850G-10PWI

Industrial 10-Port GbE Managed PoE Switch

User Manual

Version 1.00

Table of Contents

1 Introduction

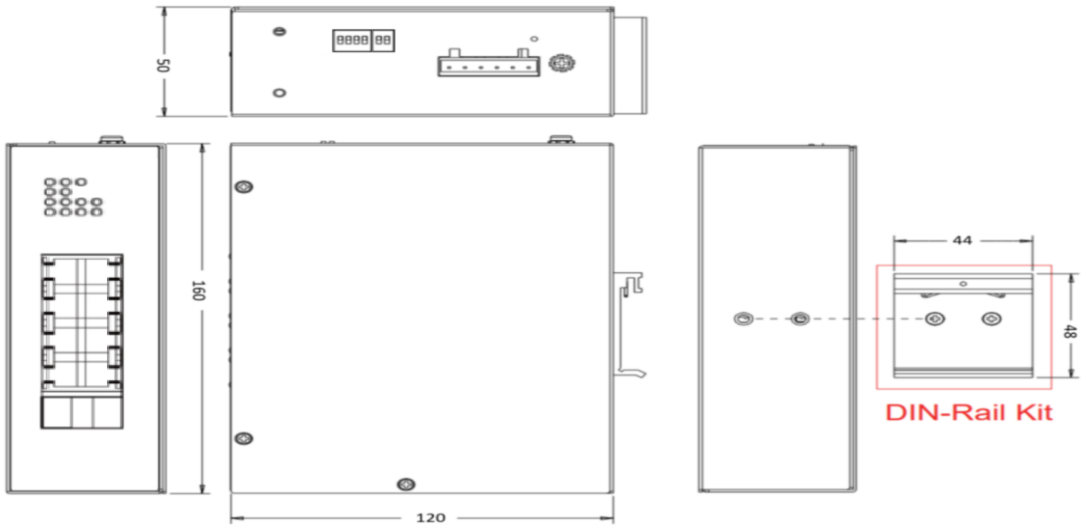
Proscend 850G-10PWI Industrial Ethernet Switch features friendly manageability in full Gigabit Ethernet networks, as well as 1000Mbps Ethernet speed over copper and fiber for enabling quality of services, network security, and resilience. As a result, the 850G-10PWI is the perfect solution for reducing network response time for mission-critical applications such as video security, transportation, energy, etc.

The 850G-10PWI's built-in power booster enables extra wide range power input from 24VDC to 57VDC, for widening external power supply selection, each of the 8 10/100/1000Base-T ports with Power-over-Ethernet power source is IEEE 802.3at compliant and capable of delivering up to 30 watts to power an IP camera, IP phone, Wi-Fi Access Point or advanced HMI, to ease the power cabling over single Ethernet cable. The 2 SFP slots are used to work with SFP (Small form-factor pluggable) fiber transceivers to scale out modern industrial networks with the ring, daisy chain, or tree topologies.

1.1 Features

- Wide range power DC input 24 - 57VDC/6A
- Embedded dashboard of real-time device monitoring
- Embedded topology map and friendly management on neighboring devices
- Operating temperature -10°C ~ 70°C
- Total PoE power budget up to 240W
- ERPS Ring failover protection
- Jumbo Frames
- DIN-rail mounted

1.2 Dimensions



1.3 Specifications

Interface

- 8 x 10/100/1000BASE-T PoE RJ45
- 2 x 100FX/GbE SFP
- DIP Switch
- 6-PIN Terminal Block

Standards

- IEEE 802.3 10BASE-T
- IEEE 802.3u 100BASE-TX/FX
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3z 1000BASE-SX/LX
- IEEE 802.3 Auto-negotiation
- IEEE 802.3x Flow Control
- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- IEEE 802.1Q VLAN Tagging
- IEEE 802.1p Class of Service
- IEEE 802.1X Port Authentication
- IEEE 802.1AB LLDP
- IEEE 802.1D STP
- IEEE 802.3az Energy Efficient Ethernet (EEE)
- IEEE 802.3af Power over Ethernet
- IEEE 802.3at Power over Ethernet Plus

Performance

- Jumbo Frame Size: 10KBytes
- MAC Table Entries: 8K
- Switch Fabric: 20Gbps

Reliability

- STP/RSTP
- ERPS v1/v2
- Code redundancy

Management

- HTTP, HTTPS, CLI, Telnet, SSH
- SNMP v1, v2c, v3, Trap, Syslog,
- Management VLAN
- LLDP
- Web Firmware Upgrade, SNTP, DHCP Client
- Port Mirroring

VLAN

- 802.1Q VLAN
- Port-based VLAN (Port Isolation)

Traffic Control

- 802.1p QoS, Flow Control, Traffic Monitor
- Storm Control, Port Isolation, Loop Detection
- Storm alarm threshold per port

Security

- ACL
- Port Security (MAC limit)
- Port-based 802.1X
- BPDU Guard / Filter, ROOT Guard
- Trusted Managed Host

PoE/PoE+

- PoE Scheduling, PD Alive Check
- PoE Power on/off, PoE Priority
- Power budget control per system/port
- Power Delay

Mechanical

- Dimension (H x D x W): 160 x 120 x 50 mm
- Weight: 560g
- DIN-rail
- Metal IP30

Power

- DC input 24~57 VDC/6A
- System power consumption: 13W
- PoE Power Budget: 120W @ 24 VDC, 240W @ 48 VDC
- Alarm relay output: 1A @ 24 VDC

LED Indicators

- Power input, PoE, Alarm
- Ethernet LAN Port Link & Speed, SFP Port Link

Environment & Regulatory Compliance

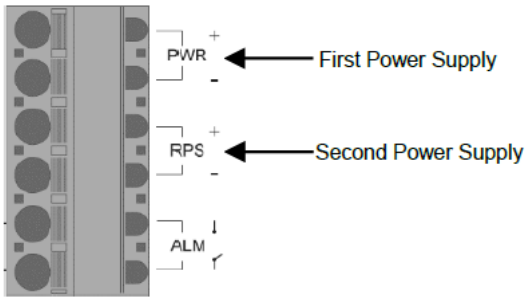
- Operation temperature: -10 to +70°C
- Storage temperature: -40 to +85 °C
- Humidity (non-condensing): 5 to 95% RH
- Vibration, Shock & Freefall: IEC60068-2-6, -27, -32
- EMI: FCC Part 15 Subpart B Class A, EN 55032 (class A), EN55011 (2009 class A), EN 61000-6-4
- EMS: EN 55035, EN 61000-6-2, EN 61000-4-2 (ESD), EN 61000-4-3 (RS), EN 61000-4-4 (Burst), EN 61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-6 (PFMF)

2 Hardware Installation

This chapter introduces how to install and connect the hardware.

2.1 Connecting Power

The 850G-10PWI Industrial Ethernet Switch can be powered from two power supplies (input range 24~57 VDC). Two power supplies are on the top panel of the switch. Insert the positive and negative wires (AWG 12-24) into V+ and V- contacts on the terminal block respectively and use a flat-head screwdriver to push in and open the wire clamp

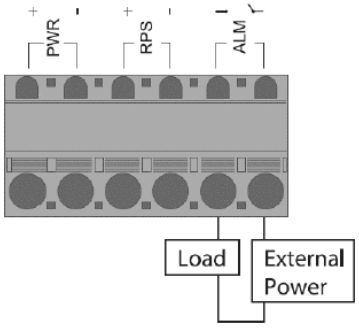


⚠ WARNING

The DC power should be connected to a well-fused power supply.

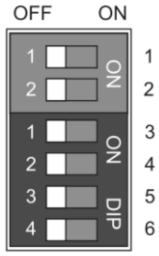
2.2 Alarm Relay and Ground

- The alarm relay output contacts are shown as ALM next to the DC terminal block connector as the figure below.
- The alarm relay out is “Normal Open”, and it will be closed when it is detecting any predefined failure such as power failures.
- The relay output with current carrying capacity of 1A @ 24 VDC.
- The switch must be properly grounded for optimum system performance.



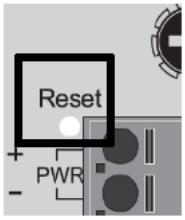
Ground Connector

2.3 DIP Switch Setting



DIP	Function Description
1 (PWR) 2 (RPS)	ON: Power alarm reporting is enabled. OFF: Power alarm reporting is disabled.
3 (Storm)	ON: Broadcast storm control is enabled. OFF: Broadcast storm control is disabled.
4 (QoS)	ON: Port Priority is enabled on Port 2. OFF: Port Priority is disabled.
5 (Port 9) 6 (Port 10)	ON: Port 100FX support is enabled. OFF: Port 100FX support is disabled.

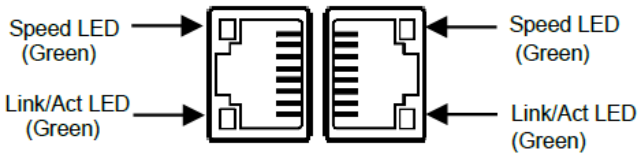
2.4 Reset Button



Function	Operation
Reboot	Press the Reset button for 2 seconds and release.
Reset to factory default	Press the Reset button for 10 seconds and release.

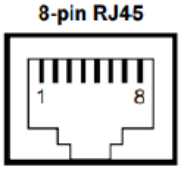
2.5 LED Indicators

LED	Color	Description
PWR/RPS	On: Green	PWR/RPS is powered.
	Off	PWR/RPS is not powered.
ALM	On: Red	Alarm for abnormal power status or function.
	Off	Normal operation or DIP switch OFF.
RJ45 LAN port Link/Act	On: Green	Ethernet LINK UP.
	Blinking: Green	Ethernet traffic detected.
	Off	Ethernet LINK DOWN.
RJ45 LAN port Speed	On: Green	Ethernet LINK UP at 1000Mbps.
	Off	Ethernet LINK DOWN or LINK UP at 10Mbps/100Mbps
UPLINK	On: Green	LINK UP.
	Blinking: Green	Traffic detected.
	Off	LINK DOWN.
PoE	On: Green	PoE PD (Powered Device) connected.
	Off	PoE PD (Powered Device) disconnected.



2.6 RJ45 Connector Pinouts

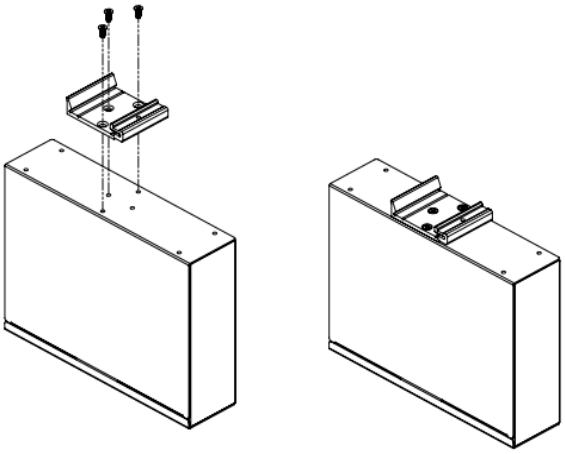
The pin assignment of RJ45 connector is shown in the following table.



Pin	Description	PoE Pinouts
1,2	T/Rx+, T/Rx-	V+
3,6	T/Rx+, T/Rx-	V-
4,5	T/Rx+, T/Rx-	X
7,8	T/Rx+, T/Rx-	X

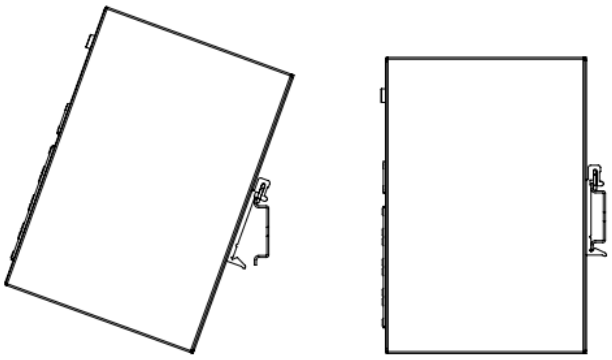
2.7 DIN-rail Mounting

STEP 1: Use the screws to install the DIN-rail kit to attach at the rear side of the switch.



STEP 2: Hook the unit onto the DIN-rail.

STEP 3: Push the bottom of the unit towards the DIN-rail until it locks in place.



2.8 Web Interface Connect & Login

1. Factory default IP: 192.0.2.1
2. Login with default account and password.

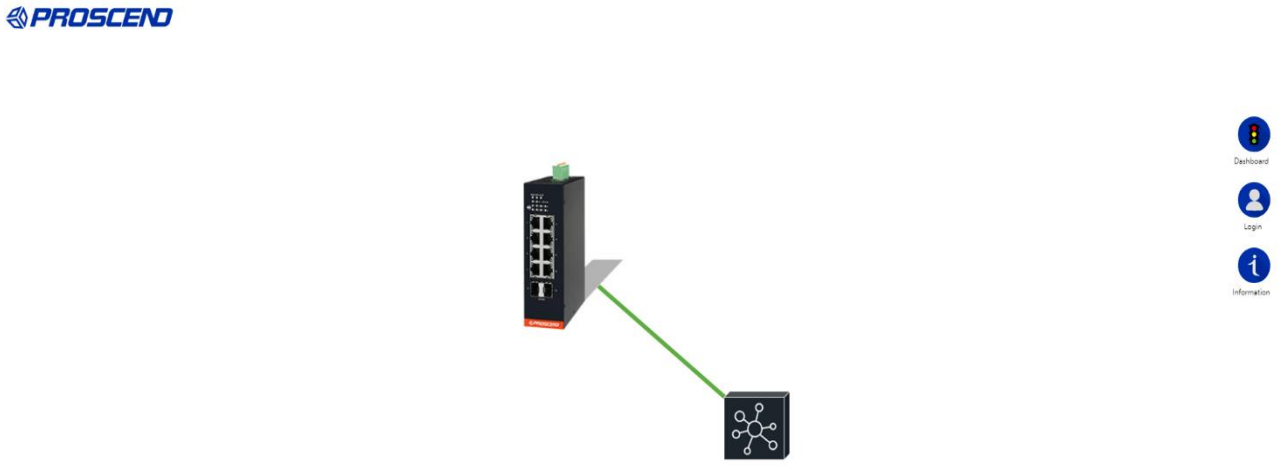
   Username: root

   Password: 2wsx#EDC

3 Using the Web

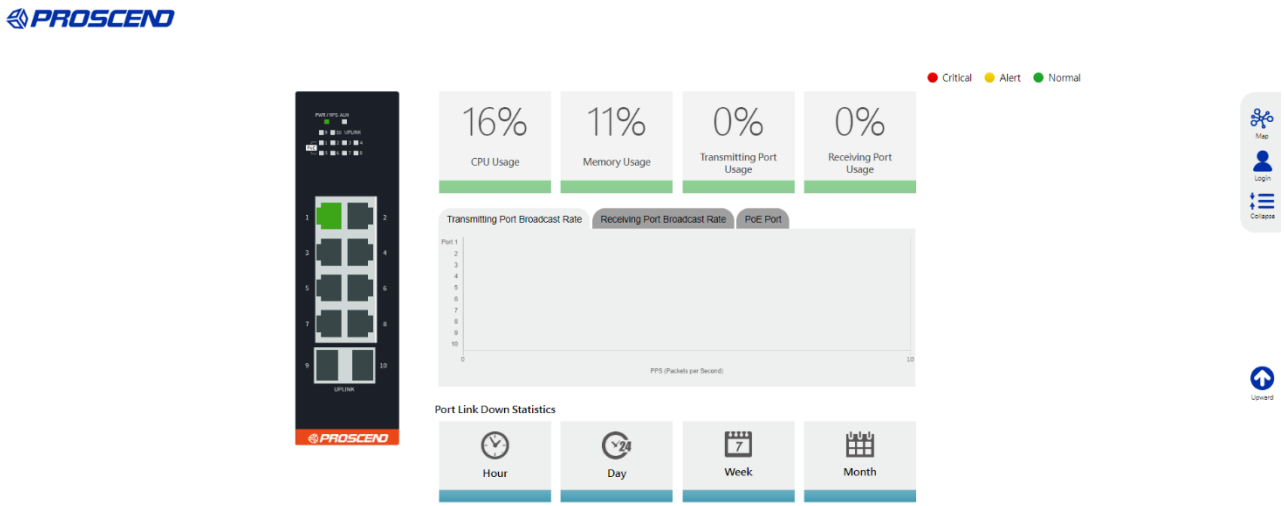
3.1 Topology Map

Open Browser and enter default IP address http://192.0.2.1, the Topology Map will be displayed, it is a feature to check neighbor devices' information or to configure them easily.



3.2 Dashboard

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 tricolor scheme as the Topology Map.



3.3 Login

This section provide instruction to login

1. Open Browser and enter default IP address http://192.0.2.1.
2. Click “Login”.
3. Fill Username and Password.
4. Click “LOGIN”.

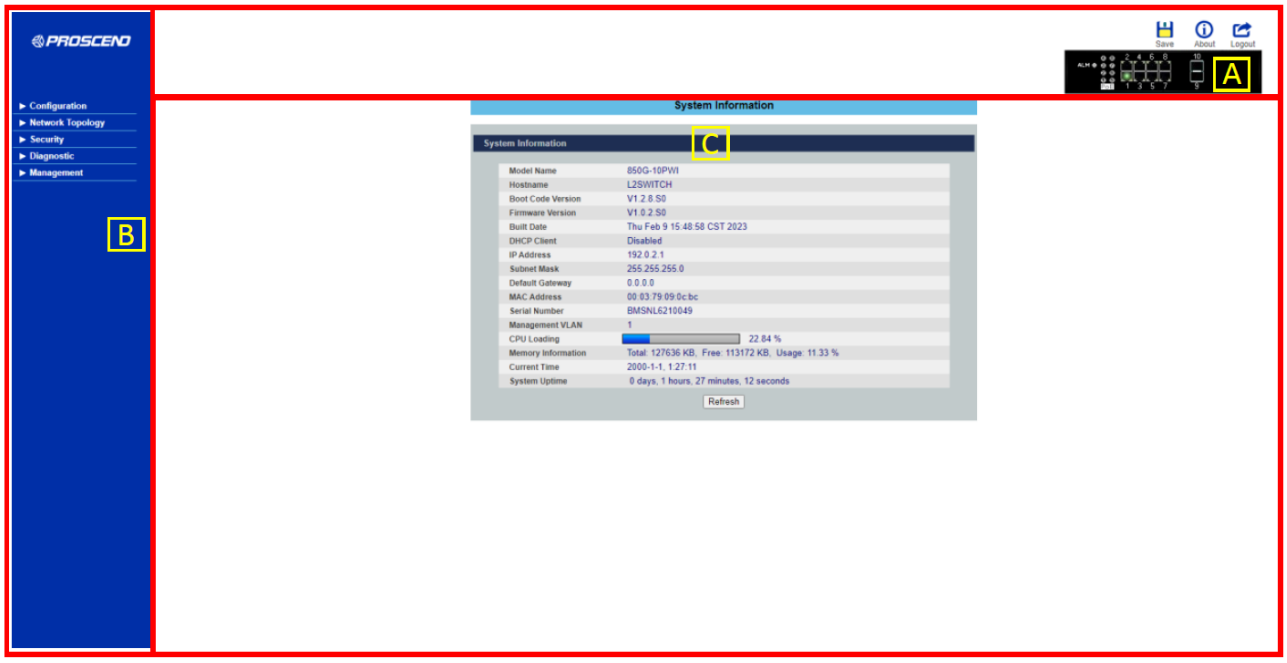
Item	Description
Username	Login username. The maximum length is 32. Default: root
Password	Login user password. The maximum length is 32. Default: 2wsx#EDC

3.4 Navigation

The main screen is divided into three parts as below.

A - Title Bar, B - Navigation Panel and C - Main Window.

The menu items are divided into main and sub menu to configure the settings and get the status of connectivity on the navigation panel.



(1) A : Title Bar

The title bar provides Save, About, Logout buttons and switch indicators.

Item	Description
Save	All configuration should be saved in order to prevent reset after switch reboot.
About	Show the switch information including model name, boot code version, firmware version and build date.
Logout	Logout from the switch.
Switch indicators	Provide switch indicators to check general status of switch including alarm, PoE and link status.

(2) B : Navigation Panel-Main Menu and Sub Menu

The menu items are divided into main and sub menu to configure the settings and get the status of connectivity on the navigation panel.

