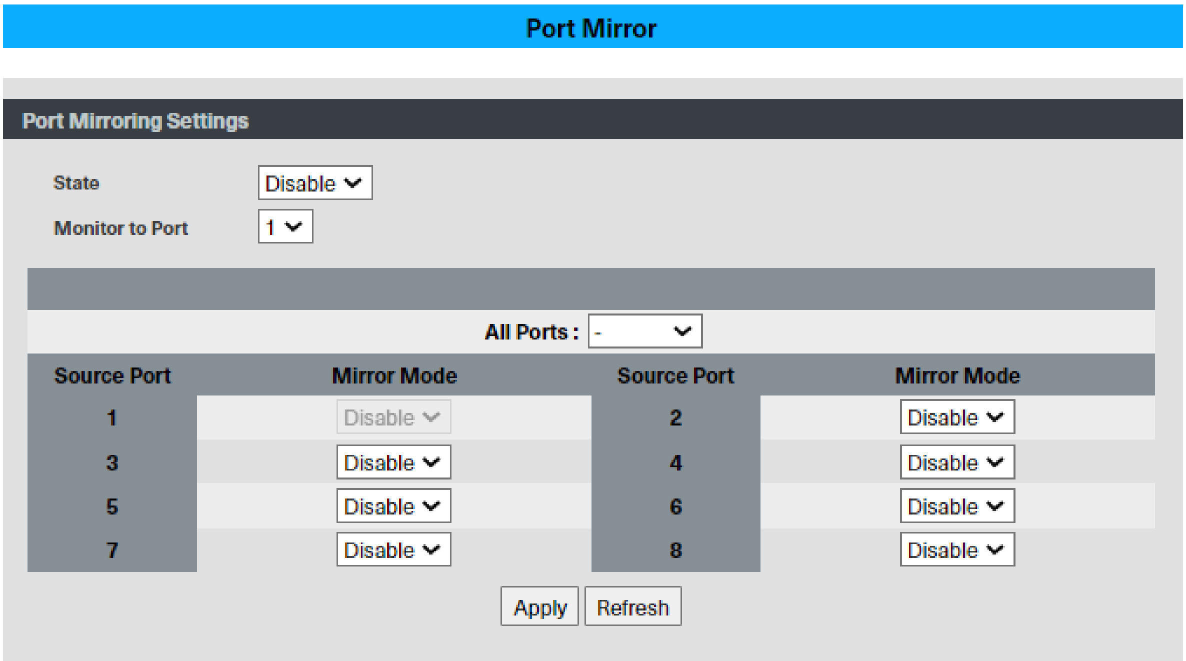
- To enter the configure node.
```
L2SWITCH#configure terminal
L2SWITCH(config)#
```

- To enable the global mirror function.
```
L2SWITCH(config)#mirror enable
```

- To configure the monitor port to port 2.
```
L2SWITCH(config)#mirror destination port 2
```

- To configure the source ports which you want to check.
```
L2SWITCH(config)#mirror source ports 3-6 mode both
```

7.2.2 Port Mirror Web Configuration



Port Mirror

Port Mirroring Settings

State: Disable

Monitor to Port: 1

All Ports : -

Source Port	Mirror Mode	Source Port	Mirror Mode
1	Disable	2	Disable
3	Disable	4	Disable
5	Disable	6	Disable
7	Disable	8	Disable

Parameter	Description
Port Mirror Settings	
State	Select option to enable / disable the port mirroring feature on the Switch globally.
Monitor to Port	Select the port which connects to a network traffic analyzer.
All Ports	Settings in this field apply to all ports. Use this field only if you want to make some settings the same for all ports. Use this field first to set the common settings and then adjust on a port-by-port basis.
Source Port	Selects a port to monitor packets received and transmit or both.
Monitor Mode	Select a port to monitor as destination for the source port. Select Ingress, Egress or Both to only copy the ingress (incoming), egress (outgoing) or both (incoming and outgoing) traffic from the specified source ports to the monitor port. Select Disable to not copy any traffic from

	the specified source ports to the monitor port.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

7.3 Port Statistics

Introduction

This feature helps users to monitor the ports' statistics, to display the link up ports' traffic utilization only.

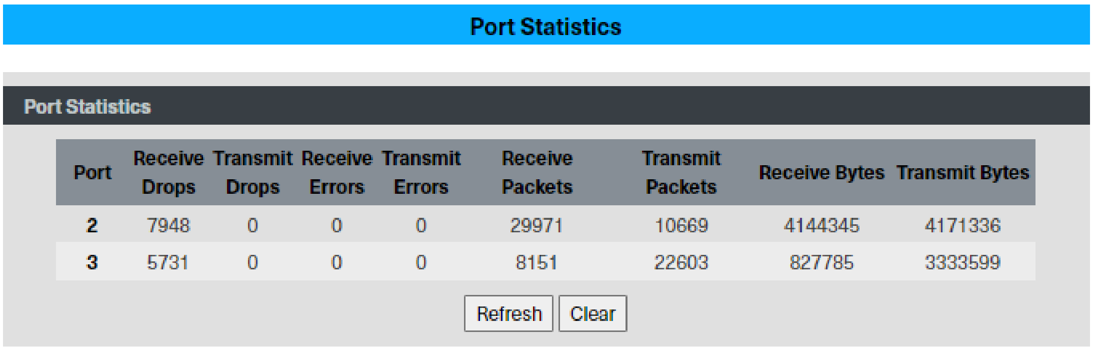
7.3.1 CLI Configuration

Node	Command	Description
enable	show port-statistics	This command displays the link up ports' statistics.

Example :

```
L2SWITCH#show port-statistics
                Packets              Bytes               Errors              Drops
Port        Rx          Tx          Rx          Tx          Rx          Tx          Rx          Tx
----   --------- ---------   --------- ---------   --------- ---------   --------- ---------
 7      1154       2            108519     1188        0          0           0          0
```

7.3.1.1 Port Statistics Web Information



Port Statistics

Port Statistics

Port	Receive Drops	Transmit Drops	Receive Errors	Transmit Errors	Receive Packets	Transmit Packets	Receive Bytes	Transmit Bytes
2	7948	0	0	0	29971	10669	4144345	4171336
3	5731	0	0	0	8151	22603	827785	3333599

Parameter	Description
Port	Select a port or a range of ports to display their statistics.
Rx Packets	The field displays the received packet count.
Tx Packets	The field displays the transmitted packet count.
Rx Bytes	The field displays the received byte count.
Tx Bytes	The field displays the transmitted byte count.
Rx Errors	The field displays the received error count.
Tx Errors	The field displays the transmitted error count.
Rx Drops	The field displays the received drop count.
Tx Drops	The field displays the transmitted drop count.
Refresh	Click this button to refresh the screen quickly.

7.4 Port Utilization

Introduction

This feature helps users to monitor the ports' traffic utilization, to display the link up ports' traffic utilization only.

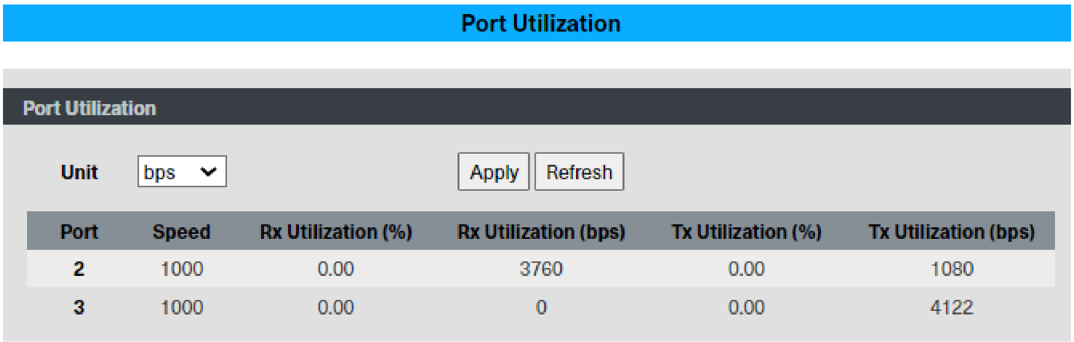
7.4.1 CLI Configuration

Node	Command	Description
enable	show port-utilization	This command displays the link up ports' traffic utilization.