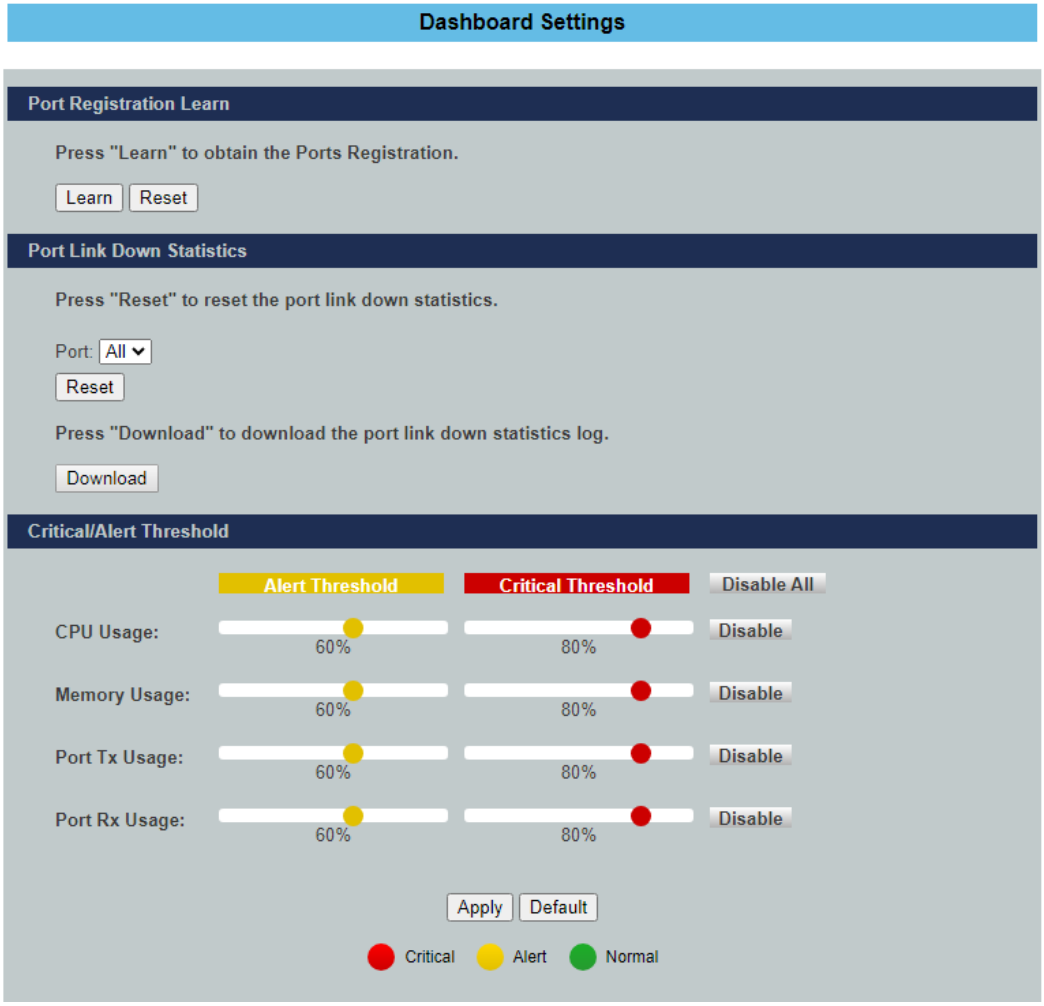
(3) C : Main Window

This section shows the information or setting fields from main menu and sub menu.

4 Configuration

4.1 Dashboard Settings

The dashboard setting enables you to setup the display of the switch performance like CPU, Memory, Port Tx Usage, Port Rx Usage. Learn option to obtain to port registration information.



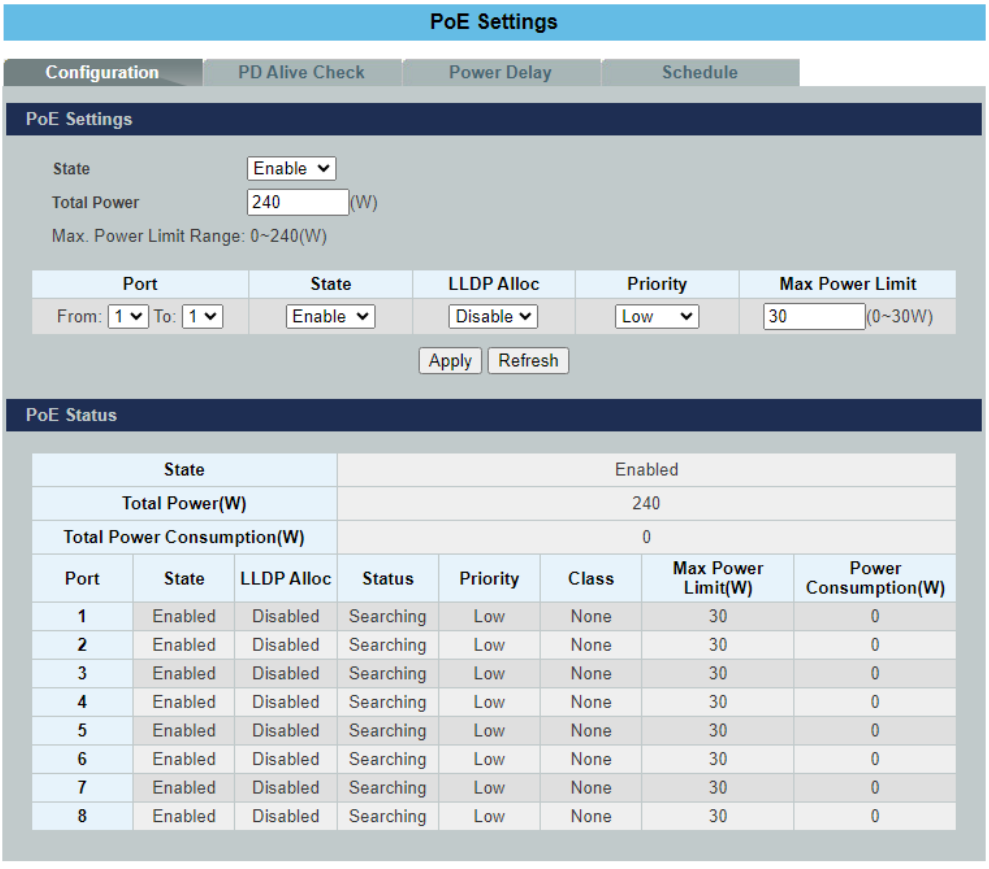
Item	Description
Port Registration Learn	
Learn	This field is to obtain the port registration information.
Reset	Reset option to reset the port registration information
Port Link Down Statistics	
Port	User can select individual port or all ports information to reset to default on registration information
Reset	Reset option to reset the selected port registration information

Download	This field will download the statistics of port down information along with date 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 normal, alert, critical percentage of the interface Tx usage or disable the feature
Port Rx Usage	User can configure threshold value to normal, alert, critical percentage of the interface Rx usage or disable the feature
Apply	This field is used for apply the changes made
Default	This field will make the Switch to default values.

4.2 PoE Settings

Power over Ethernet or PoE technology describes a system to pass electrical power safely, along with data, on Ethernet cabling.

4.2.1 Configuration

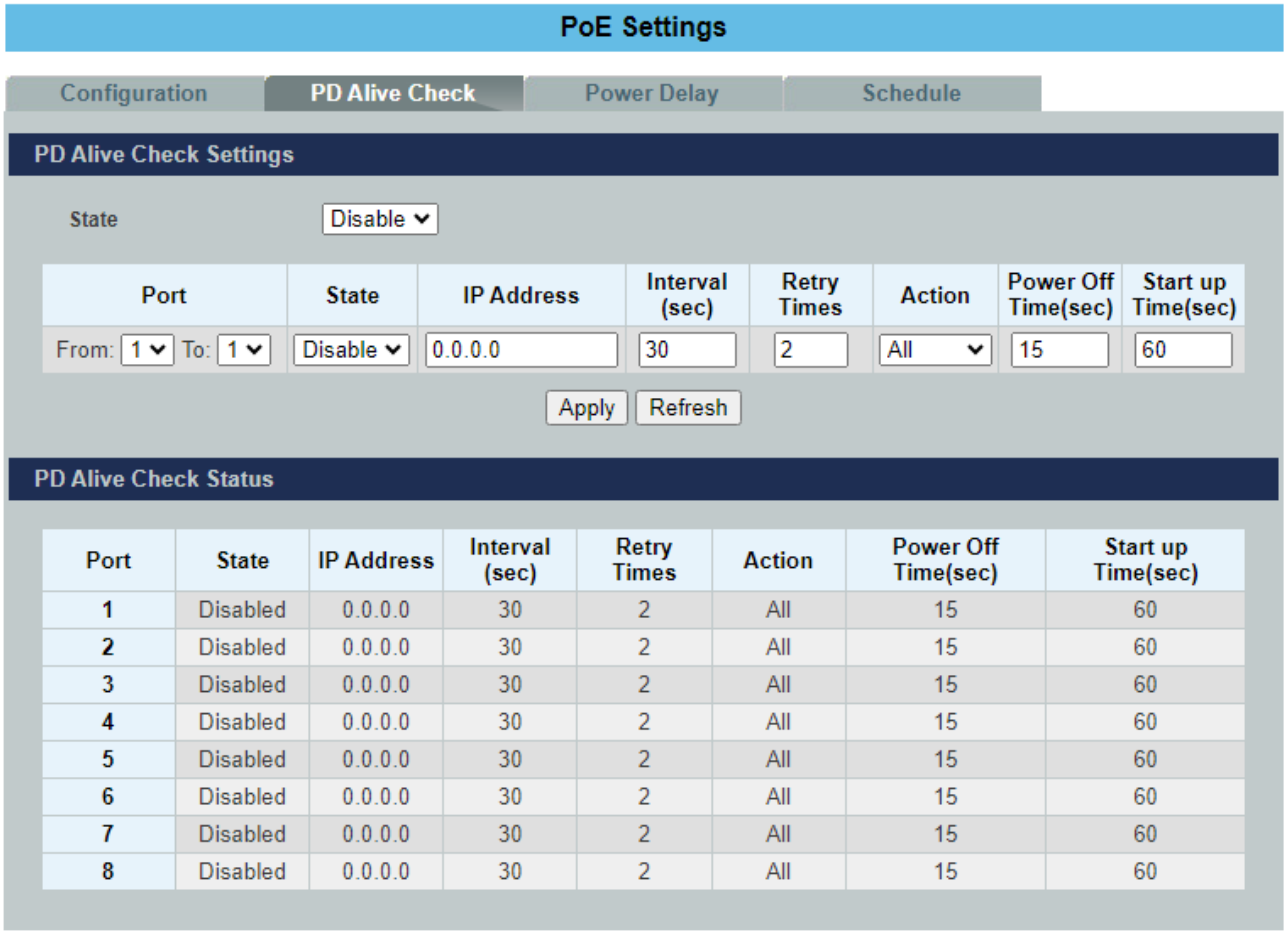


Item	Description
PoE Settings	
State	Selects **Enable** to enable the PoE function on the Switch. Selects **Disable** to disable the PoE function on the Switch.
Total Power	Total PoE power budget of the device can be configured Max Power Limit Range is 240 (W). Total Power (P) = Current of adaptor (I) * Voltage of adaptor (V)
Port	Select a port or a range of ports which to configure loop detection.
State	Selects **Enable** to enable the PoE function on the specific port. Selects **Disable** to disable the PoE function on the specific port.
Priority	Selects **Critical / High / Low** priority for the specific port.
Max Power Limit	Interface wise PoE power budget can be configured with respect to requirement Maximum Power Limit Range is 30W
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
PoE Configuration Status	
State	Displays the current PoE mode.
Total Power (W)	Displays the total power that the Switch supports.
Total Power Consumption (W)	Displays the total consuming power for all the PDs.
Port	Display the Port No.
State	Displays the PoE state for the specific port (Enable/ Disable).
Status	Displays the current status for the specific port (Searching or Delivering)
Priority	Displays the PoE priority for the specific port for PD.
Class	The field displays the class mode which the PSE negotiate with the PD on the specific port.
Max Power Limit (W)	Displays the maximum PoE power for that specific port
Power Consumption (W)	Displays the consuming power for the specific port.

4.2.2 PD Alive Check

The function has a global state configuration. If the global state configuration is enabled. The Switch will check the configurations of every port.

If the port's state is enabled, the Switch will send keep-a-live probe packet every interval time. If the host cannot respond when the keep-a-live probe packet count is over the retry times, the Switch performs the action, reboot/alarm/all to the Power Device, depending on the port's configuration.

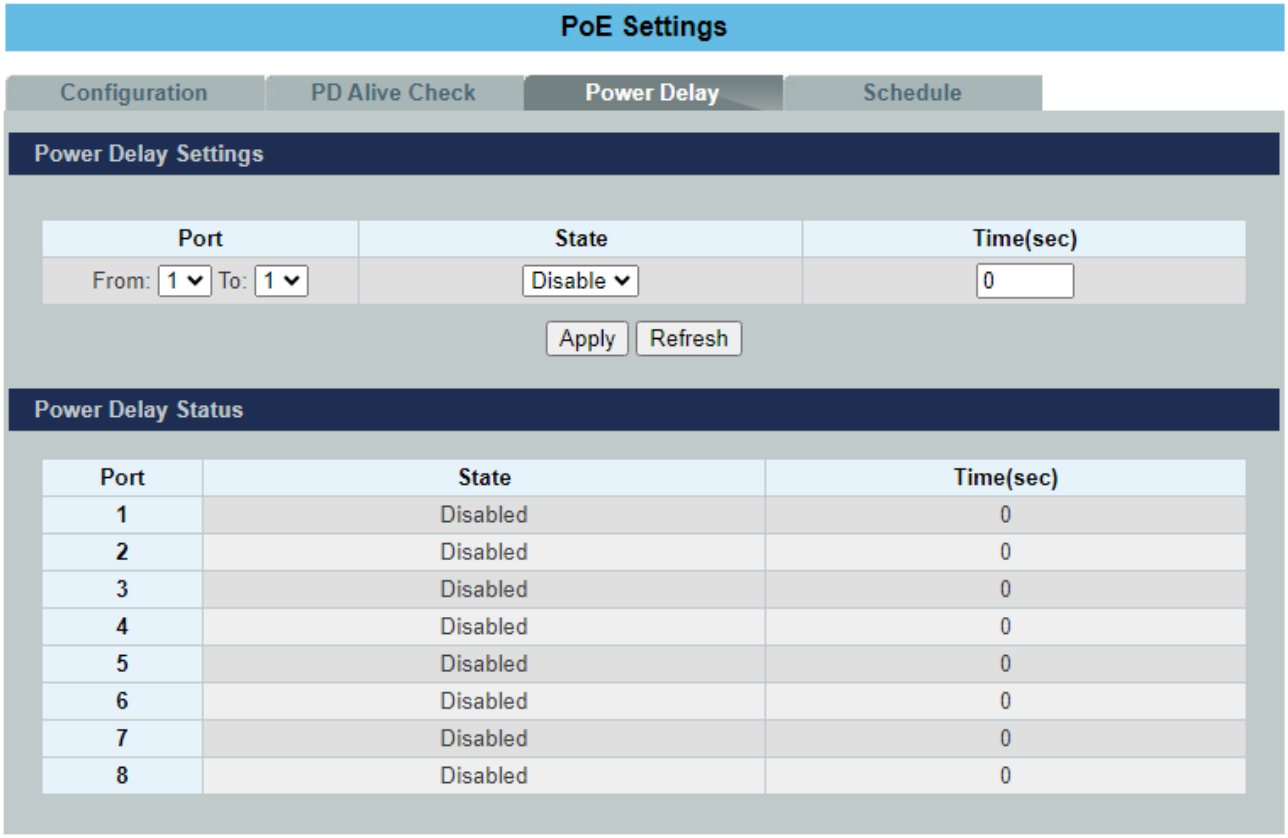


Item	Description
State	Enables/Disables the PD Alive Check.
Port	Selects a port or a range of ports which you want to configure.
State	Enables/Disables the PD Alive Check for the specific port(s).
IP Address	Specifies the Host IP address which connects to the port.
Interval	The interval to send the packet probes to check if the host is still alive.
Retry Time	The retry times when no response from the host for the keep-a-live probe packet.

Action	The action to the Power Device when the system detects that the Power Device cannot respond the keep-a-live probe packet. All: Send an alarm message to inform the administrator and then reboot the PD. Alarm: Just send an alarm message to inform the administrator. None: Keep Ping the remote PD but does nothing further. Reboot: Cut off the power of the PoE port, make PD rebooted.
Power Off Time	When PD has been rebooted, the PoE port restored power after the Power Off Time.
Start Up Time	The Switch waits the Start Up Time to do PoE Auto Checking when the PD is rebooting.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

4.2.3 Power Delay

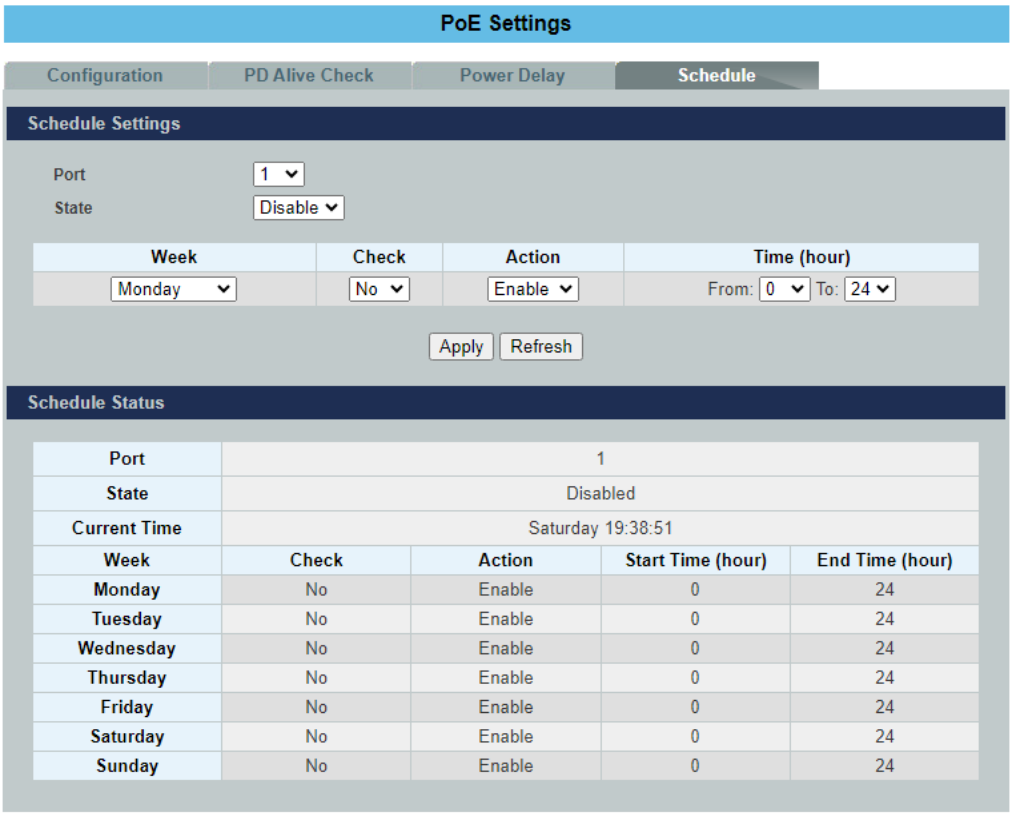
The Power Delay allows the user to setting the delay time of power providing after device rebooted.



Item	Description
Power Delay Settings	
Port	Selects a port or a range of ports which you want to configure.
State	Enables/Disables the PoE Power Delay for the specific ports.
Time	The delay time for the specific ports.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Power Delay Status	
Port	The port ID.
State	The PoE power delay state for the port.
Time	The PoE power delay time for the port.

4.2.4 Schedule

The function has a global state configuration. If the global state configuration is disabled. The Switch will not perform the schedule function. If the global state is enabled, the Switch will check every port's configuration.



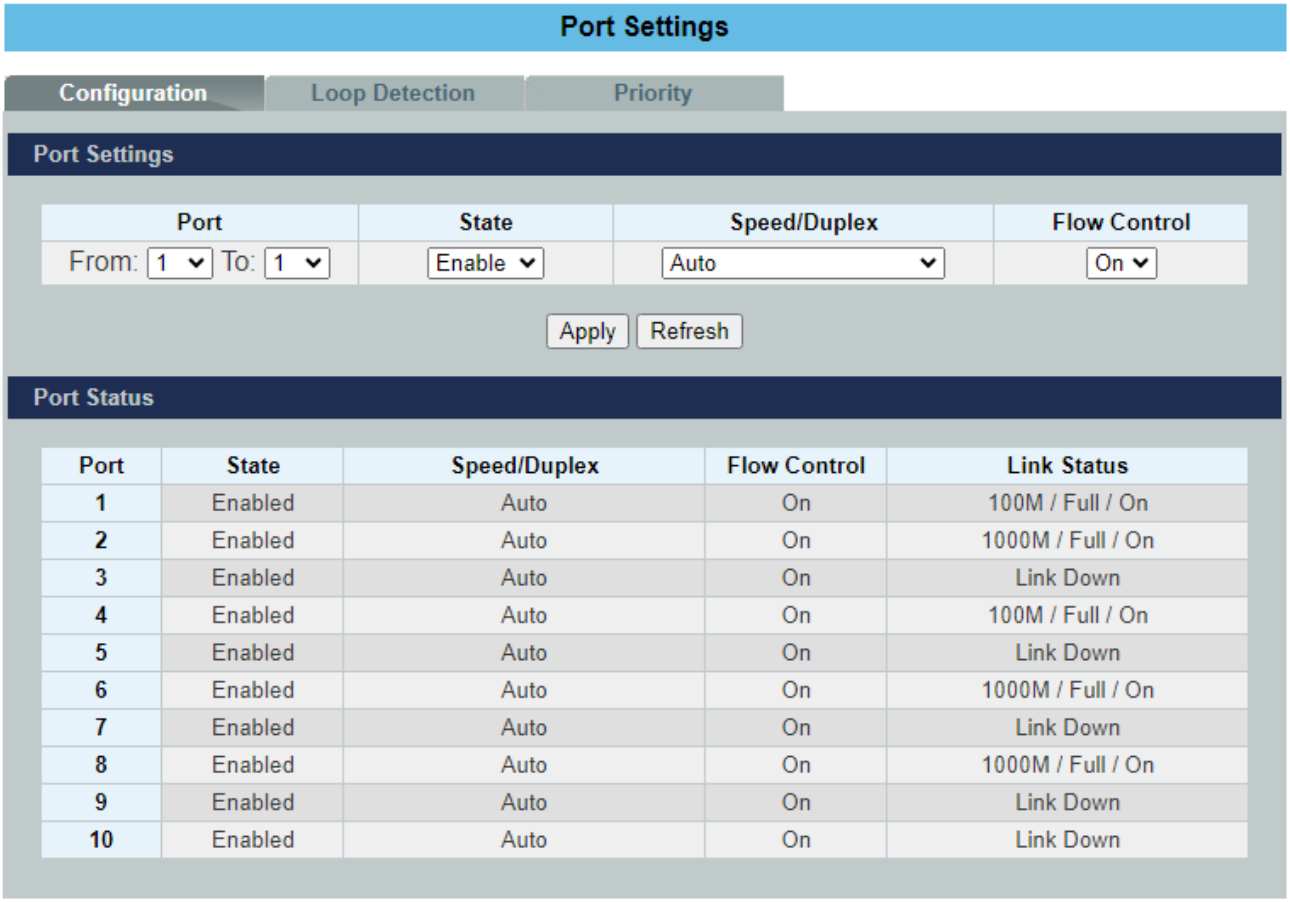
Item	Description
Schedule Settings	
Port	Selects a port that you want to configure the PoE schedule function.
State	Select PoE schedule on interface enable/disable by default it is Disabled
Week	Select a week day that you want to configure the schedule.
Check	Enables or Disables the PoE schedule on the specific port for a defined time period.
Action	Selects action enable/disable for the specific port for a particular day or week.
Time (Hour)	User can configure the PoE Schedule time from 0 to 24 Hrs
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Schedule Status	
Port	Display the port ID
State	Display the state of the interface enable/disable
Current time	Display the current day and time
Check	Display the status of yes/no for PoE schedule per week
Action	Display the status of action enable/disable
Start Time (Hour)	Display the start time in Hrs of PoE schedule configured on interface
End Time (Hour)	Display the end time in Hrs of PoE schedule configured on interface

4.3 Port Settings

This section allows you to setup port, loop detection and priority.

4.3.1 Configuration

This section allows you to setup switch port state, recovery state and recovery time(min) and check port status.

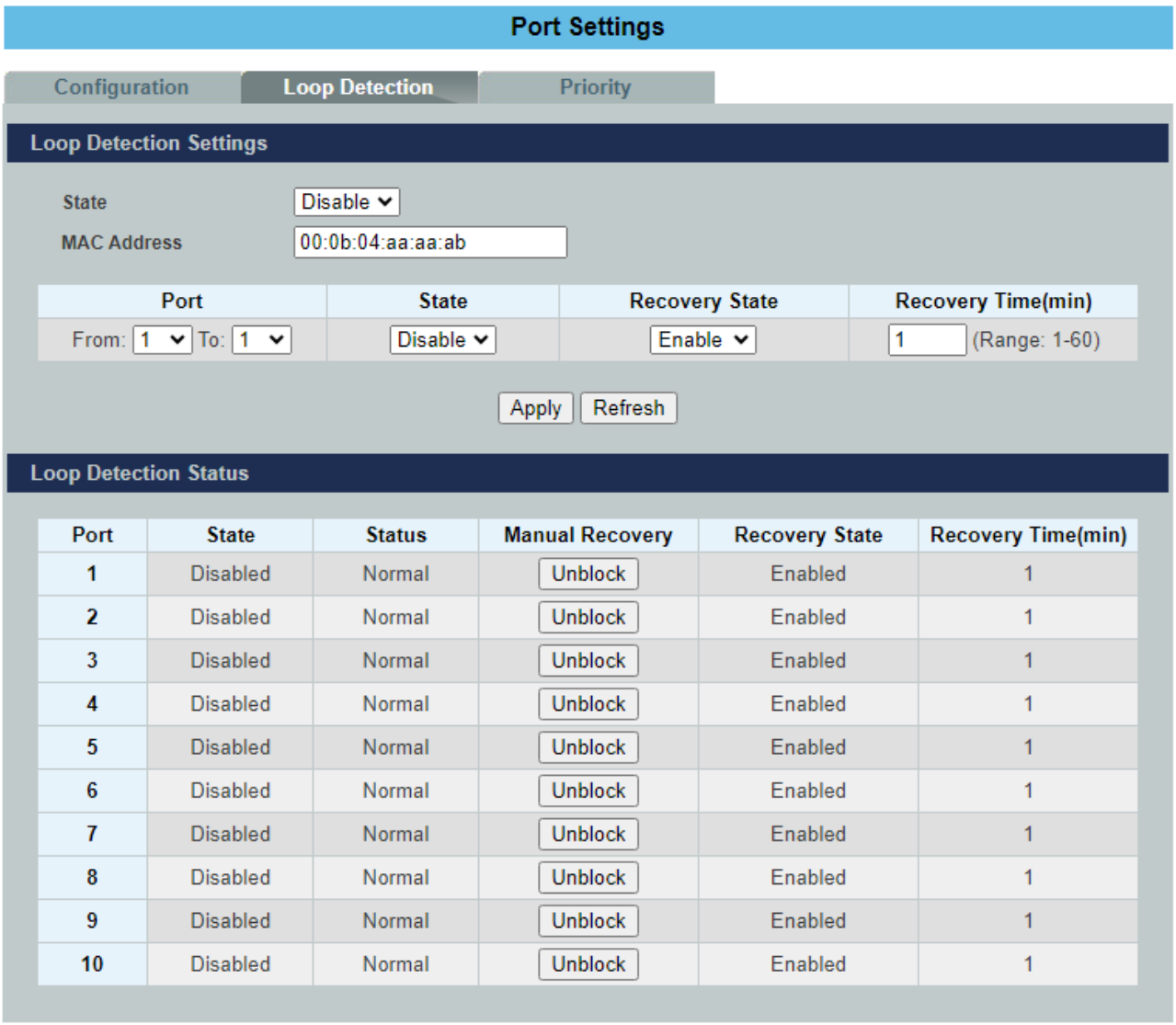


Item	Description
Port Settings	
Port	Selects a port or a range of ports on which to configure the port.
State	Select option to enable / disable the port.
Speed/duplex	Select a speed/duplex for port(s).
Flow Control	User can configure flow control on interface on/off
Apply	Click **Apply** to take effect 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 on the flow control on interface on/off
Link Status	This field displays the link status of a port.

4.3.2 Loop Detection

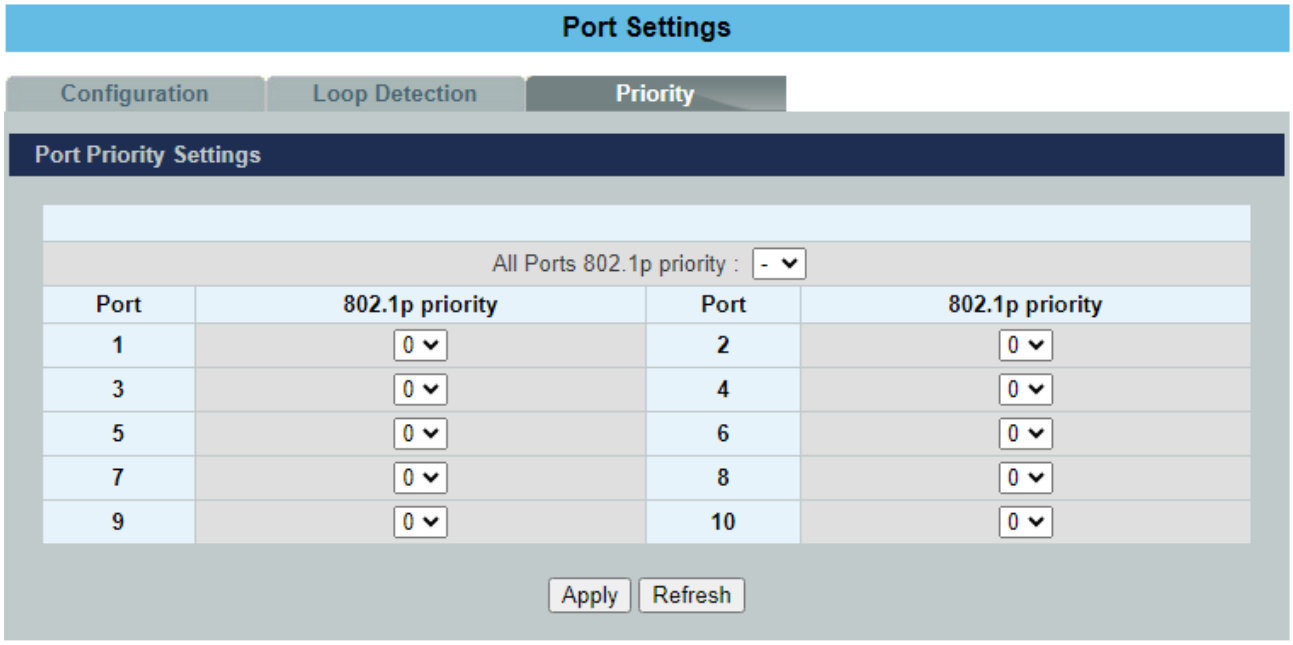
Loop detection is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. (e.g.: two ports on a switch are connected with the same cable.)



Item	Description
Loop Detection Settings	
State	User can configure loop-detection state enable/disable globally by default it is disabled.
MAC Address	Enter the **destination** MAC address the probe packets will be sent to. 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 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.
Loop Detection 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.

4.3.3 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 in a timely manner. Using Port Priority feature, you can select specific network traffic, and prioritize it according to its relative importance.



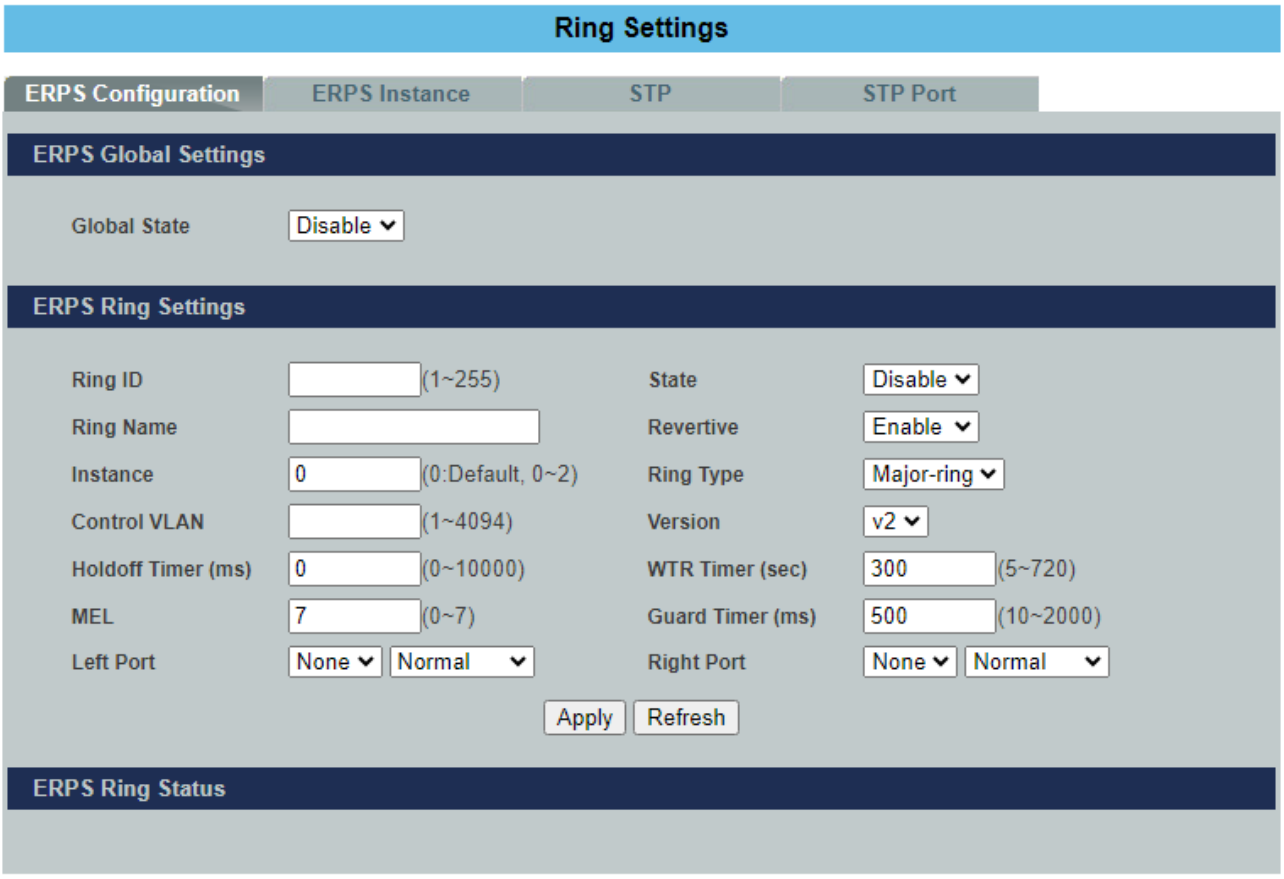
Item	Description
Port Priority Settings	
Port	Selects a port or a range of ports on which to configure the priority.
Priority	Select a priority for packets received by the port. Only packets without 802.1p priority tagged will be applied the priority you set here.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

4.4 Ring Settings

This section allows you to setup ERPS configuration, ERPS instance, STP and STP port.

4.4.1 ERPS Configuration

Ethernet Ring Protection (ERP) protocol, defined in ITU-T G.8032, to provide protection for 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.



Item	Description
ERPS Global Settings	
Global State	Enables / disables the global ERPS state.
ERPS Ring Settings	
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 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 Ring 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 type.
Right Port	The right port.

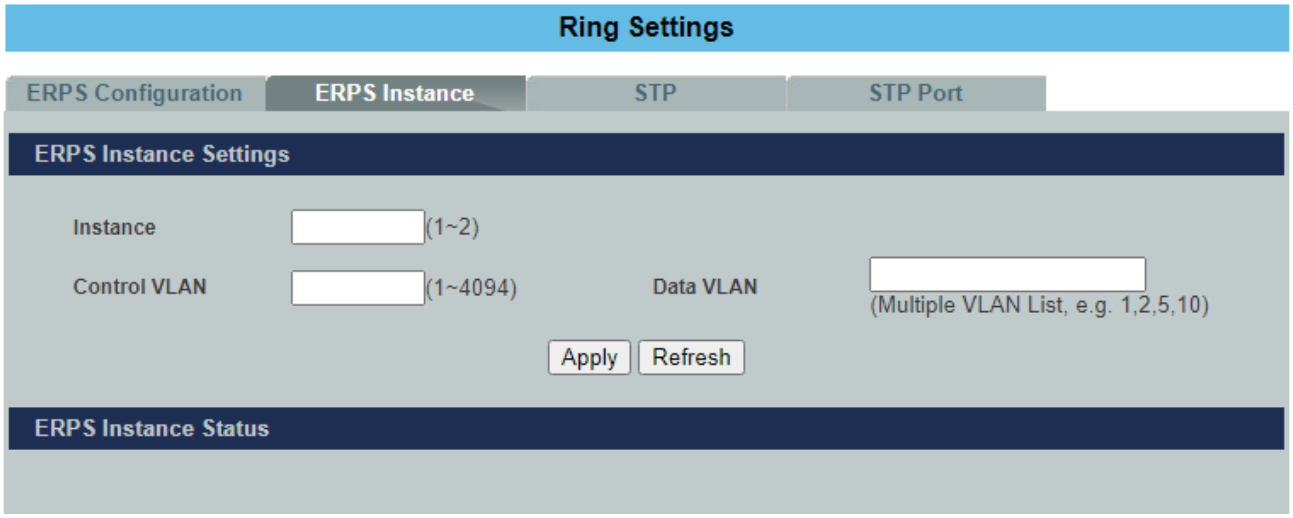
Right Port Type	The right port type.
WTB Timer	The WTB time.
Ring Status	The current ring status.
Left Port Status	The current left port status.
Right Port Status	The current right port status.

4.4.2 ERPS Instance

For ERPS version 2, the instance is a profile specifies a control vlan and a data vlan or multiple data vlans for the ERPS.

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 belong to the vlans in the instance are blocked.

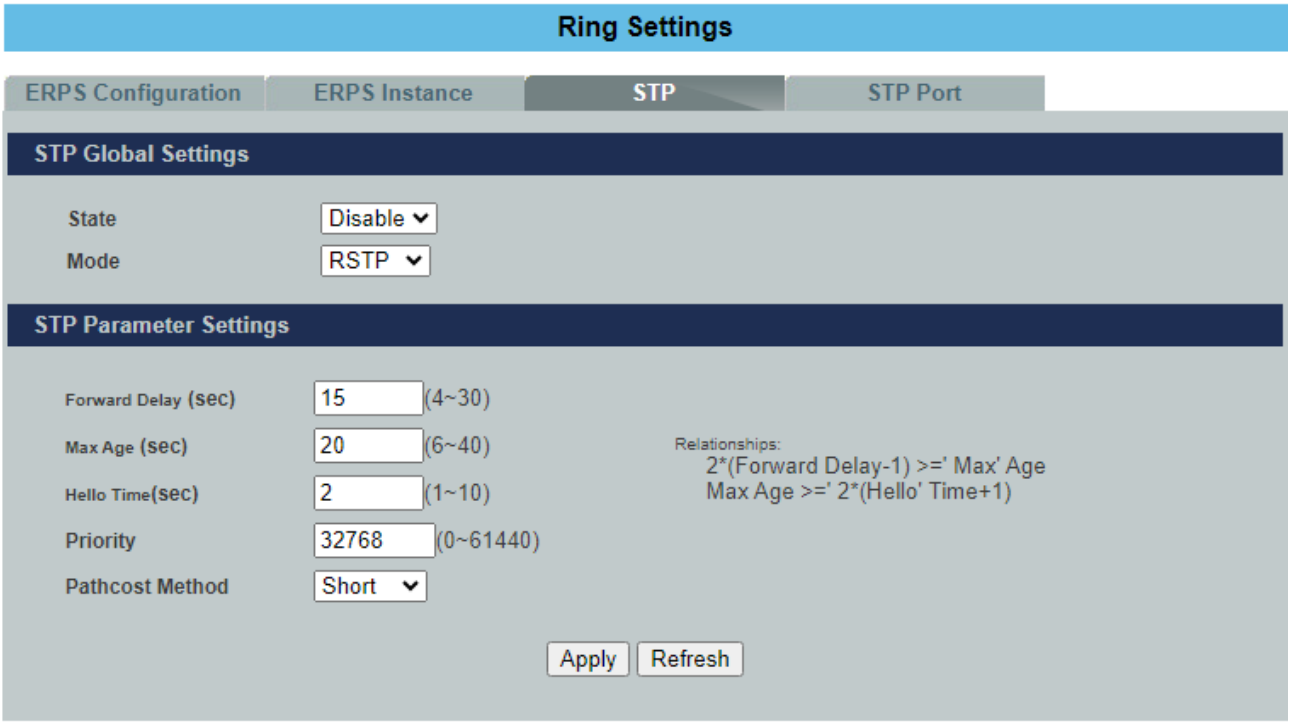


Item	Description
ERPS Instance Settings	
Global State	Enables / disables the global ERPS state.
ERPS Ring Settings	
Instance	Configures the instance ID. The valid value is from 1 to 31.
Control VLAN	Configures the control VLAN for the instance. The valid value is from 1 to 4094.