Example :

```
L2SWITCH#show port-utilization
Port   Speed   Utilization(%)
----   -----   --------------
  9     100        0.001
```

7.4.2 Web Port Utilization



Port Utilization

Port Utilization

Port	Speed	Rx Utilization (%)	Rx Utilization (bps)	Tx Utilization (%)	Tx Utilization (bps)
2	1000	0.00	3760	0.00	1080
3	1000	0.00	0	0.00	4122

Parameter	Description
Port Utilization	
Port	The field displays the port ID.
Speed	The field displays the port’s speed.
Rx Utilization (%)	The field display Rx utilization in percentage.
Rx Utilization (bps)	The field display Rx utilization in bps.
Tx Utilization (%)	The field display Tx utilization in percentage.
Tx Utilization (bps)	The field display Tx utilization in bps.

7.5 Syslog

Introduction

The syslog function records some of system information for debugging purpose. Each log message recorded with one of these levels, **Alert / Critical / Error / Warning / Notice / Information.** The syslog function can be enabled or disabled. The default setting is disabled. The log message is recorded in the Switch file system. If the syslog server's IP address has been configured, the Switch will send a copy to the syslog server.

The log message file is limited in 2000 entries. If the file is full, the oldest one will be replaced.

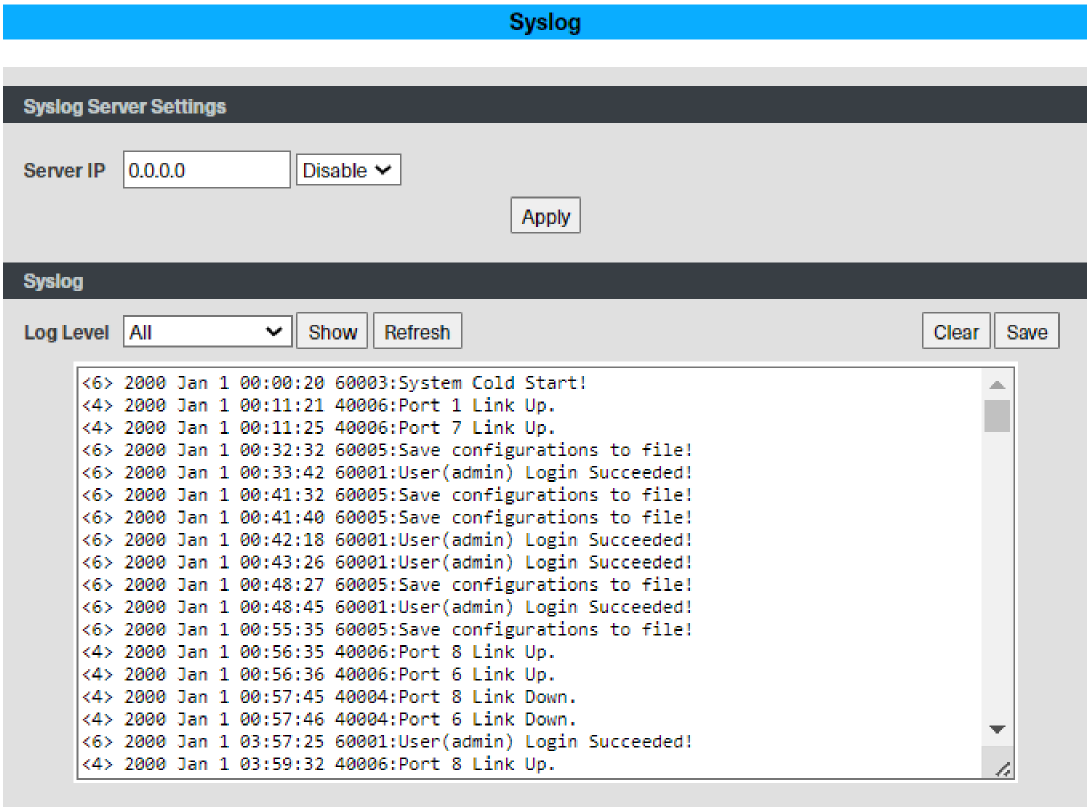
7.5.1 CLI Configuration

Node	Command	Description
enable	show syslog	The command displays all of log message recorded in the Switch.
enable	show syslog level LEVEL	The command displays the log message with the LEVEL recorded in the Switch.
enable	show syslog server	The command displays the syslog server configurations.
configure	syslog-server (disable|enable)	The command disables / enables the syslog function.
configure	syslog-server IP IPADDR	The command configures the syslog server's IP address.

Example:

- L2SWITCH#configure terminal
- L2SWITCH(config)#syslog-server IP 192.168.200.106
- L2SWITCH(config)#syslog-server enable

7.5.2 Syslog Server Setting Web Configuration



Server IP 0.0.0.0 Disable

Log Level All

```
<6> 2000 Jan 1 00:00:20 60003:System Cold Start!
<4> 2000 Jan 1 00:11:21 40006:Port 1 Link Up.
<4> 2000 Jan 1 00:11:25 40006:Port 7 Link Up.
<6> 2000 Jan 1 00:32:32 60005:Save configurations to file!
<6> 2000 Jan 1 00:33:42 60001:User(admin) Login Succeeded!
<6> 2000 Jan 1 00:41:32 60005:Save configurations to file!
<6> 2000 Jan 1 00:41:40 60005:Save configurations to file!
<6> 2000 Jan 1 00:42:18 60001:User(admin) Login Succeeded!
<6> 2000 Jan 1 00:43:26 60001:User(admin) Login Succeeded!
<6> 2000 Jan 1 00:48:27 60005:Save configurations to file!
<6> 2000 Jan 1 00:48:45 60001:User(admin) Login Succeeded!
<6> 2000 Jan 1 00:55:35 60005:Save configurations to file!
<4> 2000 Jan 1 00:56:35 40006:Port 8 Link Up.
<4> 2000 Jan 1 00:56:36 40006:Port 6 Link Up.
<4> 2000 Jan 1 00:57:45 40004:Port 8 Link Down.
<4> 2000 Jan 1 00:57:46 40004:Port 6 Link Down.
<6> 2000 Jan 1 03:57:25 60001:User(admin) Login Succeeded!
<4> 2000 Jan 1 03:59:32 40006:Port 8 Link Up.
```

Parameter	**Description**
Server IP	Enter the Syslog server IP address. Select **Enable** to activate switch sent log message to Syslog server when any new log message occurred.
Apply	Click **Apply** to add/modify the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Log Level	Select **Alert/Critical/Error/Warning/Notice/Information** to choose which log message to want to see.
Clear	Click Clear to clear all of log message.
Save	Click Save to save all of log message into NV-RAM.

7.6 Utilization Threshold

Introduction

This feature alerts the user when the packet rate in the particular port is above the required rate.

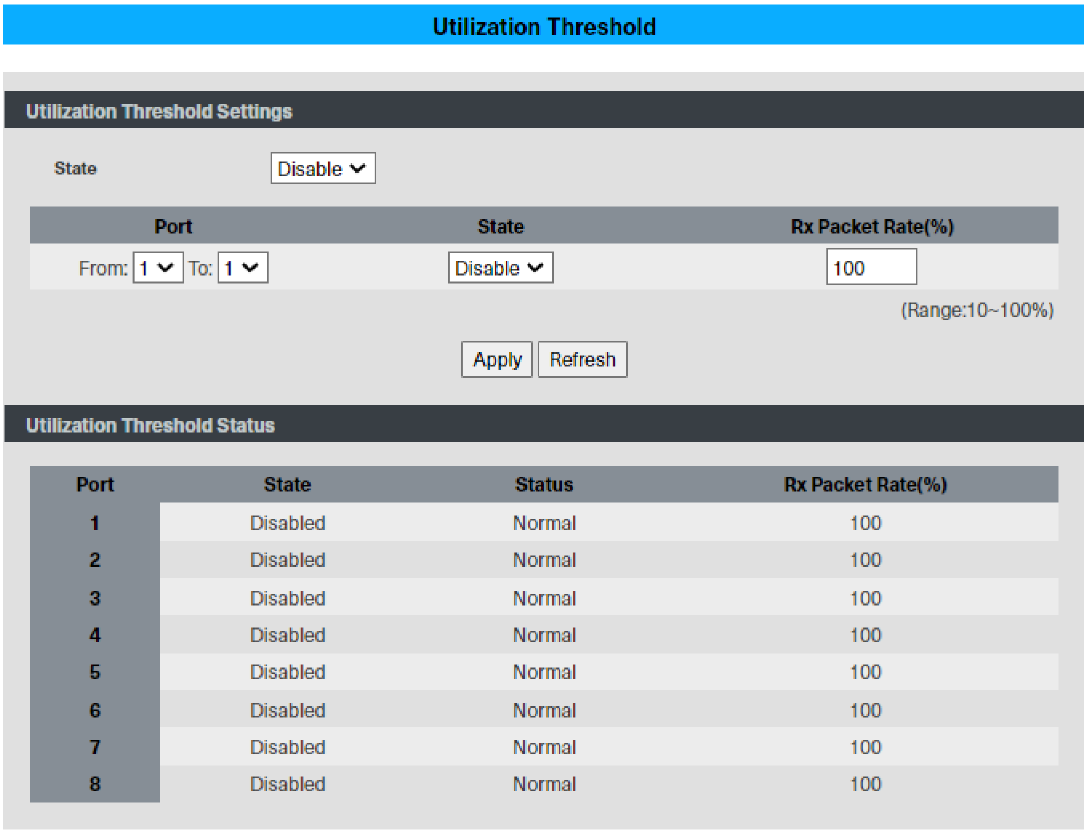
7.6.1 CLI Configuration

Node	Command	Description
configure	port-utilization threshold (disable|enable)	The command disables / enables the port utilization threshold function globally.
configure	interface IFNAME Ex: interface 1/0/4	This command enters the interface configure node.
interface	port-utilization threshold rate (value)	This command configures the port-utilization threshold value
interface	port-utilization threshold state (disable|enable)	The command disables / enables the port utilization threshold function on interface.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#port-utilization threshold enable
L2SWITCH(config)#interface 1/0/4
L2SWITCH(config-if)#port-utilization threshold rate 40
L2SWITCH(config-if)#port-utilization threshold state enables
```

7.6.2 Utilization Threshold Web Configuration



Utilization Threshold

Utilization Threshold Settings

State: Disable

Port	State	Rx Packet Rate(%)
From: 1 To: 1	Disable	100

(Range:10~100%)

Utilization Threshold Status

Port	State	Status	Rx Packet Rate(%)
1	Disabled	Normal	100
2	Disabled	Normal	100
3	Disabled	Normal	100
4	Disabled	Normal	100
5	Disabled	Normal	100
6	Disabled	Normal	100
7	Disabled	Normal	100
8	Disabled	Normal	100

Parameter	Description
Alarm Threshold Settings	
State	Select option to enable / disable the alarm threshold feature on the Switch.
Port	Selects a port or a range of ports on which to configure the alarm threshold.
State	Selects **Enable/Disable** the alarm threshold for the port(s).
Packet Rate	Configures the threshold rate. When the port packet rate over the threshold, the Switch will send trap and syslog.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Alarm Threshold Status	
Port	This field displays a port number.
State	This field displays the current alarm threshold state for the port.
Status	This field displays if alarm threshold has happened on the port.

Packet Rate	This field displays the current threshold.

8 Management

8.1 SNMPv1/v2c

Simple Network Management Protocol

Introduction

Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

8.1.1 SNMP configuration

Allows user to enable and disable SNMP protocol globally, by default SNMP state will be disabled, User can change the system name with respect to their requirement also can add system location and contact location.

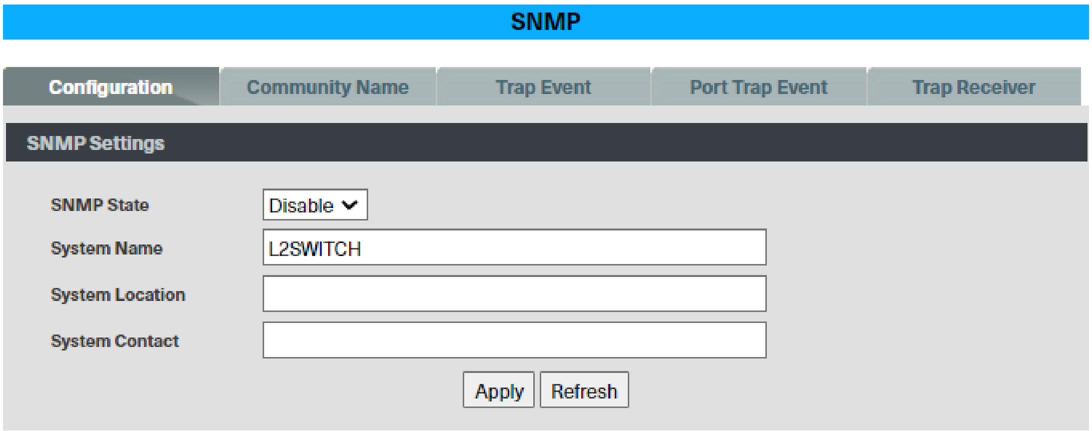
8.1.1.1 CLI Configuration

Node	Command	Description
enable	show SNMP	This command displays the SNMP configurations.
configure	SNMP (disable|enable)	This command disables/enables the SNMP on the switch.
configure	SNMP system-name STRING	This command configures a name for the system. (The System Name is same as the host name)
configure	SNMP system-location STRING	This command configures the location information for the system.
configure	SNMP system-contact STRING	This command configures contact information for the system.

Example:

- L2SWITCH#configure terminal
- L2SWITCH(config)#SNMP enable
- L2SWITCH(config)#SNMP system-contact IT engineer
- L2SWITCH(config)#SNMP system-location Branch-Office

8.1.1.2 Web SNMP Configuration



SNMP Settings

SNMP State: Disable

System Name: L2SWITCH

System Location:

System Contact:

Parameter	Description
SNMP Settings	
SNMP State	Select option to enable / disable the SNMP on the Switch.
System Name	User can configure system name
System Location	User can configure the switch deployed location for reference
System Contact	User can configure System Contact person information like name or number

8.1.2 SNMP Community Name

SNMP community act like passwords and are used to define the security parameters of SNMP clients in an SNMP v1 and SNMP v2c environments. The default SNMP community is “public” for both SNMP v1 and SNMP v2c…

Network ID of Trusted Host:

The IP address is a combination of the Network ID and the Host ID.

Network ID = (Host IP & Mask).

User need only input the network ID and leave the host ID to 0. If user has input the host ID, such as 192.168.1.102, the system will reset the host ID, such as 192.168.1.0

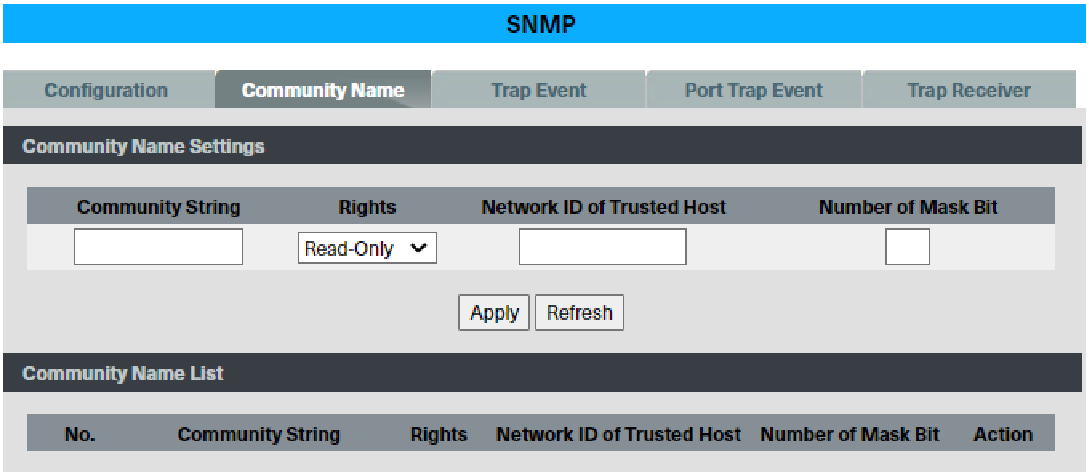
8.1.2.1 CLI Configuration

Node	Command	Description
configure	SNMP community STRING (ro|rw) trusted host IPADDR/Subnet Mask	This command configures the SNMP community name, Permission(ro/rw), Trusted host IP/Subnet mask.