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

4.4.3 STP

(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.

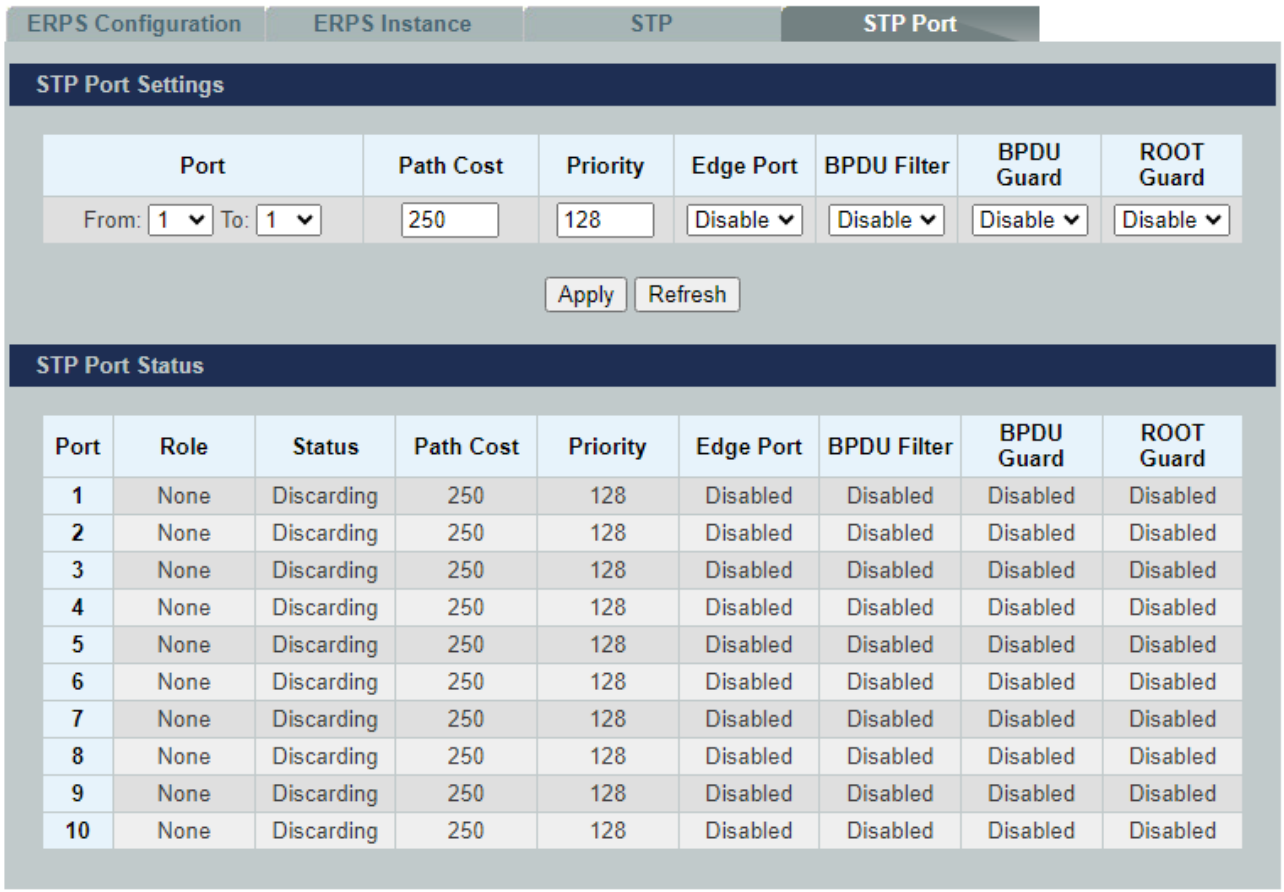


Item	Description
ERPS Instance Settings	
State	Select **Enabled** to use Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).
Mode	Select to use either Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).

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 on to 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.

4.4.4 STP Port

(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.

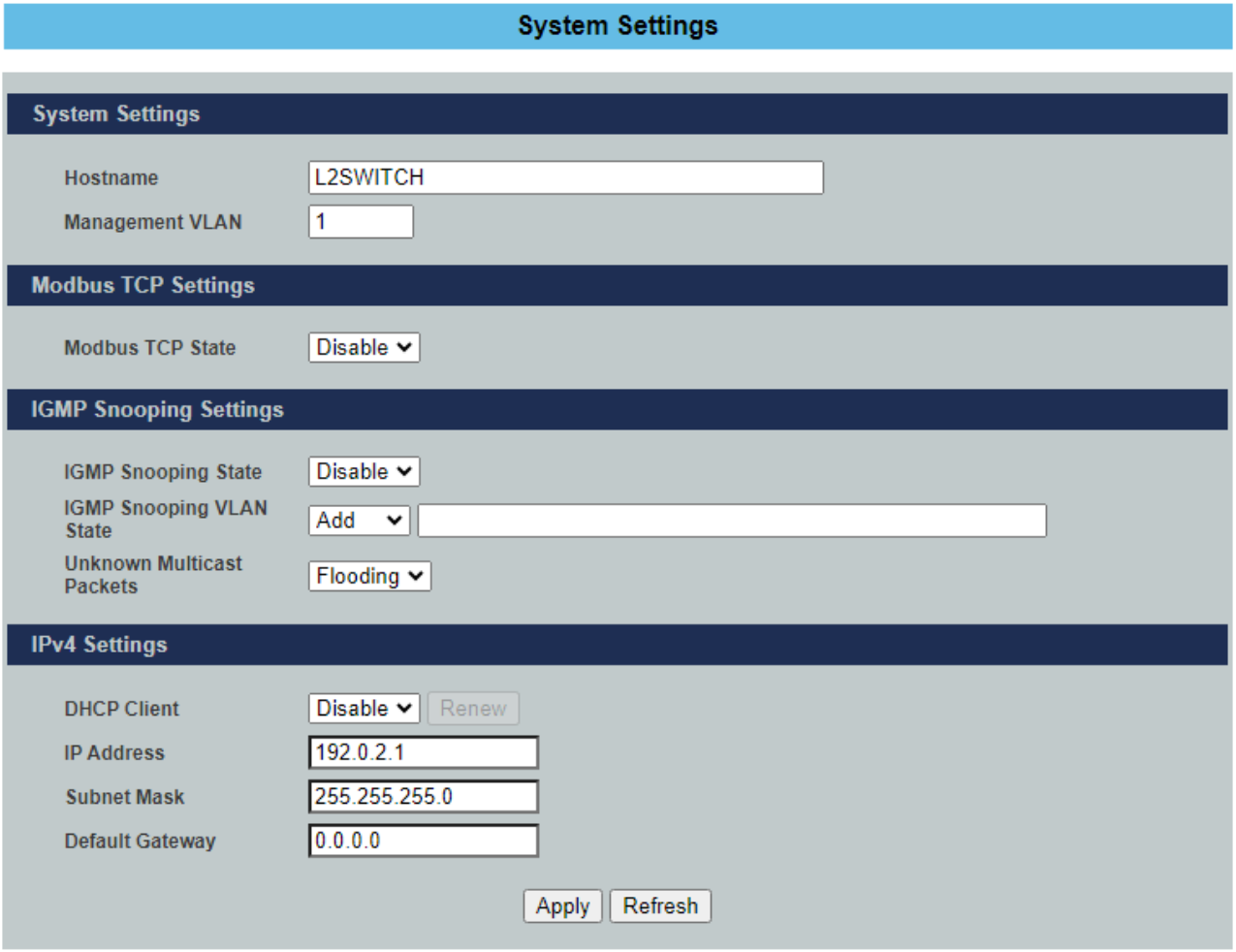


Item	Description
STP Port Settings	
Port	Selects a port that you want to configure.
Active	Enables/Disables the spanning tree function for the specific port.
Path Cost	Configures the path cost for the specific port.
Priority	Configures the priority for the specific port.
Edge Port	Configures the port 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.

4.5 System Settings

This section allows you to setup ERPS configuration, ERPS instance, STP and STP port.



Item	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

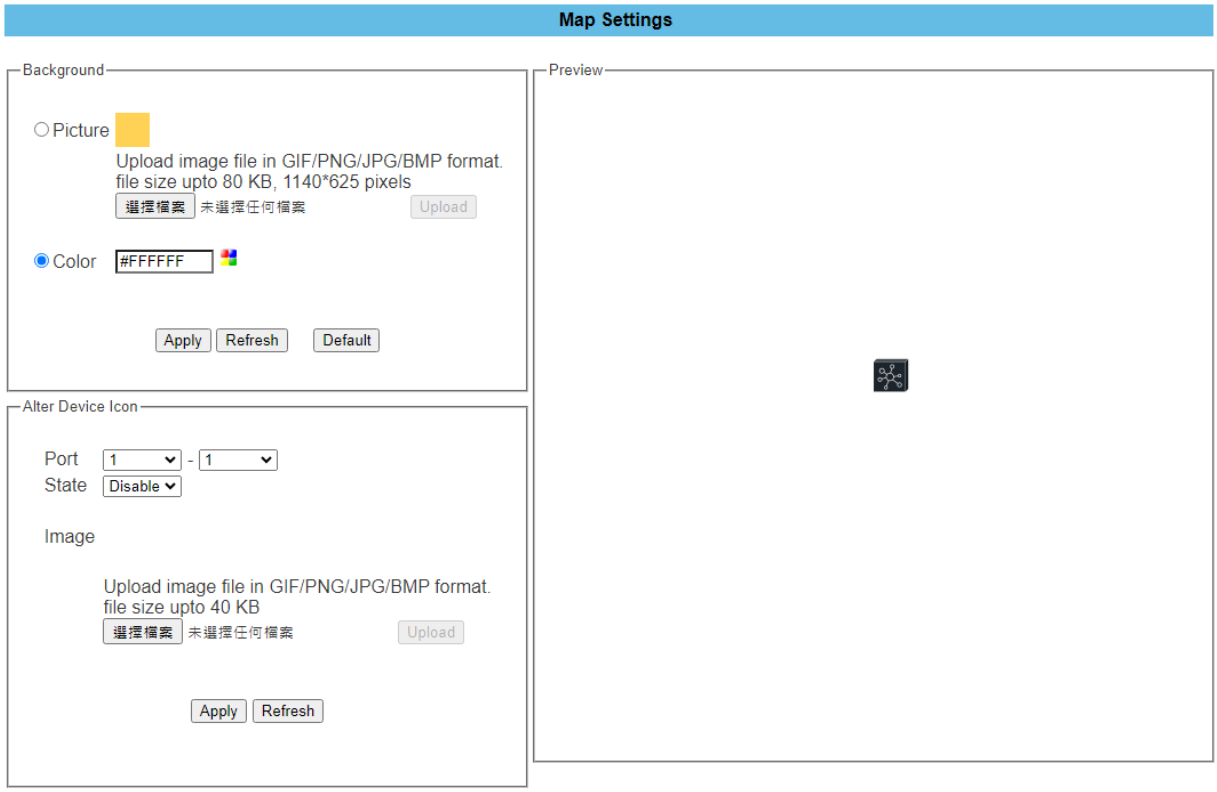
Modbus TCP Status	
Modbus TCP State	Select option to enable / disable the Modbus TCP on the Switch.
IGMP Snooping Settings	
IGMP Snooping State	Select **Enable** to activate IGMP Snooping to forward group multicast traffic only to ports that are members of that group. Select **Disable** to deactivate 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 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.
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

This section allows you to setup map settings, neighbor devices and topology map.

5.1 MAP Settings

This section allows you to preview topology map, change background and replace icon.



Item	Description
Background	
Picture	You can upload your company floor layout plan picture in to the background image so that you can identify easily where the switch has been placed.
Color	Allow user to select standard color for the background and the Preview window will display your select immediately.
Alter Device Icon	
Port	Select port to replace icon.
State	Enable or disable display of uploaded image.
Image	You can upload image to replace the default icon from dashboard.

5.2 Neighbor Devices

This section allows you to setup LLDP, manual registration and ONVIF.

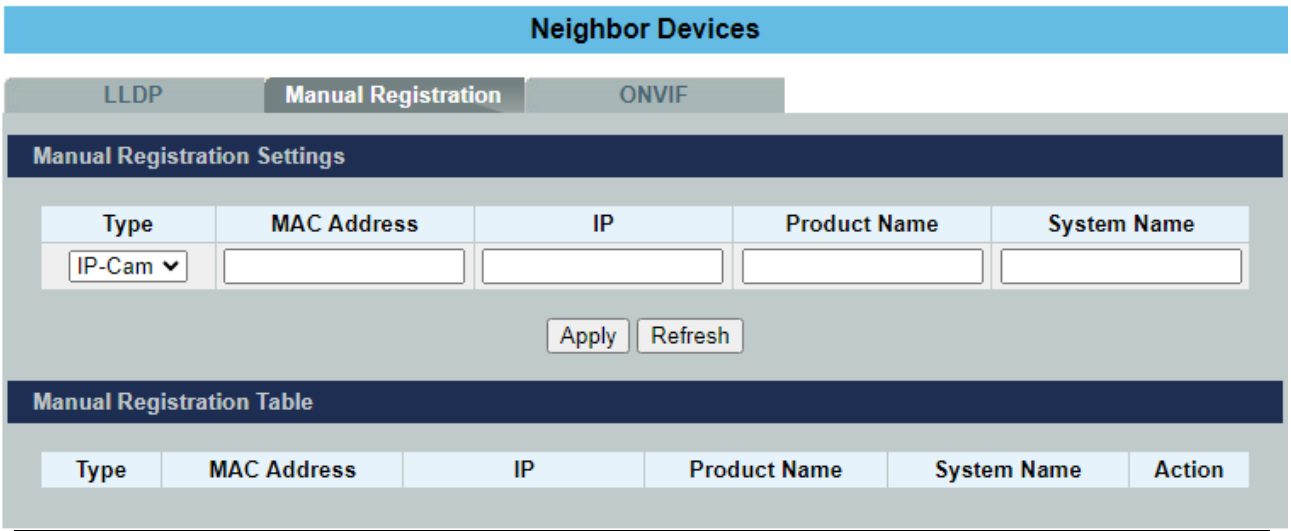
5.2.1 LLDP

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.

Item	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

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

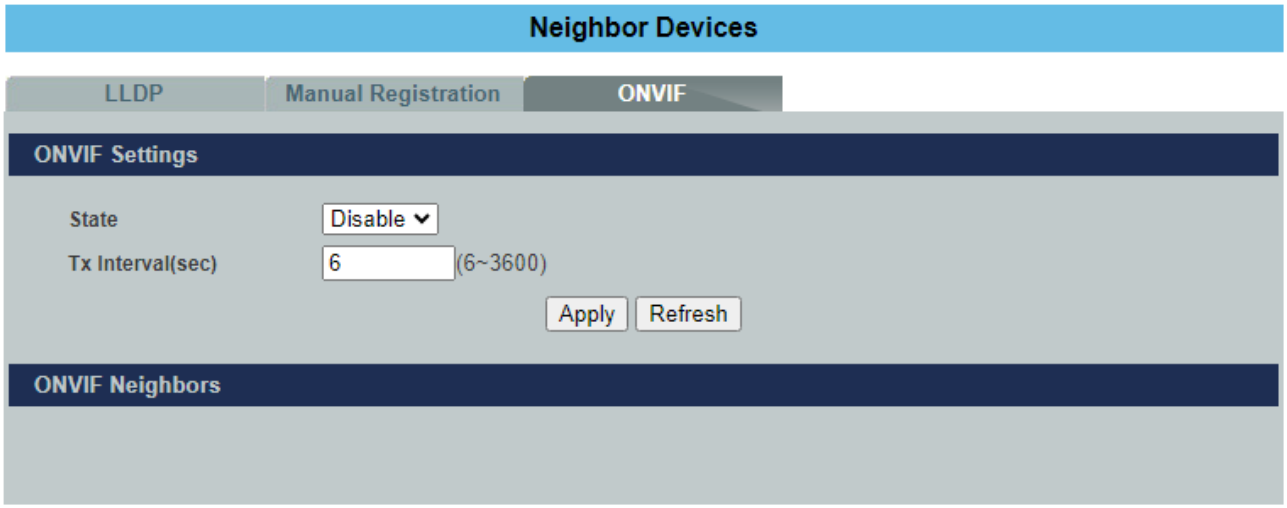


Item	Description

Manual Registration Settings	
Type (IP cam /PLC /Switch /PC)	User can select the type of the device for manual registration like (IP cam /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

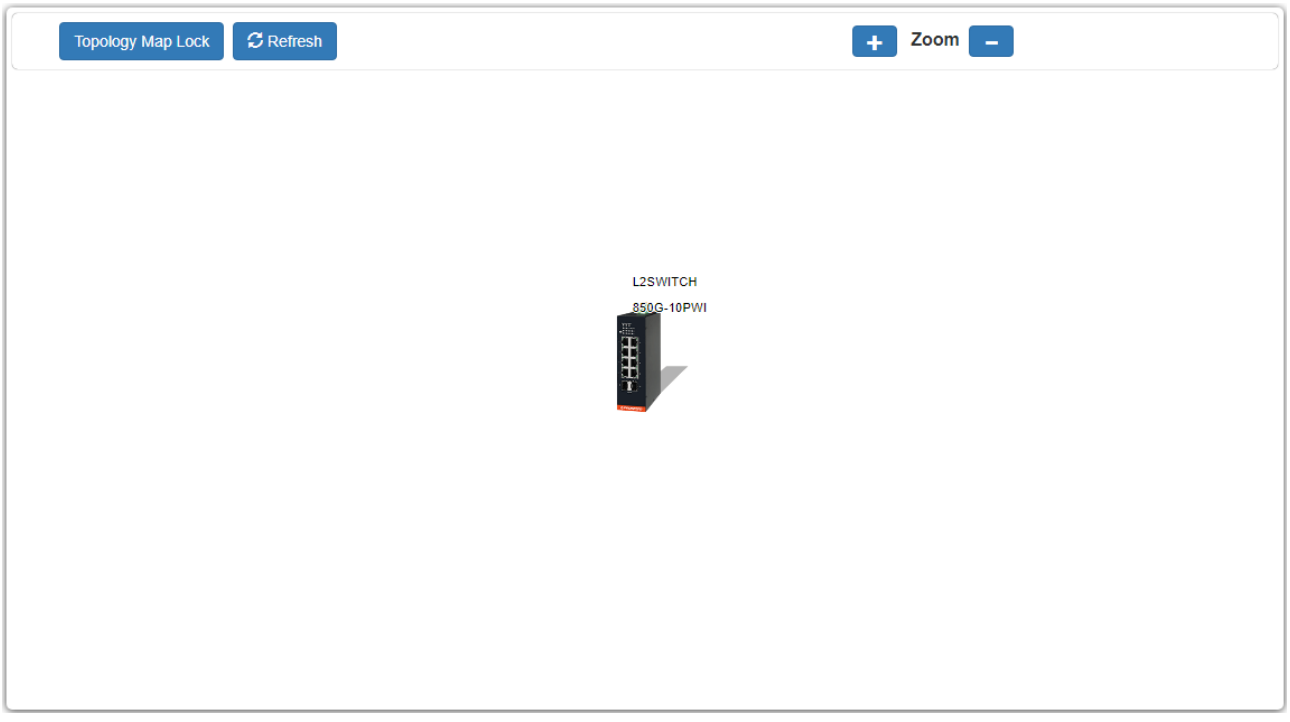
ONVIF is an open industry forum that provides and promotes standardized interfaces for effective interoperability of IP-based physical security products.



Item	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	
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

5.2.4 Topology Map

This section allow you to adjust location of deivce and lock.



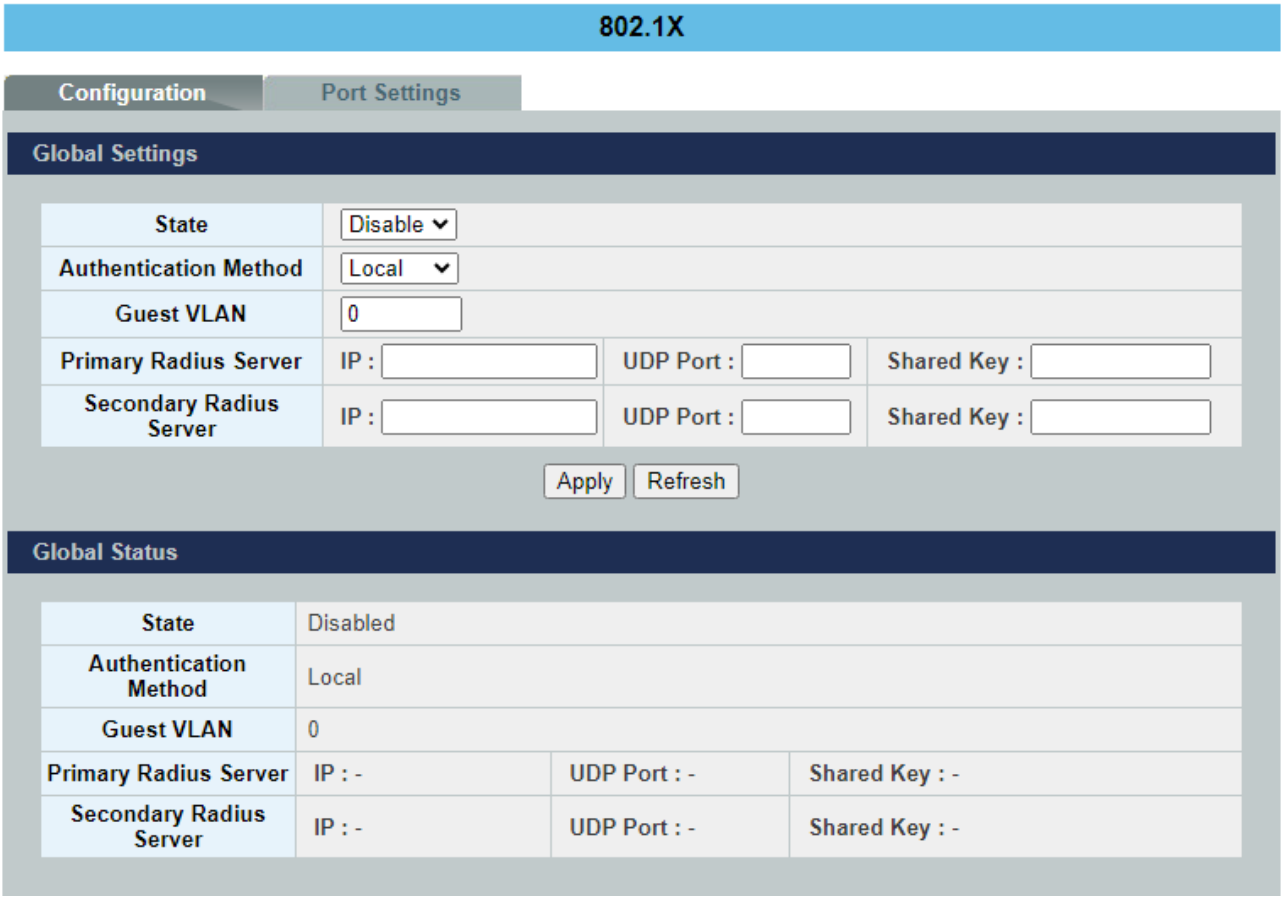
6 Security

This section allows you to setup 802.1X, ACL, port security, server control, storm control, VLAN.

6.1 802.1X

6.1.1 Configuration

802.1X provides port-based authentication, which involves communications between a supplicant, authenticator, and authentication server.

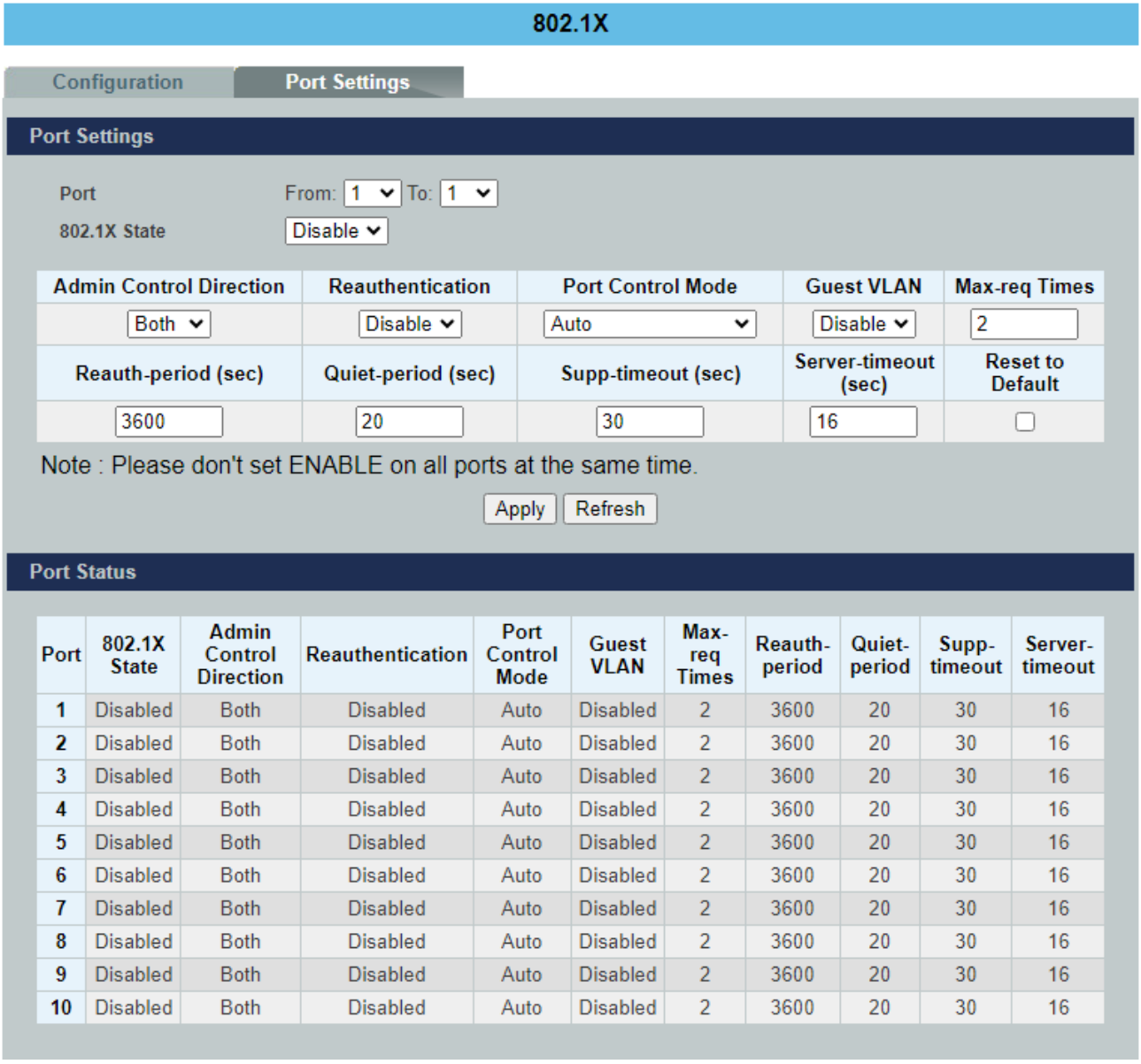


Item	Description
Global Settings	
State	Select **Enable** to permit 802.1 x authentications on the Switch. Note: You must first enable 802.1 x authentications on the Switch before configuring it on each port.
Authentication Method	Select whether to use **Local** or **RADIUS** as the authentication method. 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.

6.1.2 Port Settings

This section allows setup 802.1x port including authentication method, guest VLAN, primary radius server, secondary radius server.



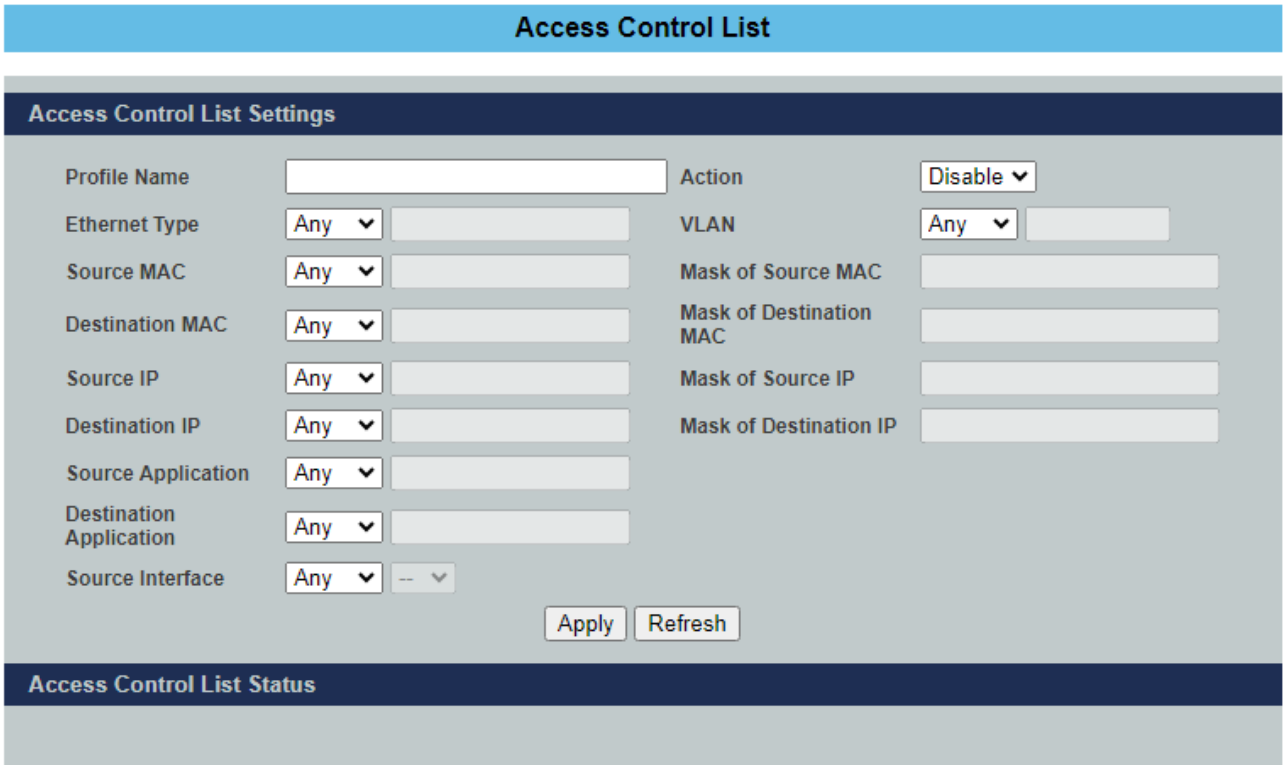
Item	Description
Port Settings	
Port	Select a port number to configure.
802.1x State	Select **Enable** to permit 802.1 x authentications on the port. You must first enable 802.1 x authentications on the Switch before configuring it on each port.
Admin Control Direction	Select **Both** to drop incoming 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 has to periodically re-enter his or her user name 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 amount 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 has to 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 has to 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 amount 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 has to 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 has to 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

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.

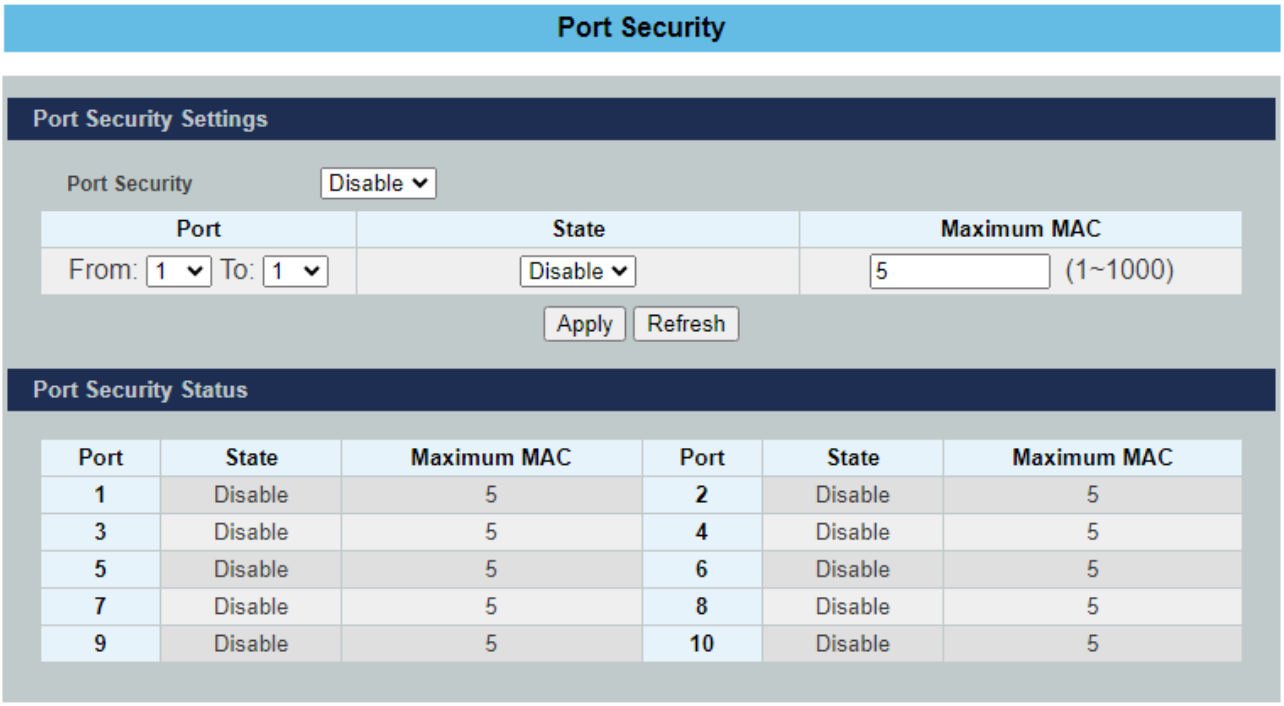


Item	Description
Profile Name	The access control profile name.
State	Selects Disables / Drop / Permits/ DSCP action for the profile.
Ethernet Type	Configures the Ethernet type of the packets that you want to filter.
VLAN	Configures the VLAN of the packets that you want to filter.
Source MAC	Configures 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

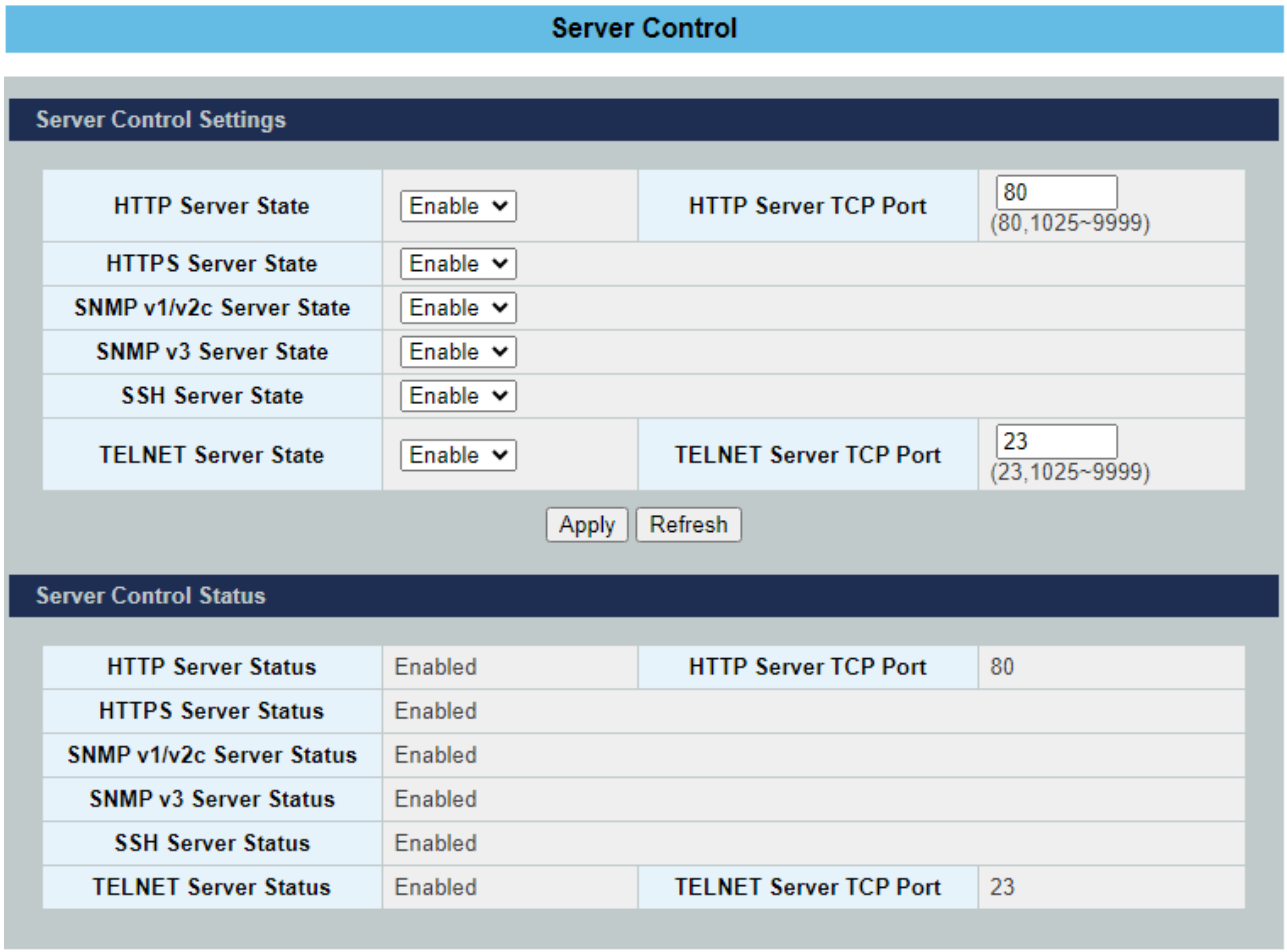
Port security can set maximum number of MAC addresses allowed per interface. When the limit is exceeded, incoming packets with new MAC addresses are dropped.