Example:

- L2SWITCH#configure terminal
- L2SWITCH(config)#SNMP community public rw trusted-host 192.168.200.106/24

8.1.2.2 Community Name Web Configuration



Community Name Settings

Community String	Rights	Network ID of Trusted Host	Number of Mask Bit
	Read-Only		

Community Name List

No.	Community String	Rights	Network ID of Trusted Host	Number of Mask Bit	Action

Parameter	Description
Community Name	
Community String	Enter a community string; this will function as a password for requests from the management station. An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The

	community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
Rights	Select Read-Only to allow the SNMP manager using this string to collect information from the Switch. Select Read-Write to allow the SNMP manager using this string to create or edit MIBs (configure settings on the Switch).
Network ID of Trusted Host	Type the IP address of the remote SNMP management station in dotted decimal notation, for example 192.168.1.0.
Number of Mask Bit	Type the length of the subnet mask bits.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Community Name List	
No.	This field displays the index number of an entry.
Community String	This field displays the community string of an entry.
Rights	This field displays the right of an entry.
Network ID of Trusted Host	This field displays the network ID of trusted host of an entry.
Number of Mask Bit	This field displays the length of the subnet mask bits of an entry.
Action	Click the **Delete** button to remove the entry.

8.1.3 SNMP Trap Event State Settings

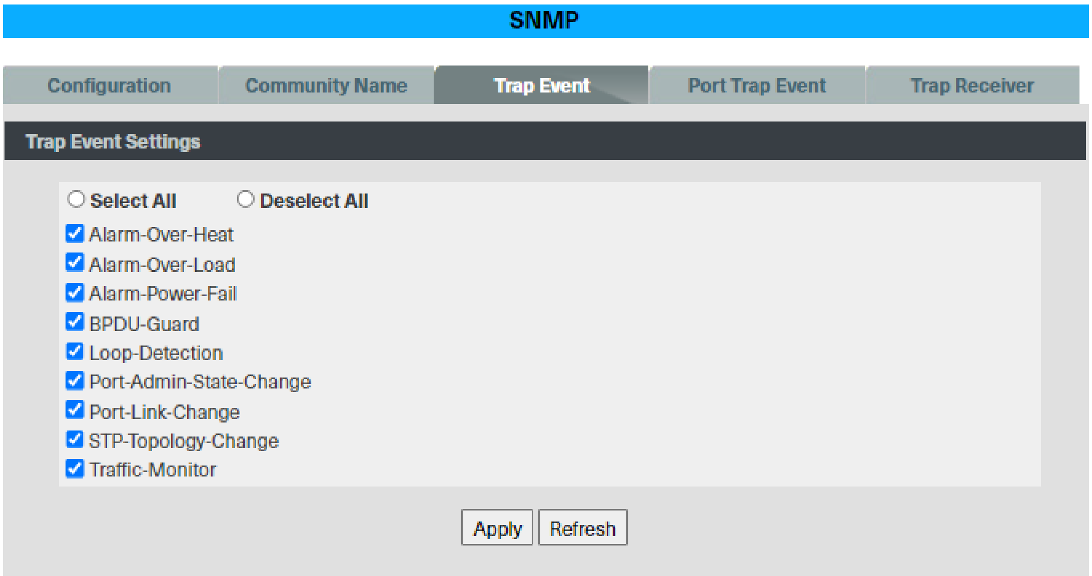
The features allow users to enable/disable individual trap notification.

8.1.3.1 Event Settings CLI Configuration

Node	Command	Description
enable	show SNMP trap-event	This command displays the SNMP configurations.

configure	SNMP trap-event alarm-over-heat (disable/enable)	This command enables/disables the alarm-over-heat trap.
configure	SNMP trap-event alarm-over-load (disable/enable)	This command enables/disables the alarm-over-load trap.
configure	SNMP trap-event alarm-power-fail (enable/enable)	This command enables/disables the alarm-power-fail trap.
configure	SNMP trap-event bpdu (disable/enable)	This command enables/disables the BPDU port state change/BPDU Root Guard/BPDU Guard trap.
configure	SNMP trap-event loop-detection (disable/enable)	This command enables/disables the loop-detection trap.
configure	SNMP trap-event port-admin-state-change (disable/enable)	This command enables/disables the port-admin-state-change trap.
configure	SNMP trap-event port-link-change (disable/enable)	This command enables/disables the port-link-change trap.
configure	SNMP trap-event power-source-change (disable/enable)	This command enables/disables the power-source-change trap.
configure	SNMP trap-event stp-topology-change (disable/enable)	This command enables/disables the stp-topology-change trap.
configure	SNMP trap-event traffic-monitor (disable/enable)	This command enables/disables the traffic-monitor trap.

8.1.3.2 Web Trap Event Settings Configuration



○ Select All ○ Deselect All

☑ Alarm-Over-Heat
☑ Alarm-Over-Load
☑ Alarm-Power-Fail
☑ BPDU-Guard
☑ Loop-Detection
☑ Port-Admin-State-Change
☑ Port-Link-Change
☑ STP-Topology-Change
☑ Traffic-Monitor

The features allow users to enable/disable individual trap notification.

Alarm-Over-Heat Alarm-Over-Load Alarm-Power-Fail	- Trap when system's temperature is too high. - Trap when system is overloaded. - Trap when system power is over voltage/under voltage/RPS over voltage/RPS under voltage.
BPDU-Guard Loop-Detection Port-Admin-State-Change Port-Link-Change STP-Topology-Change Traffic-Monitor	- Trap when port is blocked by BPDU Guard/BDPU Root Guard/BPDU port state changed. - Trap when port is blocked by Loop Detection. - Trap when port is enabled/disable by administrator. - Trap when port is link up/down change. - Trap when the STP topology change. - Trap when port is blocked by Traffic Monitor.

Parameter	Description
Trap Event State Settings	
Select all	Enables all of trap events.
Deselect All	Disables all of trap events.
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

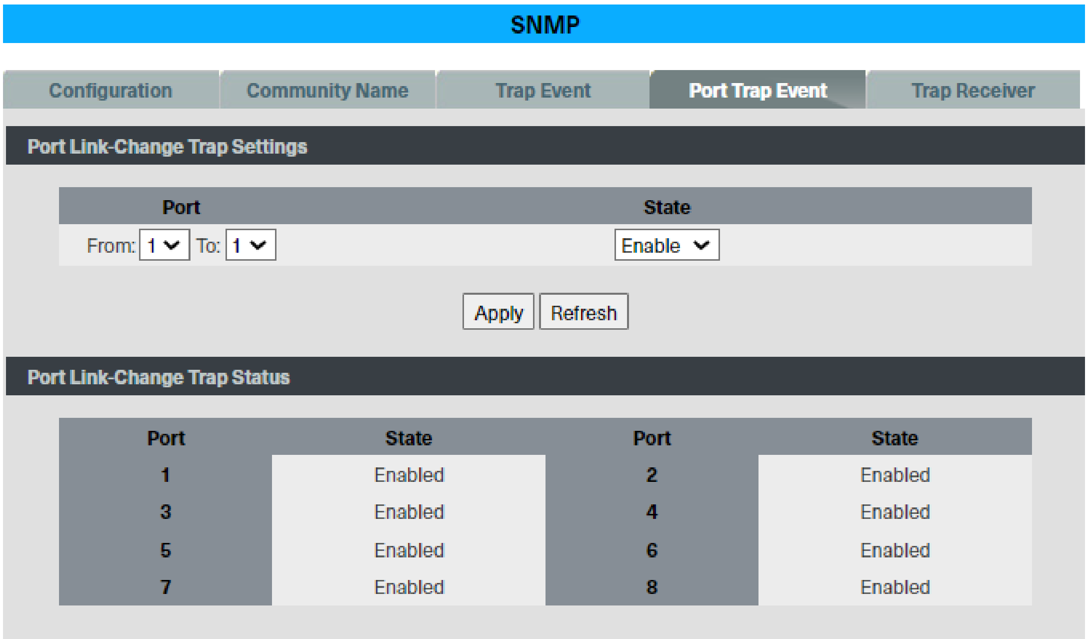
8.1.4 SNMP Port Link-Change Trap Settings