Item	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

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

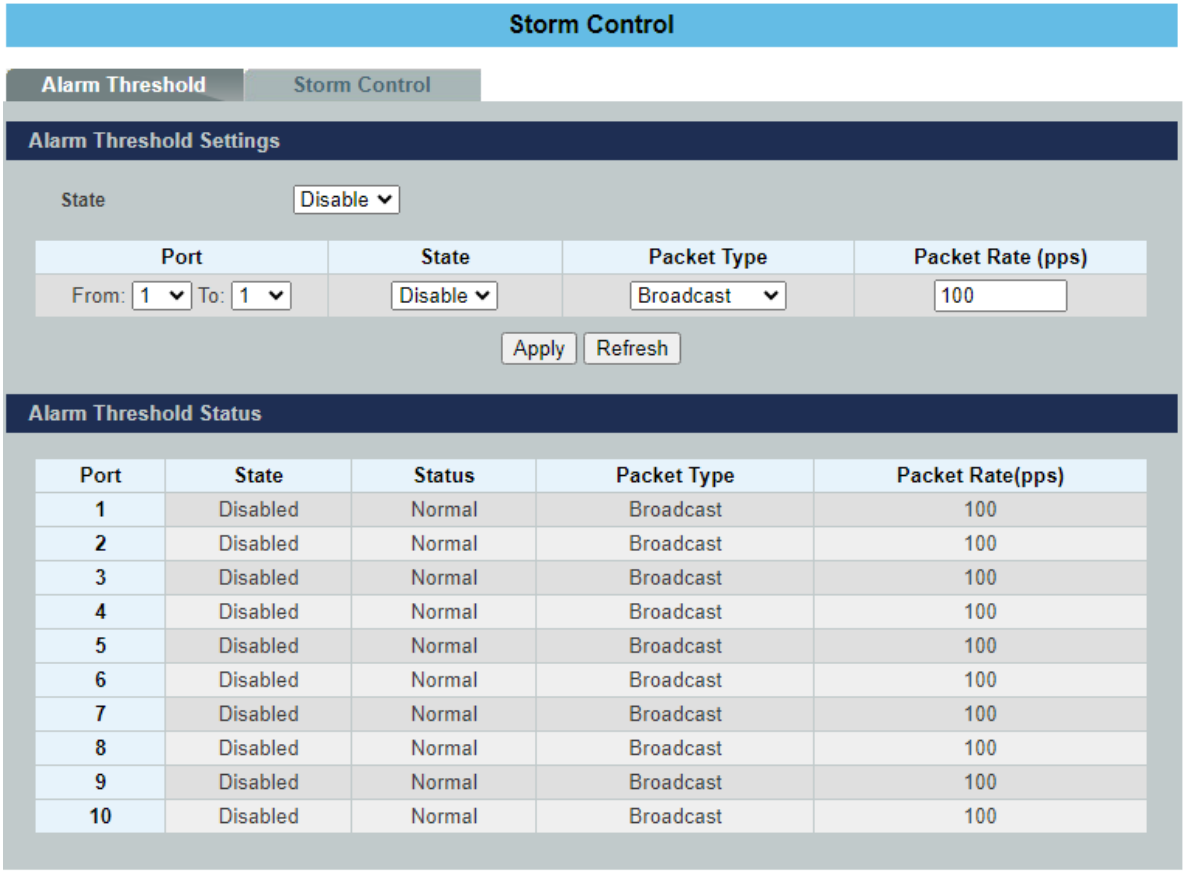


Item	Description
Server Control Settings	
HTTP Server State	Selects Enable or Disable to enable or disable the HTTP service.
HTTPS Server State	Selects Enable or Disable to enable or disable the HTTPS service.
SNMPv1/v2c Server State	Selects Enable or Disable to enable or disable the SNMPv1/v2c service.
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 Control 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

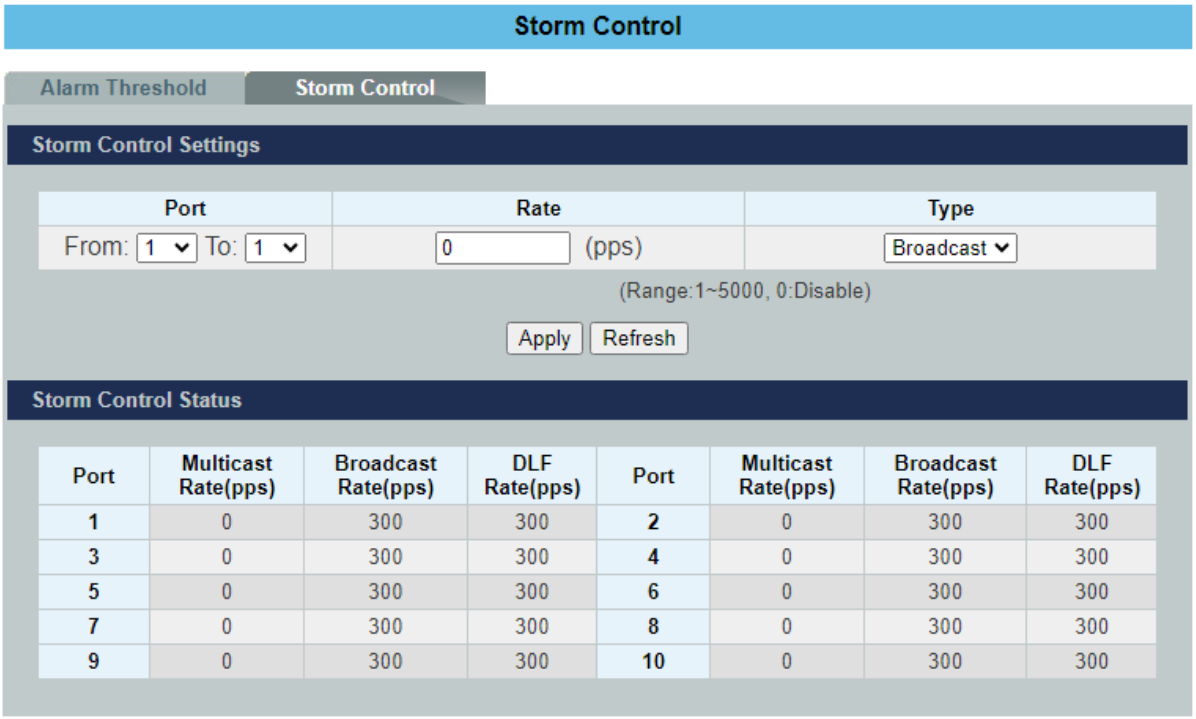
When the selected packet rate is over the alarm threshold, the Switch will send syslog alarm to syslog server.



Item	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	
State	Display the current state
Status	Display the current status
State	Display the current packet type
Packet Type	Display the current packet type
Packet Rate	Display the current packet rate

6.5.2 Storm Control

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

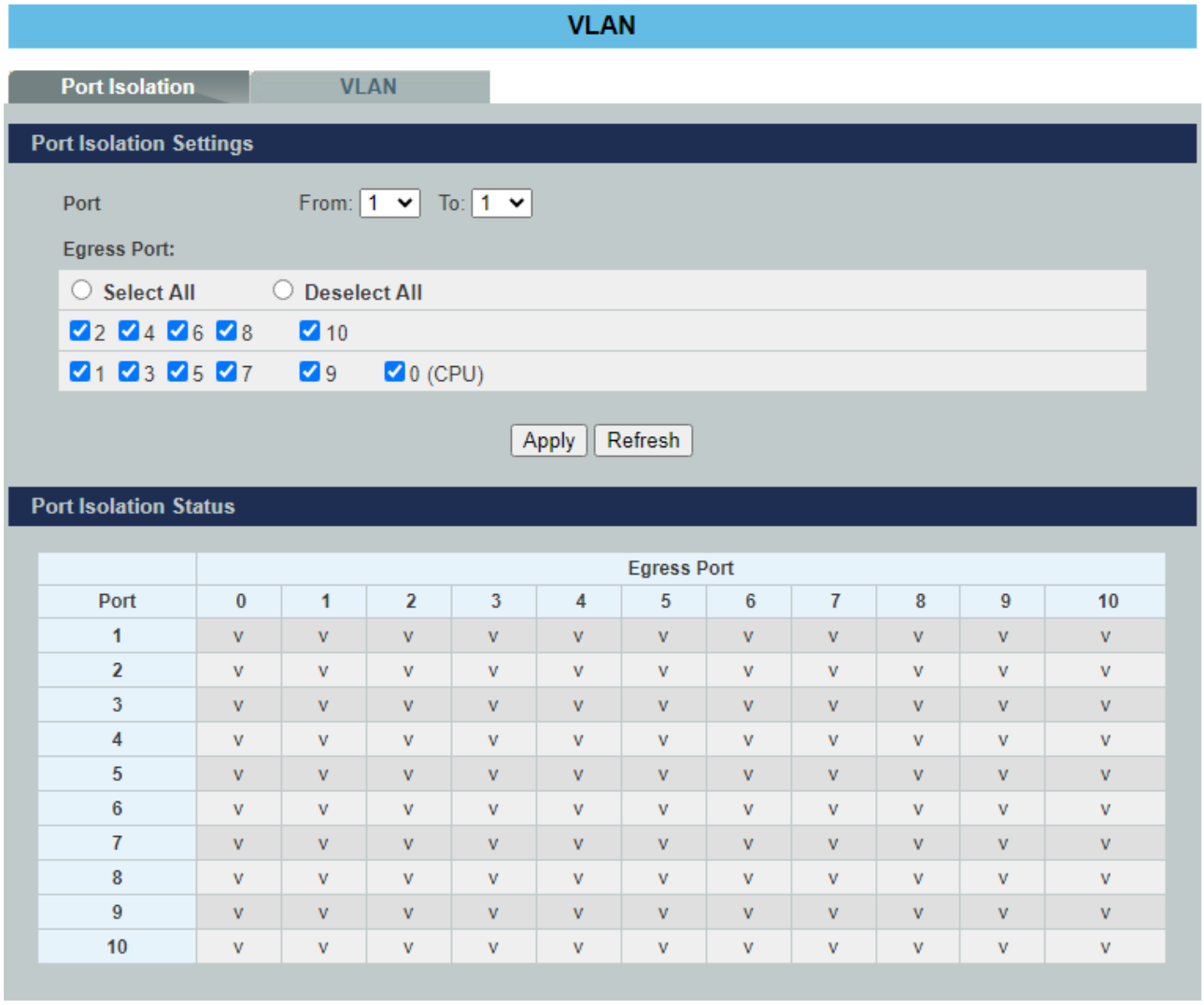


Item	Description
Storm Control Settings	
Port	Select individual port number or range for which you want to configure storm control settings.
Rate	Configure the packet rate in pps to allow on interfaces. Disable for 0 and ranges 1 ~ 5000. .
Type	Click the check box to select Multicast / Broadcast / DLF 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.

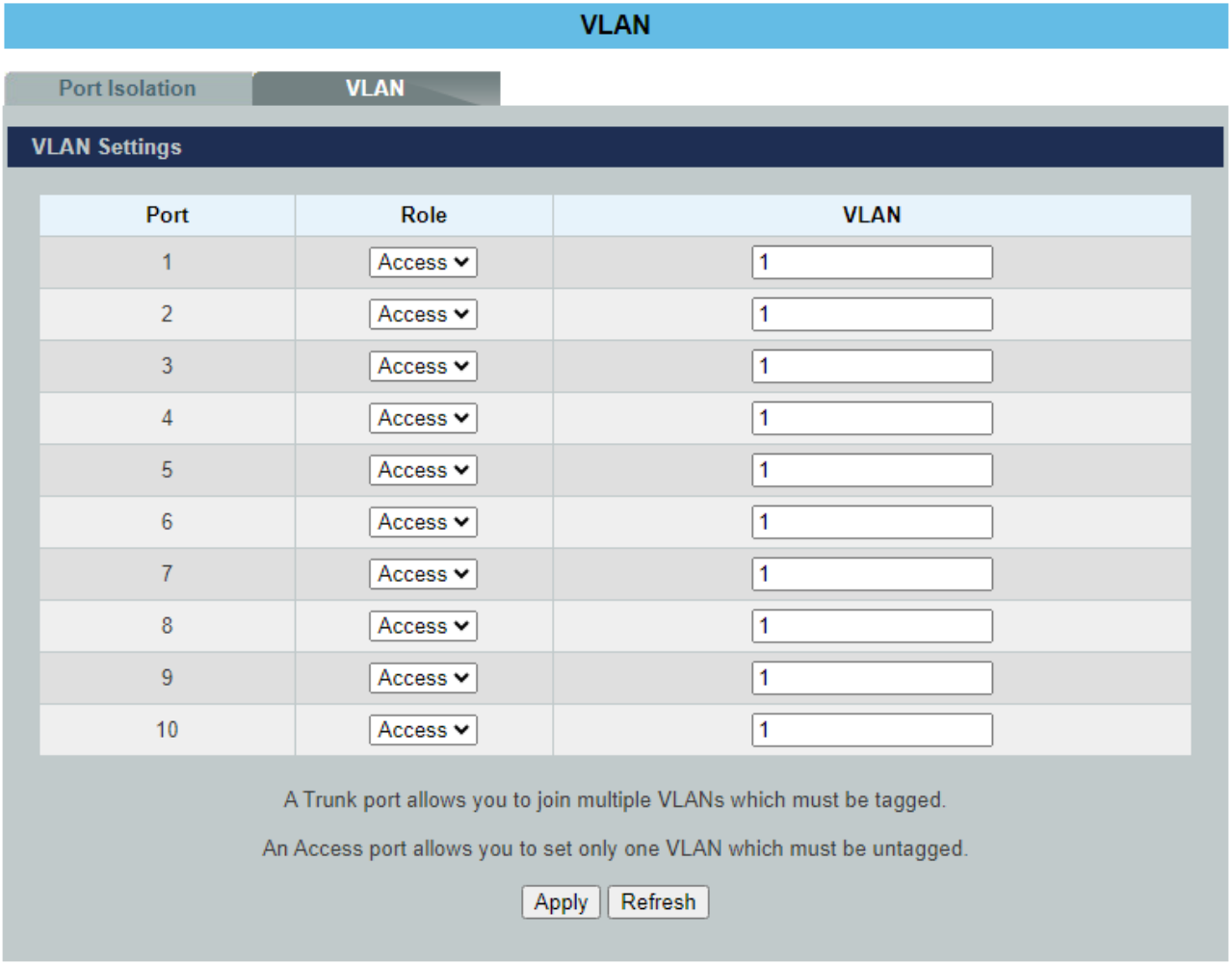


Item	Description
Port Isolation Settings	
Port	Select a port number to configure its port isolation settings. Select **All Ports** to configure the port isolation settings for all ports on the Switch.
Egress Port	An egress port is an outgoing port, that is, a port through which a data packet leaves.

	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

This section allows you to setup VLAN of every port play as access/truck mode.



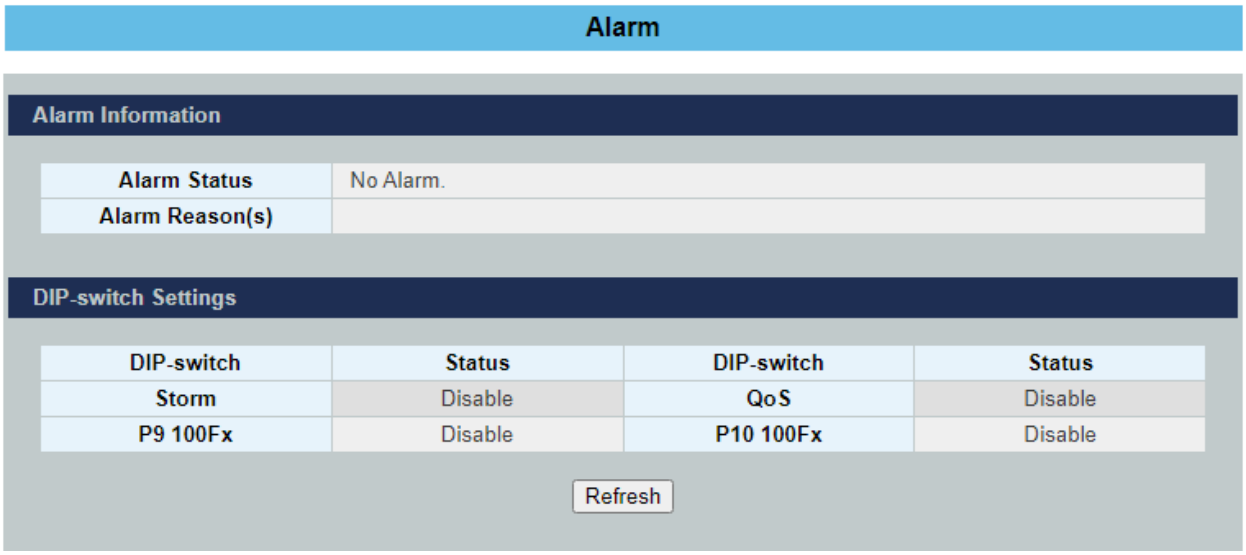
Item	Description
VLAN Settings	
Port	Select a port number to configure from the drop-down box. Select **All** to configure all ports at the same time.
Role	Select role on interface as access or trunk.
VLAN	User can configure maximum of 5 VLAN's on each interface in the format 1,3,7,10,25
Apply	Click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

7 Diagnostic

This section allows you to diagnose by alarm, port mirroring, port statistics, port utilization, syslog, utilization threshold.

7.1 Alarm

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

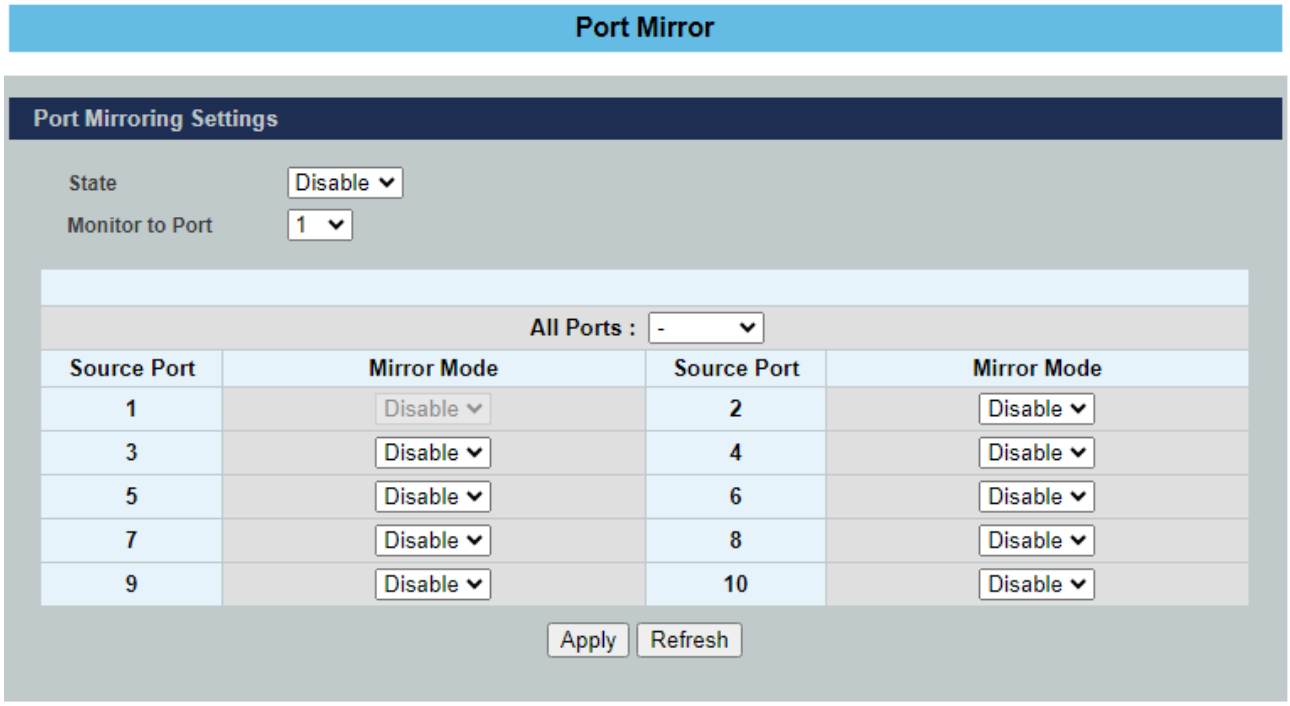


Item	Description
Alarm Information	
Alarm Status	This field indicates if there is any alarm events.
Alarm Reason(s)	This field displays all the detail alarm events.
Function DIP Switch Settings:	
Storm	The field display the current Storm Control DIP settings. Disable – Storm Control controlled by user 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 Mirroring

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).