The features allow users to enable/disables port-link-change trap notification by individual port.

8.1.4.1 Port Event Settings CLI Configuration

Node	Command	Description
enable	show SNMP port-link-change-trap	This command displays the SNMP port link-change trap configurations.
interface	SNMP port-link-change-trap	This command enables the link change trap on the specific port.
interface	no SNMP port-link-change-trap	This command disables the link change trap on the specific port.
config	interface range (fastethernet1/0/ | gigabitethernet1/0/) PORTLISTS	This command enters the interface configure node.
if-range	SNMP port-link-change-trap	This command enables the link change trap on the specific ports.
if-range	no SNMP port-link-change-trap	This command disables the link change trap on the specific ports.

8.1.4.2 Port Even Settings Web Configuration



Port Link-Change Trap Settings

Port	State
From: 1 To: 1	Enable

Port Link-Change Trap Status

Port	State	Port	State
1	Enabled	2	Enabled
3	Enabled	4	Enabled
5	Enabled	6	Enabled
7	Enabled	8	Enabled

Parameter	Description
Trap Event State Settings	
Port	Selects the range of ports.
State	User can enable /disable trap events when port link change.
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

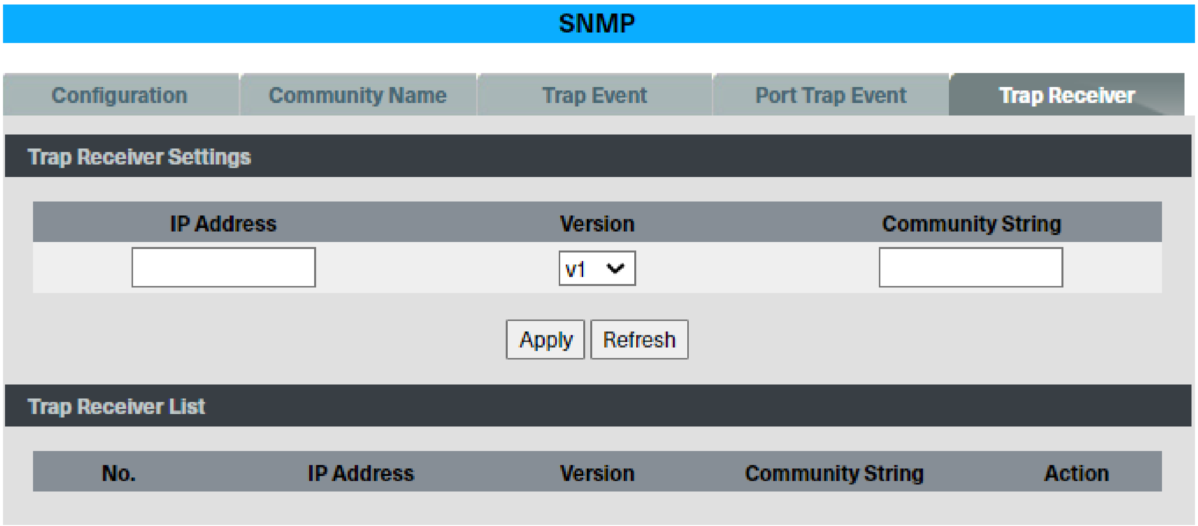
8.1.5 SNMP Trap Receiver Settings

The features allow users to configure trap receiver configuration.

8.1.5.1 SNMP Trap Receiver CLI Configuration

Node	Command	Description
configure	SNMP trap-receiver IPADDR VERSION COMMUNITY String	This command configures the trap receiver's configurations, including the IP address, version (v1 or v2c) and community String.

8.1.5.2 Web Trap Receiver Configuration



IP Address	Version	Community String
	v1	

No.	IP Address	Version	Community String	Action

Parameter	Description
IP Address	Enter the IP address of the remote trap station in dotted decimal notation.
Version	Select the version of the Simple Network Management Protocol to use. **v1**or **v2c**.
Community String	Specify the community string used with this remote trap station.
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Trap Receiver List	
No.	This field displays the index number of the trap receiver entry. Click the number to modify the entry.
IP Address	This field displays the IP address of the remote trap station.
Version	This field displays the version of Simple Network Management Protocol in use. **v1**or **v2c**.
Community String	This field displays the community string used with this remote trap station.
Action	Click **Delete** to remove a configured trap receiver station.

8.2 SNMPv3

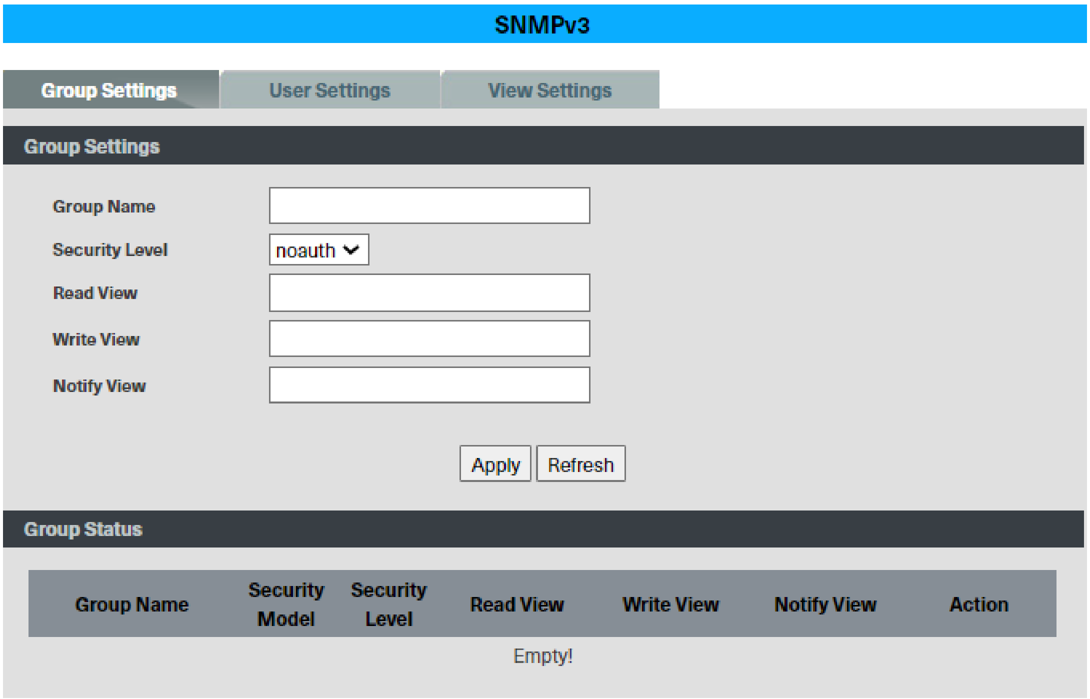
SNMP version 3 (SNMPv3) supports authentication and encryption. SNMPv3 uses the user-based security model (USM) for message security and the view-based access control model (VACM) for access control. USM specifies authentication and encryption.

8.2.1 CLI Configuration

Node	Command	Description
enable	show SNMP user	This command displays all SNMP v3 user.
enable	show SNMP group	This command displays all SNMP v3 group.
enable	show SNMP view	This command displays all SNMP v3 view.
configure	SNMP user USERNAME GROUPNAME noauth	Configures v3 user of non-authentication.
configure	SNMP user USERNAME GROUPNAME auth (MD5|SHA) STRINGS	Configures v3 user of authentication.
configure	SNMP user USERNAME GROUPNAME priv (MD5|SHA) STRINGS des STRINGS	Configures v3 user of authentication and encryption.
configure	SNMP group GROUPNAME noauth (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of non-authentications.
configure	SNMP group GROUPNAME auth (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of authentications.
configure	SNMP group GROUPNAME priv (read STRINGS write STRINGS notify STRINGS)	Configures v3 group of authentication and encryption.
configure	SNMP view VIEWNAME STRINGS (included|excluded)	To identify the subtree.
configure	no SNMP user USERNAME GROUPNAME	This command removes a v3 user from switch.
configure	no SNMP group GROUPNAME	This command removes a v3 group from switch.

configure	no SNMP view VIEWNAME STRINGS	This command removes a v3 view from switch.

8.2.2 Web SNMPv3 Group Configuration



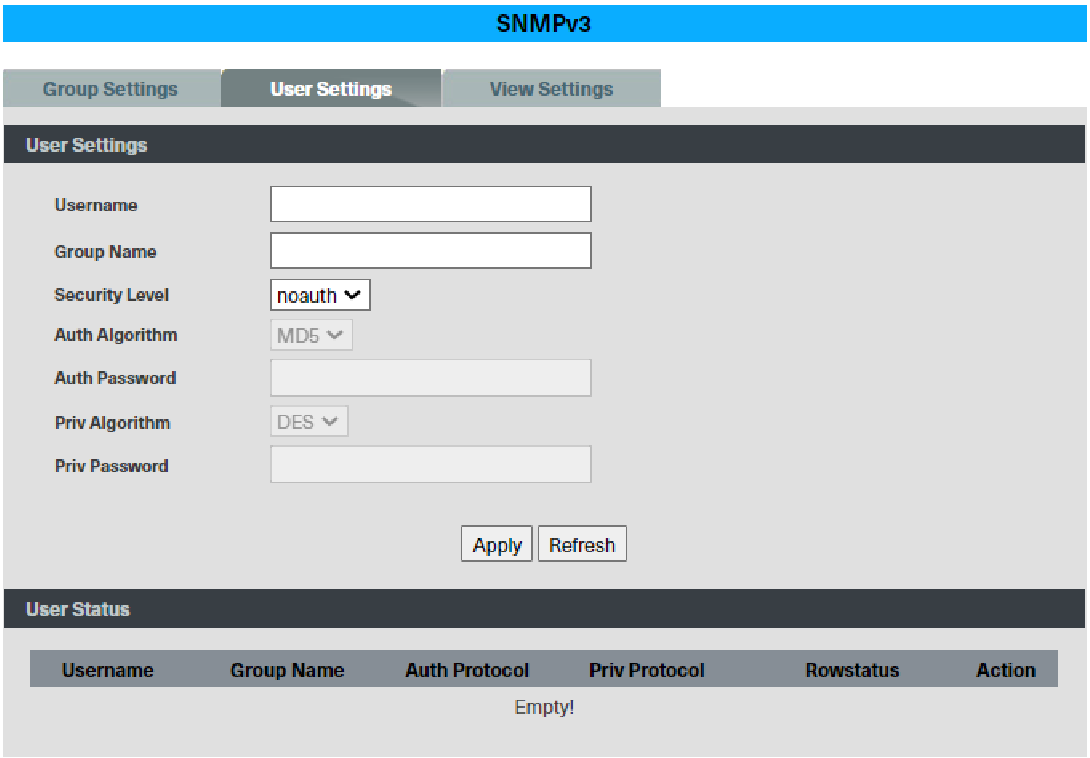
Group Name	Security Model	Security Level	Read View	Write View	Notify View	Action

Empty!

Parameter	Description
Group Name	Enter the v3 username.