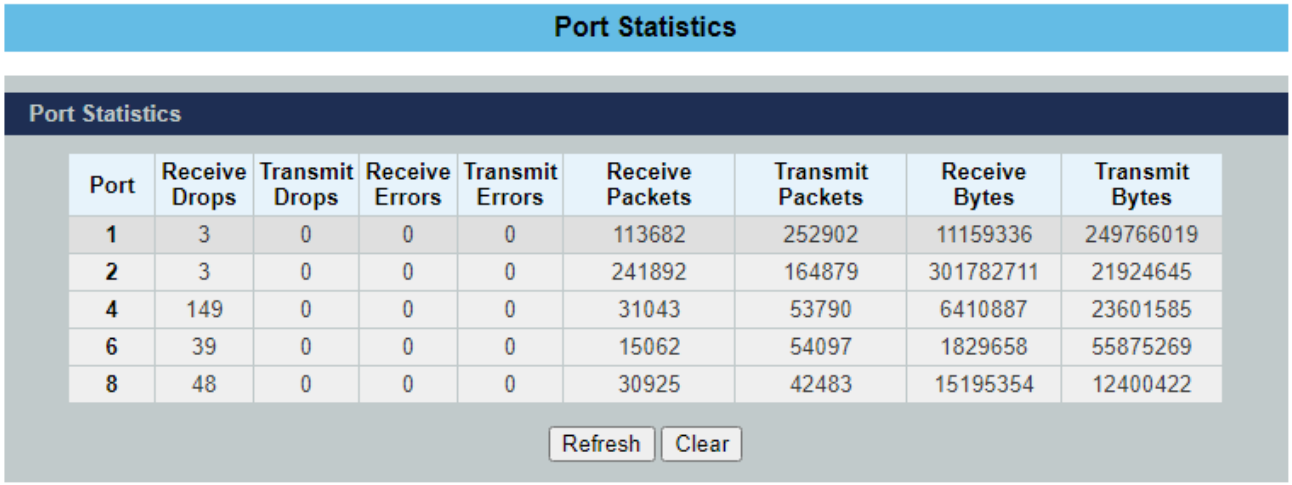


Item	Description
Port Mirror Settings	
State	Select option to enable / disable the port mirroring feature on the Switch globally.
Monitor to Port	Select the port which connects to a network traffic analyzer.
All Ports	Settings in this field apply to all ports. Use this field only if you want to make 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

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

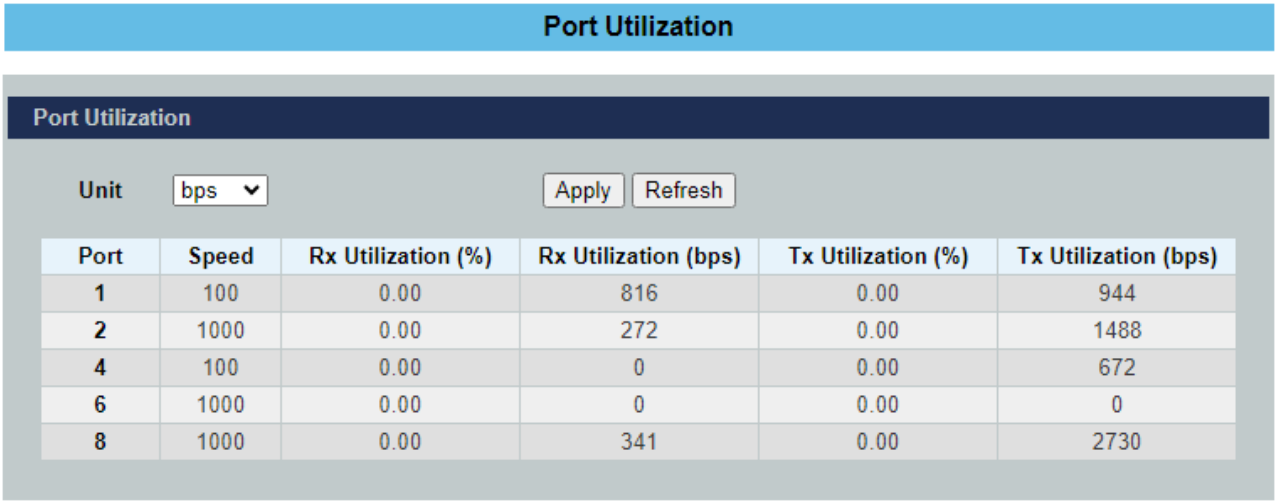


Item	Description
Port Statistics	
Port	Select a port or a range of ports to display their statistics.
Rx Packets	The field displays the received packet count.
Tx Packets	The field displays the transmitted packet count.
Rx Bytes	The field displays the received byte count.
Tx Bytes	The field displays the 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

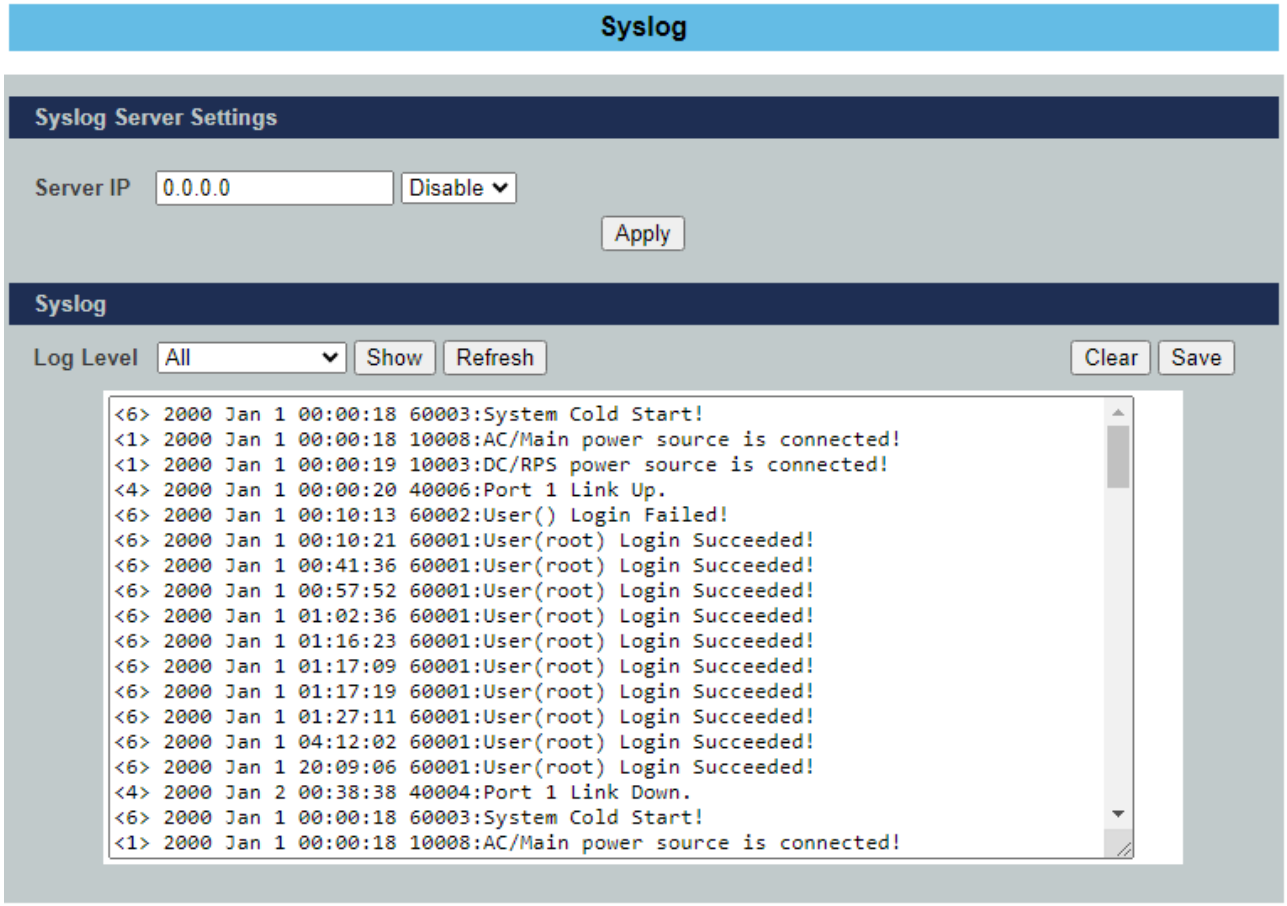
This feature helps users to monitor the ports' traffic utilization, to display the link up ports' traffic utilization only.



Item	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

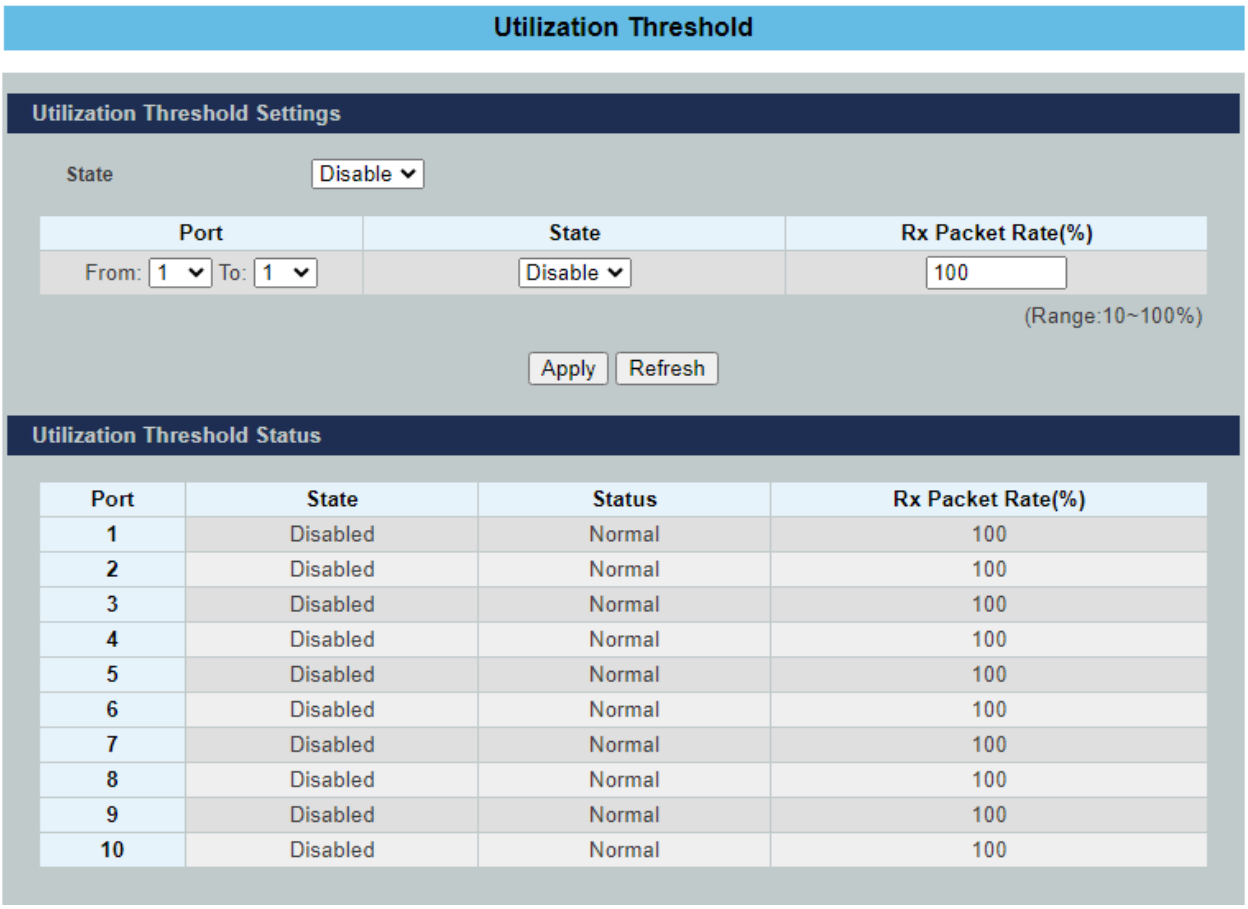
The syslog function records some of system information for debugging purpose.



Item	Description
Port Utilization	
Server IP	1. Enter the Syslog server IP address. 2. 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 Settings

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



Item	Description
Utilization Threshold	
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.
Rx Packet Rate	This field displays the current threshold.

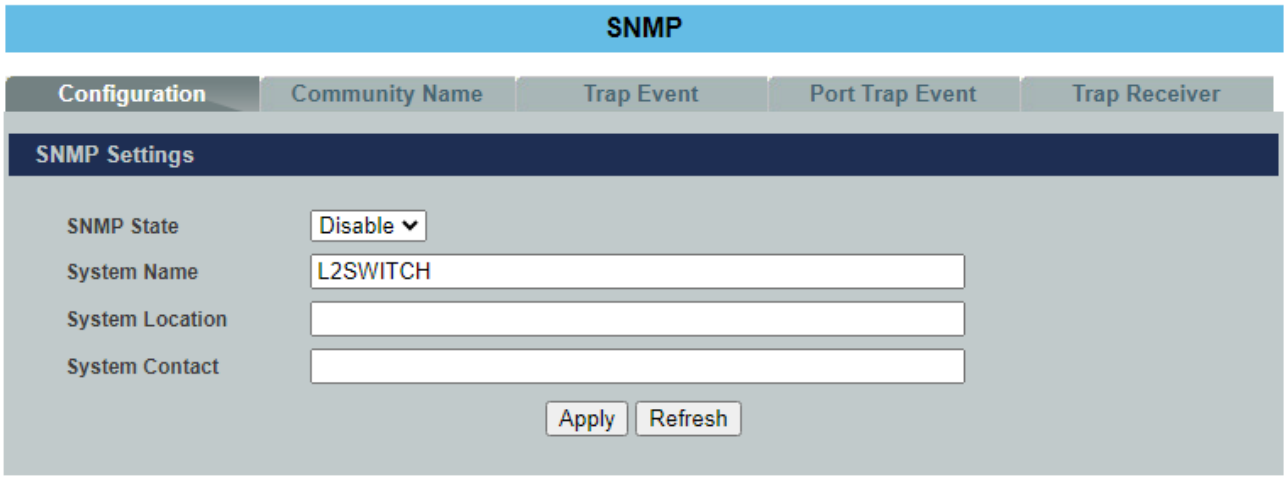
8 Management

This section allows you to setup SNMP, SNMPv3, SNTP, System maintenance, User Account and check system information.

8.1 SNMP

8.1.0 Configuration

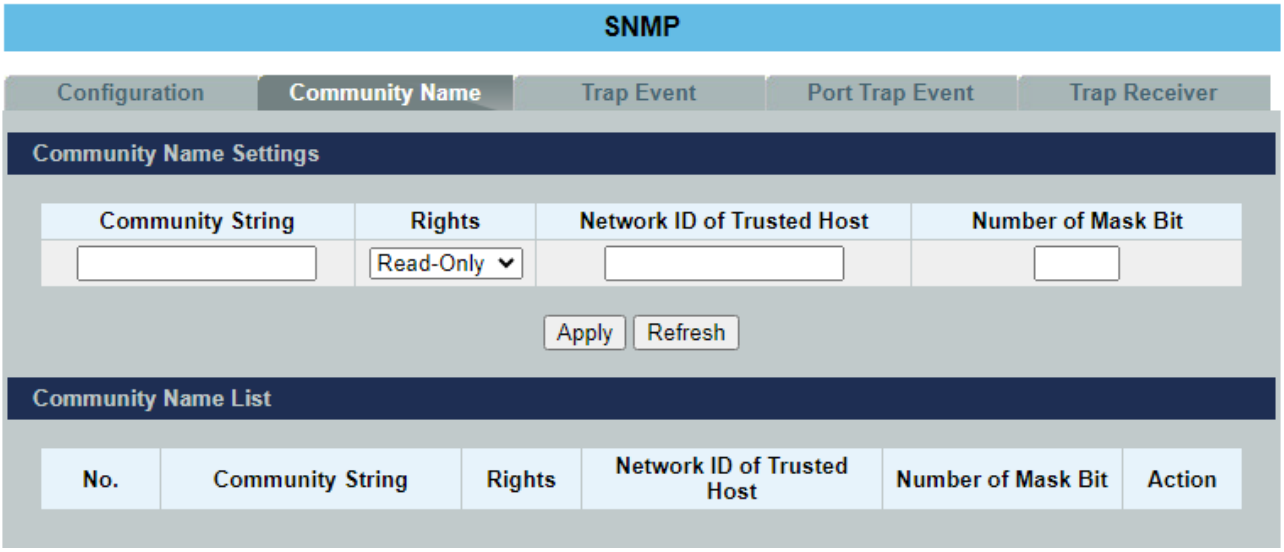
Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.



Item	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

8.1.1 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.

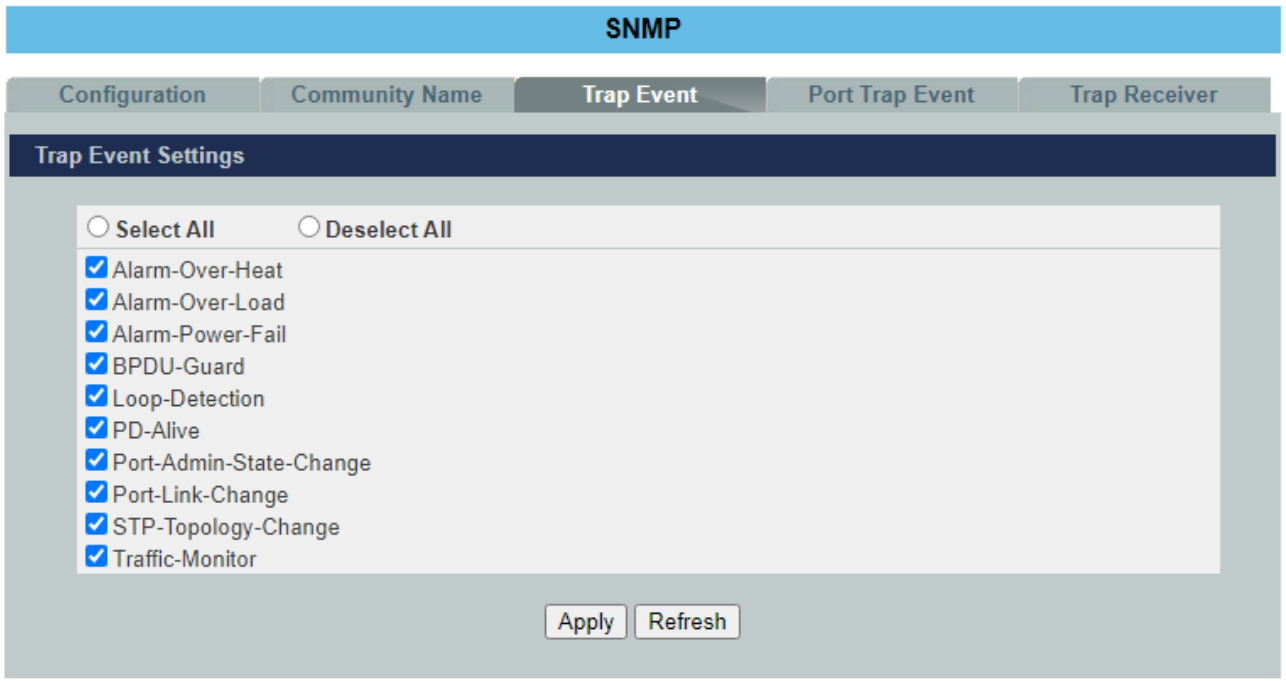


Item	Description
SNMP Settings	
Community String	Enter a community string; this will act as a password for requests from the management station. An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP 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.

8.1.2 Trap Event

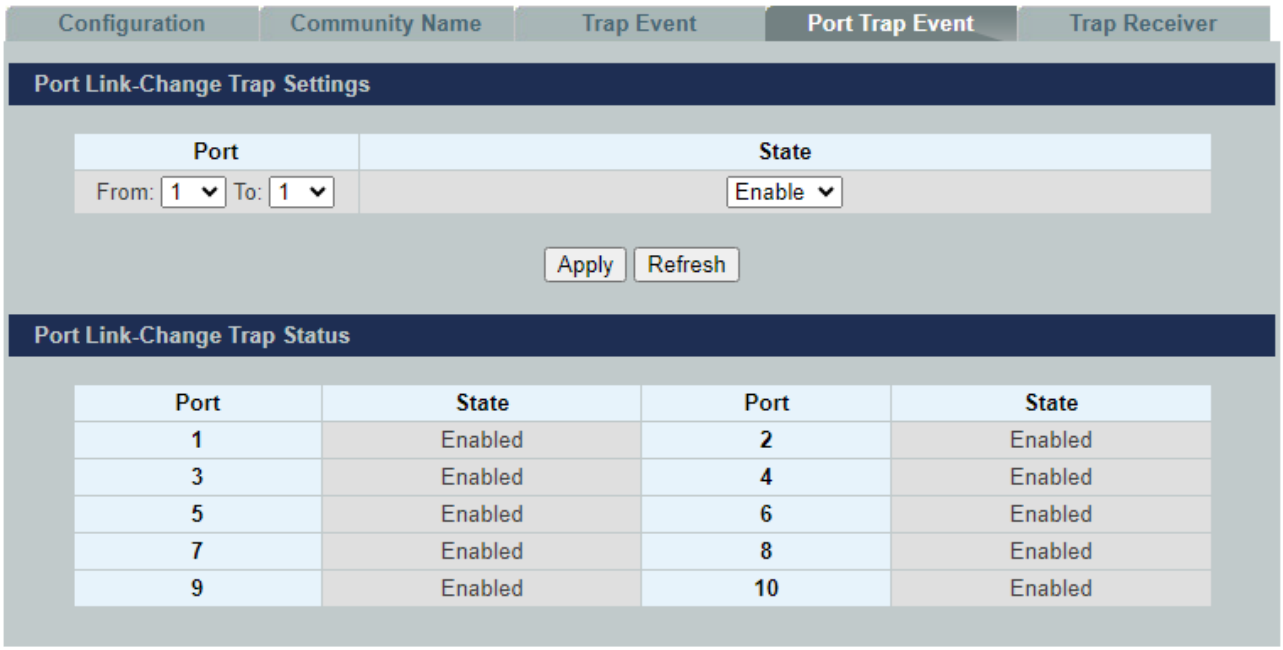
The features allow users to enable/disables individual trap notification.



Item	Description
Trap Event 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.