Security Level	Select the security level of the v3 group to use.
Read View	Note that if a group is defined without a read view than all objects are available to read. (Default value is **none**.)
Write View	if no write or notify view is defined, no write access is granted, and no objects can send notifications to members of the group. (Default value is **none**.)
Notify View	By using a notify view, a group determines the list of notifications its users can receive.(default value is **none**.)
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
SNMPv3 Group Status	
Group Name	This field displays the v3 username.

Security Model	This field displays the security model of the group. Always displayed **v3**: User-based Security Model (USM)
Security Level	This field displays the security level to this group.
Read View	These fields display the View list of this group.
Write View	
Notify View	
Action	Click **Delete** to remove a v3 group.

8.2.3 Web SNMPv3 User Configuration



SNMPv3

User Settings

Username:
Group Name:
Security Level: noauth
Auth Algorithm: MD5
Auth Password:
Priv Algorithm: DES
Priv Password:

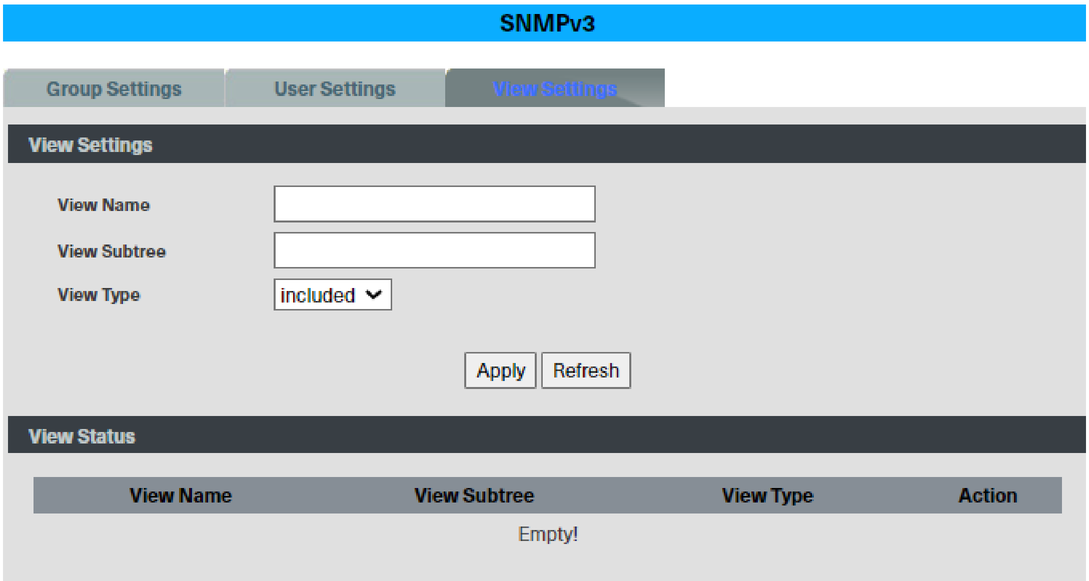
User Status

Username	Group Name	Auth Protocol	Priv Protocol	Rowstatus	Action
Empty!					

Parameter	Description
Username	Enter the v3 username.
Group Name	Map the v3 username into a group name.
Security Level	Select the security level of the v3 user to use. **noauth** means no authentication and no encryption. **auth** means messages are authenticated but not encrypted. **priv** means messages are authenticated and encrypted.

Auth Algorithm	Select **MD5** or **SHA** Algorithm when security level is **auth** or **priv.**
Auth Password	Set the password for this user when security level is **auth** or **priv.** (pass phrases must be at least 8 characters long!)
Priv Algorithm	Select **DES** encryption when security level is **priv.**
Priv Password	Set the password for this user when security level is **priv.** (pass phrases must be at least 8 characters long!)
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
SNMPv3 User Status	
Username	This field displays the v3 username.
Group Name	This field displays the group name which the v3 user mapping.
Auth Protocol	These fields display the security level to this v3 user.
Priv Protocol	
Row status	This field displays the v3 user row status.
Action	Click **Delete** to remove a v3 user.

8.2.4 Web SNMPv3 View



View Settings

View Name:

View Subtree:

View Type: included

View Status

View Name	View Subtree	View Type	Action

Empty!

Parameter	Description
View Name	Enter the v3 view name for creating an entry in the SNMPv3 MIB view table.
View Subtree	The OID defining the root of the subtree to add to (or exclude from) the named view.
View Type	Select **included** or **excluded** to define subtree adding to the view or not.
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
SNMPv3 View Status	
View Name	This field displays the v3 view name.
View Subtree	This field displays the subtree.
View Type	This field displays the subtree adding to the view or not.
Action	Click **Delete** to remove a v3 view.

8.3 SNTP

Introduction

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. A less complex implementation of NTP, using the same protocol but without requiring the storage of state over extended periods of time is known as the **Simple Network Time Protocol** (**SNTP**). NTP provides Coordinated Universal Time (UTC). No information about time zones or daylight-saving time is transmitted; this information is outside its scope and must be obtained separately.

UDP Port: 123.

Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.

Note:

1. The SNTP server always replies to the UTC current time.
2. When the Switch receives the SNTP reply time, the Switch will adjust the time with the time zone configuration and then configure the time to the Switch.
3. If the time server's IP address is not configured, the Switch will not send

any SNTP request packets.

4. If no SNTP reply to packets, the Switch will retry every 10 seconds forever.
5. If the Switch has received SNTP reply, the Switch will re-get the time from NTP server every 24 hours.
6. If the time zone and time NTP server have been changed, the Switch will repeat the query process.
7. No default SNTP server.

Default Settings

```
Current Time:
---------------------------------------------
   Time: 0:3:51 (UTC)
   Date: 1970-1-1
Time Server Configuration:
---------------------------------------------
   Time Zone : +00:00
   IP Address: 0.0.0.0

Daylight Saving Time Configuration:
---------------------------------------------
   State       : disabled
   Start Date: None.
   End Date : None.
```

8.3.1 SNTP CLI Configuration

Node	Command	Description
enable	show time	This command displays current time and time configurations.
configure	time HOUR:MINUTE:SECOND	Sets the current time on the Switch. *hour*: 0-23 *min*: 0-59 *sec*: 0-59 Note: If you configure Daylight Saving

		Time after you configure the time, the Switch will apply Daylight Saving Time.
configure	time date YEAR/MONTH/DAY	Sets the current date on the Switch. *year*: 1970- *month*: 1-12 *day*: 1-31
configure	time daylight-saving-time	This command enables the daylight-saving time.
configure	no time daylight-saving-time	This command disables daylight saving on the Switch.
configure	time daylight-saving-time start-date (first | second | third | fourth | last) (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) MONTH HOUR	This command sets the start time of the Daylight-Saving Time.
configure	time daylight-saving-time end-date (first | second | third | fourth | last) (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) MONTH HOUR	This command sets the end time of the Daylight-Saving Time.
configure	time ntp-server (disable|enable)	This command disables / enables the NTP server state.
configure	time ntp-server IP_ADDRESS	This command sets the IP address of your time server.
configure	Time zone STRING	Configures the time difference between UTC (formerly known as GMT) and your time zone. Valid value: -1200 ~ +1200.

8.3.2 SNTP Web Configuration

Parameter	Description
Current Time and Date	
Current Time	This field displays the time you open / refresh this menu.
Current Date	This field displays the date you open / refresh this menu.
Time and Date Setting	
Manual	Select this option if you want to enter the system date and time manually.
New Time	Enter the new date in year, month and day format and time in hour, minute and second format. The new date and time then appear in the **Current Date** and **Current Time** fields after you click **Apply**.
Enable Network Time Protocol	Select this option to use Network Time Protocol (NTP) for the time service.
NTP Server	Select a pre-designated time server or type the IP address or type the domain name of your time server. The Switch searches for the timeserver for up to 60 seconds.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone.
Daylight Saving Settings	
State	Select **Enable** if you want to use Daylight Saving Time. Otherwise, select **Disable** to turn it off.
Start Date	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving Time. The time is displayed in the 24-hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So, in the United States you would select **Second**, **Sunday**, 3(**March)** and **2:00**.

	Daylight Saving Time starts in the European Union on the last Sunday of March. All the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So, in the European Union you would select **Last**, **Sunday**, 3(**March)** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving Time. The time field uses the 24-hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So, in the United States you would select **First**, **Sunday**, 11(**November)** and **2:00**. Daylight Saving Time ends in the European Union on the last Sunday of October. All the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So, in the European Union you would select **Last**, **Sunday**, 10(**October)** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click this button to take effect the settings.
Refresh	Click this button to reset the fields to the last setting.

8.4 System Information

Introduction

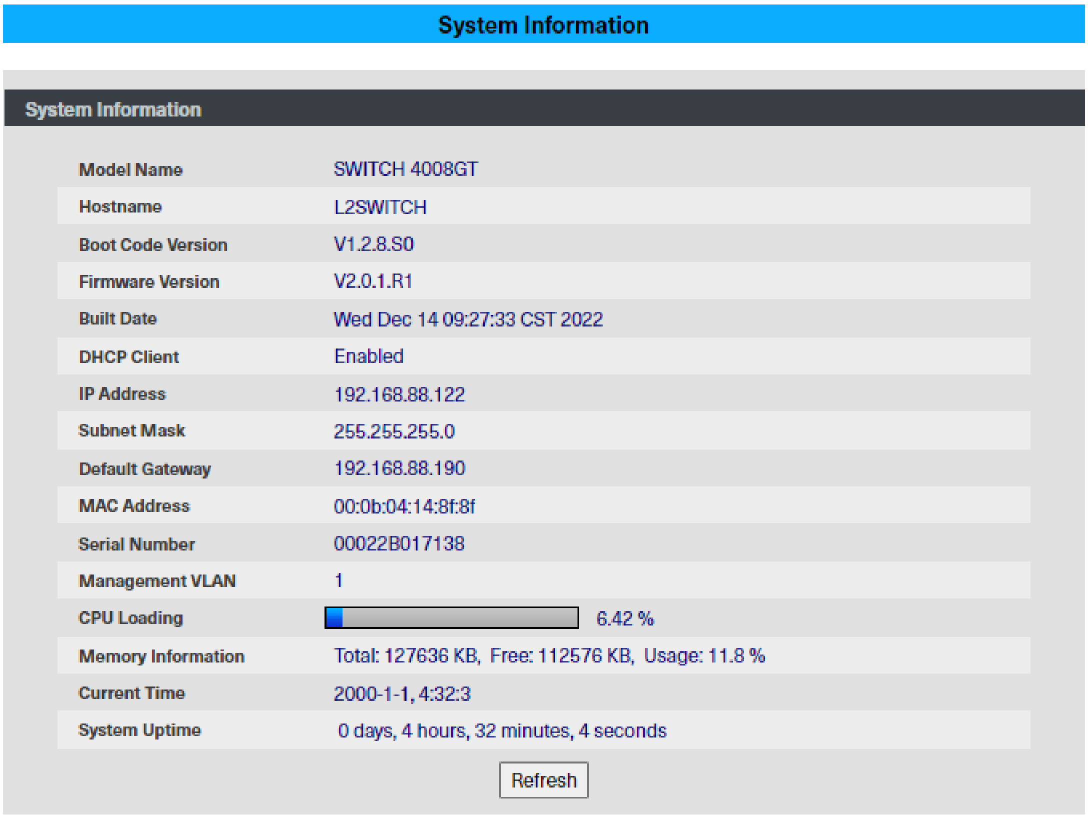
The System Information window appears each time you log into the program. Alternatively, this window can be accessed by clicking System Information.

8.4.1 CLI System Information command

Node	**Command**	**Description**
enable	show model	This command will display information of

		switch like vendor, product, mac-address, serial boot code, firmware version etc....

8.4.2 GUI System Information



System Information

System Information

Model Name	SWITCH 4008GT
Hostname	L2SWITCH
Boot Code Version	V1.2.8.S0
Firmware Version	V2.0.1.R1
Built Date	Wed Dec 14 09:27:33 CST 2022
DHCP Client	Enabled
IP Address	192.168.88.122
Subnet Mask	255.255.255.0
Default Gateway	192.168.88.190
MAC Address	00:0b:04:14:8f:8f
Serial Number	00022B017138
Management VLAN	1
CPU Loading	6.42 %
Memory Information	Total: 127636 KB, Free: 112576 KB, Usage: 11.8 %
Current Time	2000-1-1, 4:32:3
System Uptime	0 days, 4 hours, 32 minutes, 4 seconds

Parameter	**Description**
System Information	
Model Name	This field displays the model’s name of the Switch.
Host name	This field displays the host name of the Switch.
Boot Code Version	This field displays the boot code version.
Firmware Version	This field displays the firmware version.
Built Date	This field displays the built date of the firmware.
DHCP Client	This field displays whether the DHCP client is enabled on the Switch.
IP Address	This field indicates the IP address of the Switch.
Subnet Mask	This field indicates the subnet mask of the Switch.

Default Gateway	This field indicates the default gateway of the Switch.
MAC Address	This field displays the MAC (Media Access Control) address of the Switch.
Serial Number	The serial number assigned by manufacture for identification of the unit.
Refresh	Click **Refresh** to begin configuring this screen afresh.

8.5 System Maintenance

8.5.1 Configuration

Upload and Download Configuration

8.5.1.1 CLI Configuration

Node	**Command**	**Description**
configure	write memory	This command writes current operating configurations to the configuration file.
configure	archive download-config <URL PATH>	This command downloads a new copy of configuration file from TFTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file
configure	archive upload-config <URL PATH>	This command uploads the current configurations file to a TFTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file
configure	reload default-config	This command copies a default-config file to replace the current one. **Note:** The system will reboot automatically to take effect the configurations.

8.5.1.2 GUI Configuration

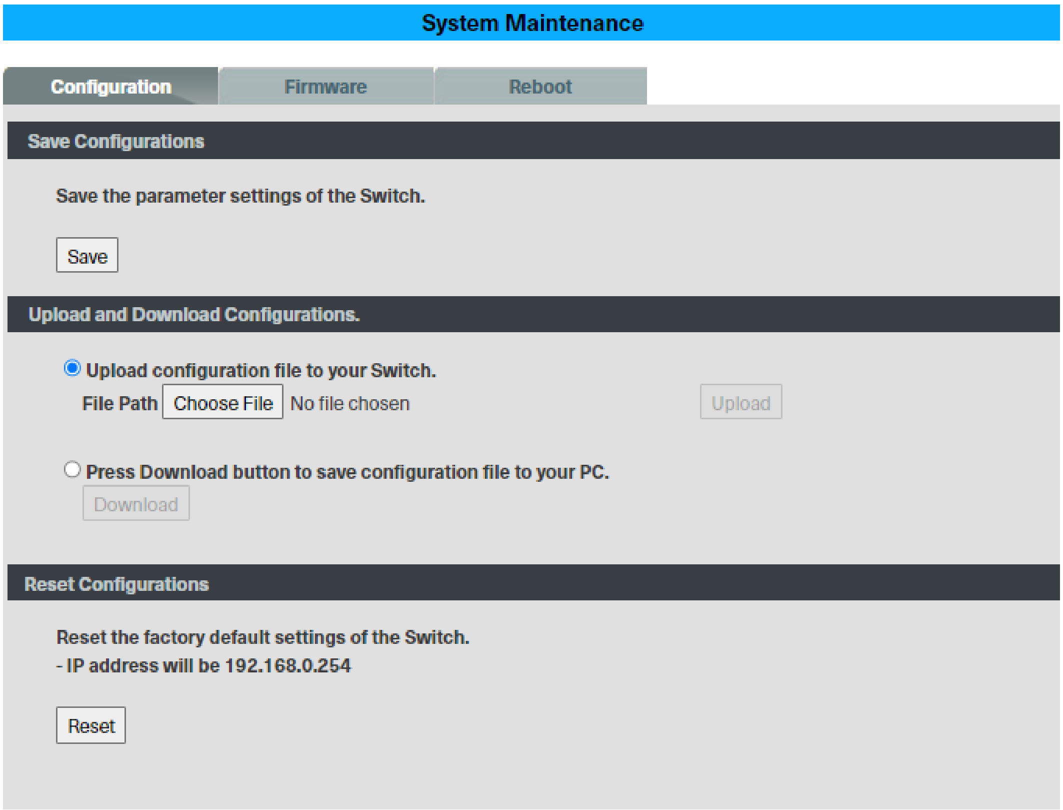
Click the “**Choose File**” button to select the new configuration file which you want to upgrade it to the Switch.

Click the “**Upload**” button to start the upgrade procedures.

Click the “**Download**” button to download the current configurations to local host.

Reset Configuration

Click the “**Reset**” button to reset the system configurations to default values.



System Maintenance

Save Configurations

Save the parameter settings of the Switch.

Upload and Download Configurations.

● Upload configuration file to your Switch.

File Path Choose File No file chosen

○ Press Download button to save configuration file to your PC.

Reset Configurations

Reset the factory default settings of the Switch.
- IP address will be 192.168.0.254

8.5.2 Firmware

Upgrade Firmware

8.5.2.1 CLI Configuration

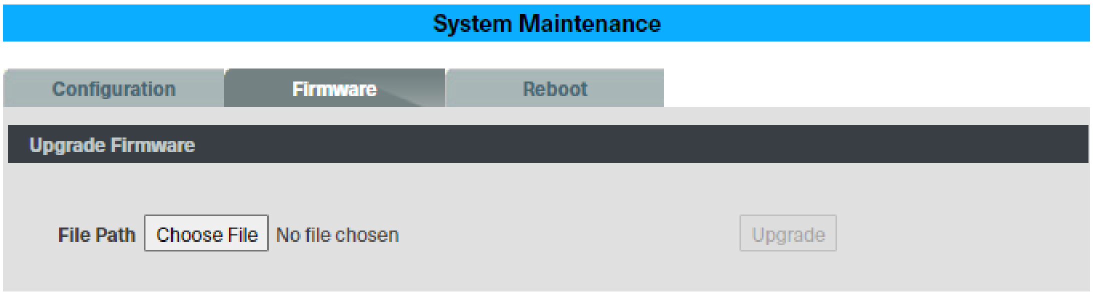
Node	Command	Description
configure	archive download-fw <URL PATH>	This command downloads a new copy of firmware file from TFTP / FTP / HTTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file

		http://192.168.1.1/file tftp://192.168.1.1/file

8.5.2.2 GUI Configuration

Click the “**Choose File**” button to select the new firmware which you want to upgrade it to the Switch.

Click the “**Upgrade**” button to start the upgrade procedures.



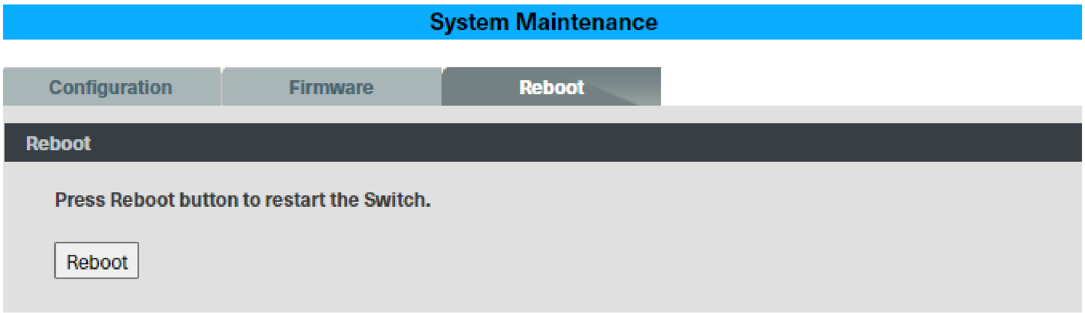
8.5.3 Reboot

8.5.3.1 CLI Configuration

Node	Command	Description
configure	reboot	This command reboots the system.

8.5.3.2 GUI Configuration

Click the “**Reboot**” button to restart the Switch.



Press Reboot button to restart the Switch.

8.6 User Account

Introduction

The Switch allows users to create up to 6 user account. The Username and the password should be the combination of the digit or the alphabet. The last admin user account cannot be deleted. Users should input a valid user account to login the CLI or web management.

User Authority:

The Switch supports two types of the user account, admin and normal. The **default** users account is **username (admin) / password (admin)**.

- Admin - read / write.
- Normal - read only.
  ; Cannot apply any configurations in web.

The Switch also supports backdoor user account. In case of that user forgot their Username or password, the Switch can generate a backdoor account with the system's MAC. Users can use the new user account to enter the Switch and then create a new user account.

Default Settings

Maximum user account	: 6.
Maximum Username length	: 32.
Maximum password length	: 32.
Default user account for privileged mode	: admin / admin.

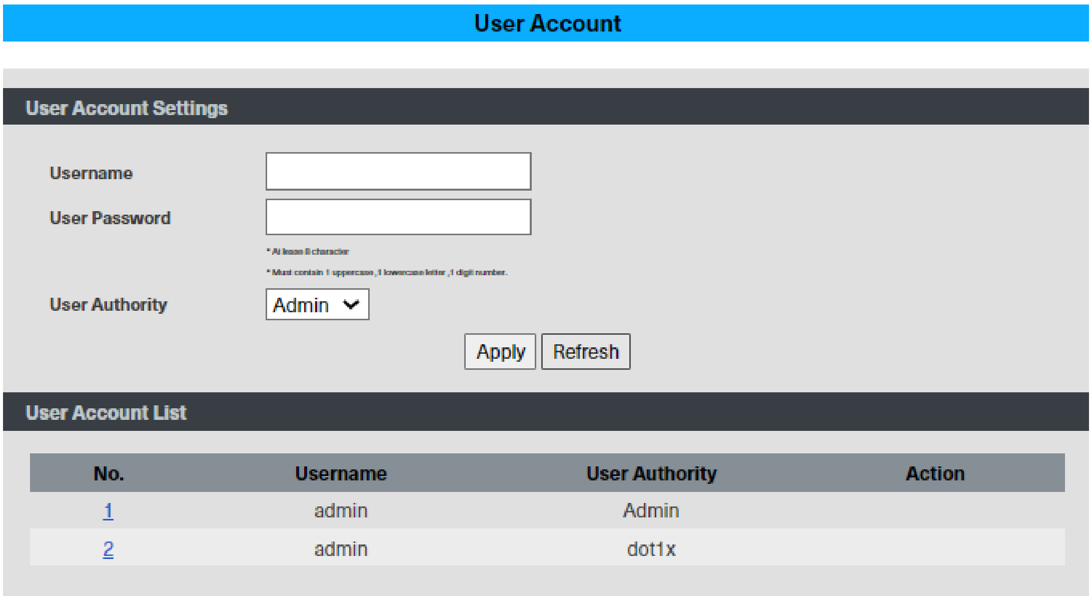
Notices

- The Switch allows users to create up to 6 user account.
- The Username and the password should be the combination of the digit or the alphabet.
- The last admin user account cannot be deleted.
- The maximum length of the username and password is 32 characters.

8.6.1 CLI Configuration

Node	Command	Description
enable	show user account	This command displays the current user accounts.
configure	add user USER_ACCOUNT PASSWORD (normal|admin|dot1x)	This command adds a new user account with choice of privileges normal/admin/dot1x.
configure	delete user USER_ACCOUNT	This command deletes a present user account.

8.6.2 Web configuration



User Account

User Account Settings

Username	
User Password	
	* At least 8 character * Must contain 1 uppercase ,1 lowercase letter ,1 digit number.
User Authority	Admin

User Account List

No.	Username	User Authority	Action
1	admin	Admin	
2	admin	dot1x	

Parameter	Description
User Account Settings	
Username	Type a new username or modify an existing one.
User Password	Type a new password or modify an existing one. Enter up to 32 alphanumeric or digit characters.
User Authority	Select with which group the user associates. **admin** (read and write) or **normal** (read only) for this user account Dot1x user for radius.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
User Account List	
No.	This field displays the index number of an entry.
Name	This field displays the name of a user account.
Authority	This field displays the associated group.
Action	Click the **Delete** button to remove the user account. Note: You cannot delete the last admin accounts.

9 SALZ Automation Support

9.1 Contact and Support Information

QR code below will provide the complete contact information along with respective branch addresses

Official Website: https://www.salz-automation.com