8.1.3 Port Trap Event

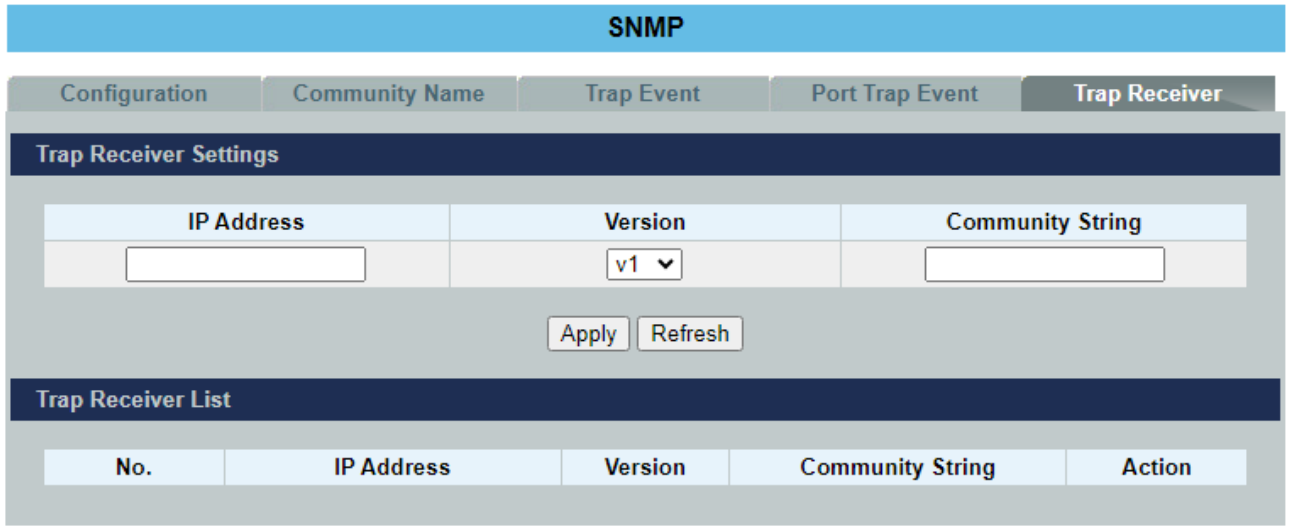
The features allow users to enable/disables port-link-change trap notification by individual port.



Item	Description
Port Link Change Trap 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.

8.1.4 Trap Receiver

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

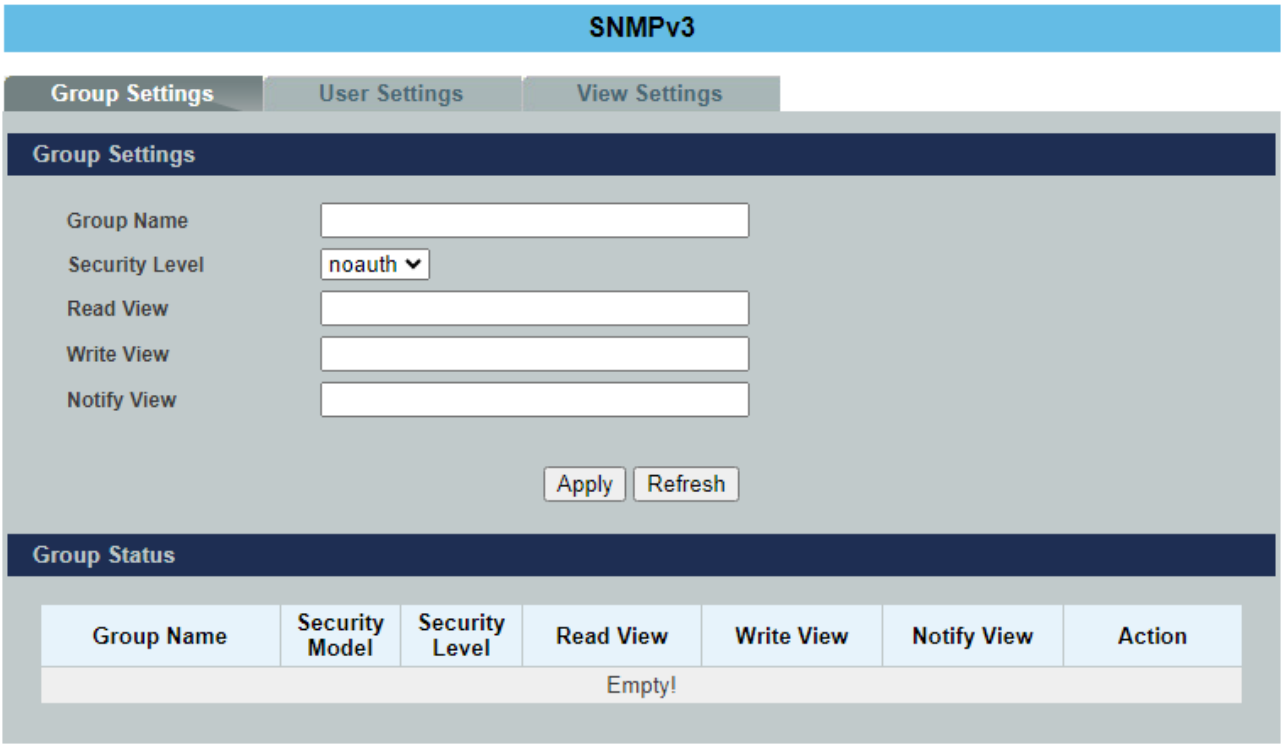


Item	Description
Trap Receiver Settings	
IP Address	Enter the IP address of the remote trap station in dotted decimal notation.
Version	Select the version of the Simple Network Management Protocol to use. **v1**or **v2c**.
Community String	Specify the community string used with this remote trap station.
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.

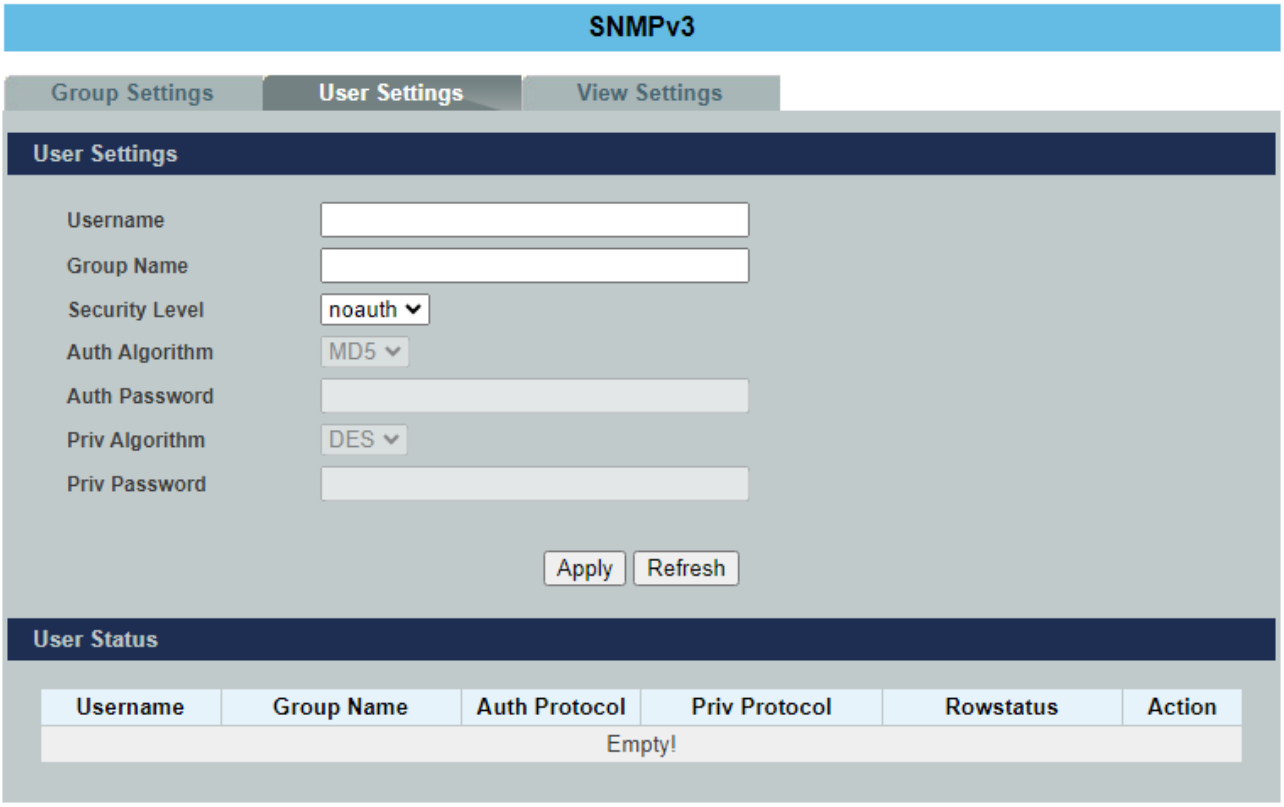
8.2.1 Group Settings



Item	Description
Group Settings	
Group Name	Enter the v3 user name.
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.
Group Status	
Group Name	This field displays the v3 user name.
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 read View list of this group.

Write View	These fields display the write View list of this group.
Notify View	These fields display the notify View list of this group.
Action	Click **Delete** to remove a v3 group.

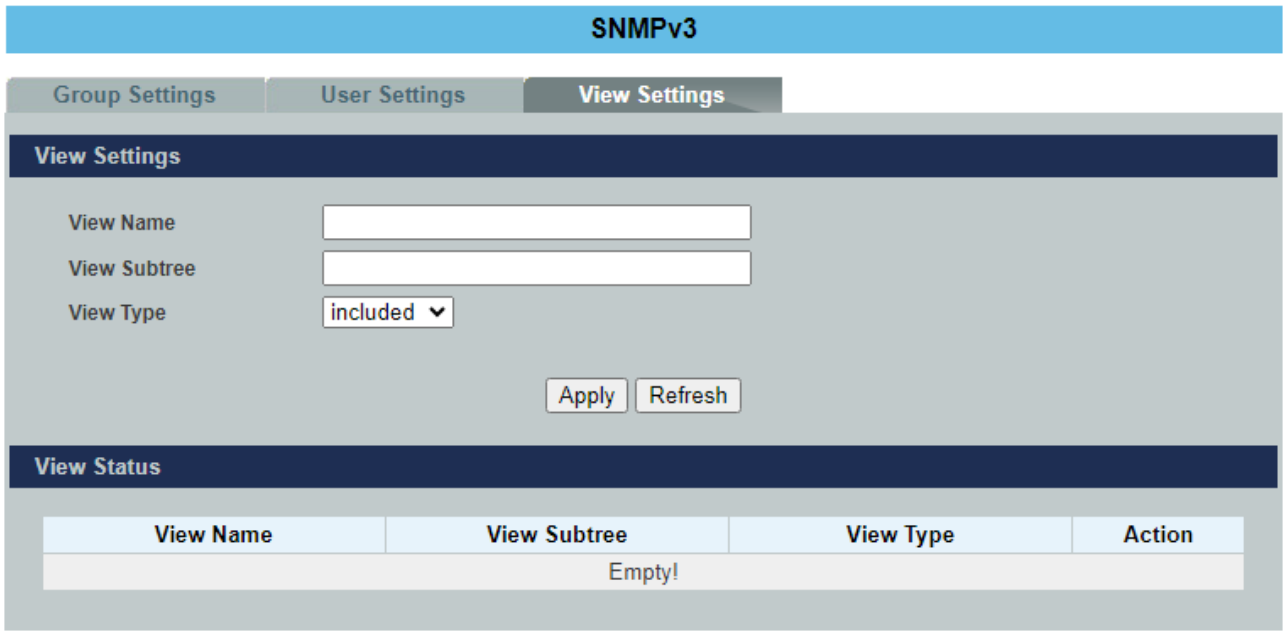
8.2.2 User Settings



Item	Description
User Settings	
User Name	Enter the v3 user name.
Group Name	Map the v3 user name 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.
User Status	
Username	This field displays the v3 user name.
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	These fields display the read View list of this group.
Rowstatus	This field displays the v3 user row status.
Action	Click **Delete** to remove a v3 user.

8.2.3 View Settings

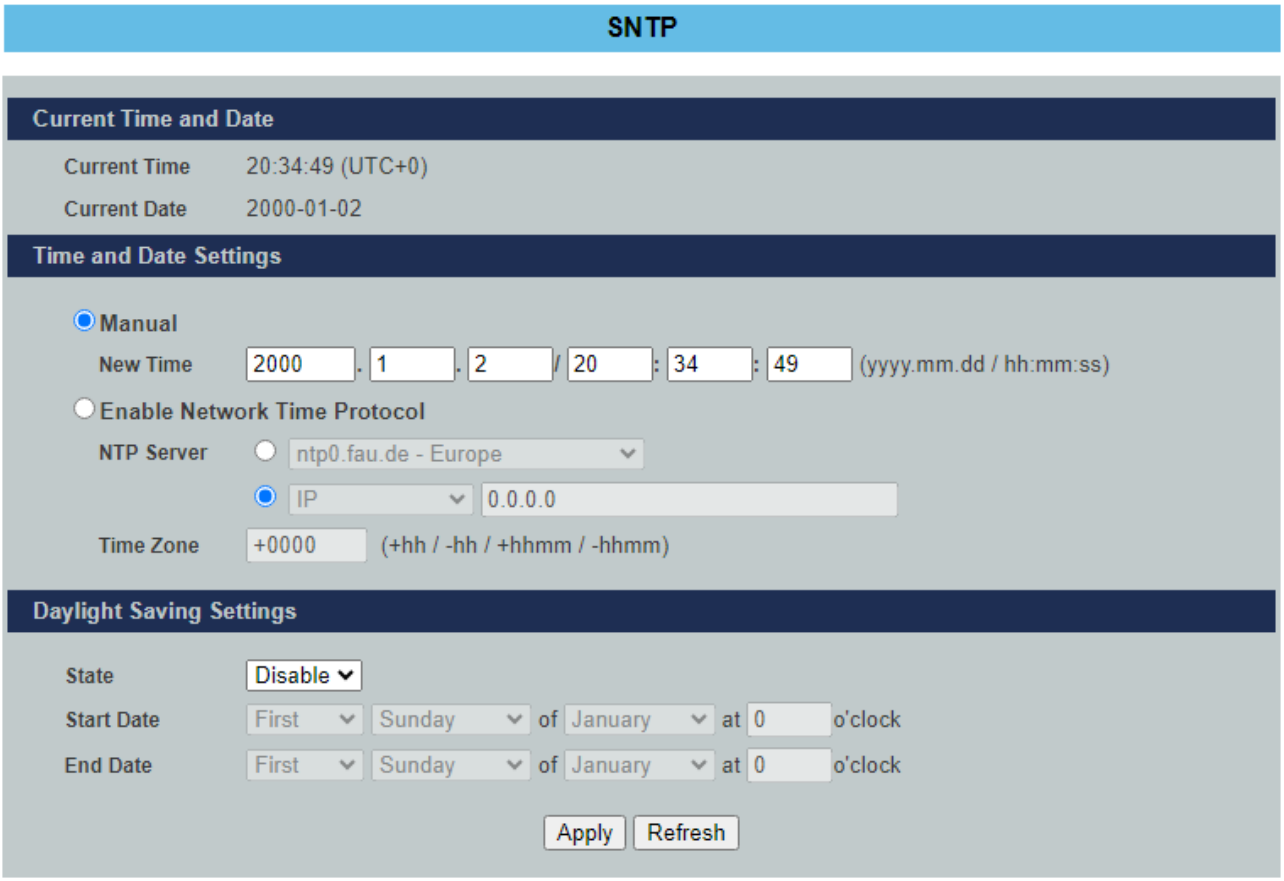


Item	Description
View Settings	
View Name	Enter the v3 view name for creating an entry in the SNMPv3 MIB view table.
View Subtree	The OID defining the root of the subtree to add to (or exclude from) the named view.

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.
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

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.



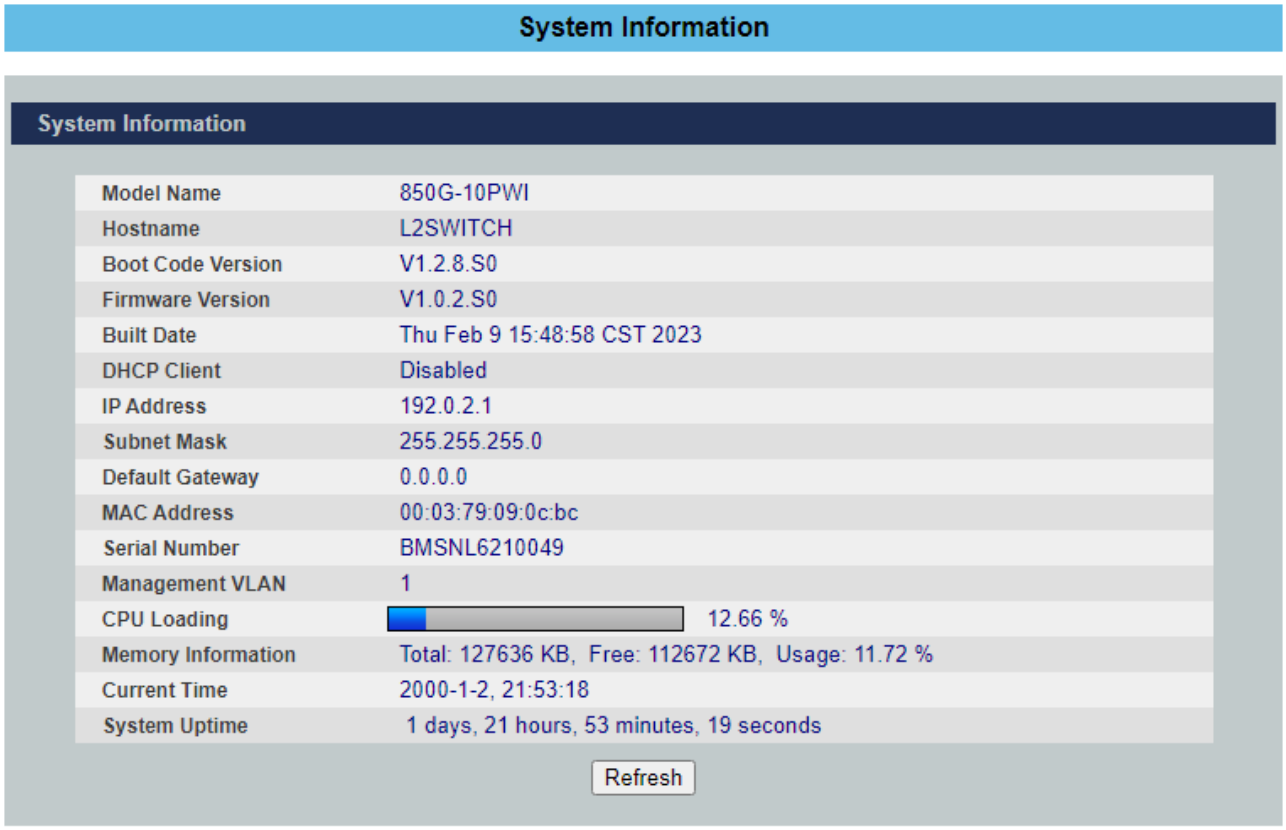
Item	Description
Group Time and Date	
Current Time	This field displays the time you open / refresh this menu.
Current Date	This field displays the date you open / refresh this menu.

Time and Date Settings	
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 of 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 of 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

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



Item	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.

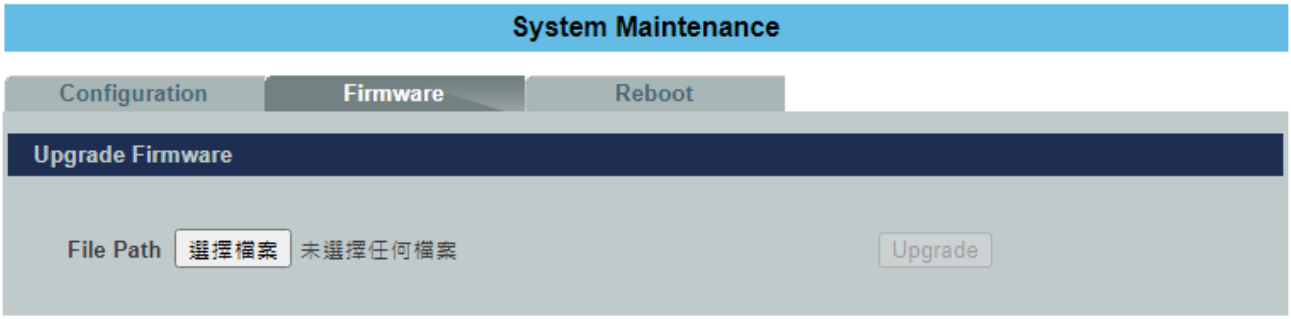
8.5 System Maintenance

This section provides system maintenance including configuration, firmware and reboot.

8.5.1 Configurations

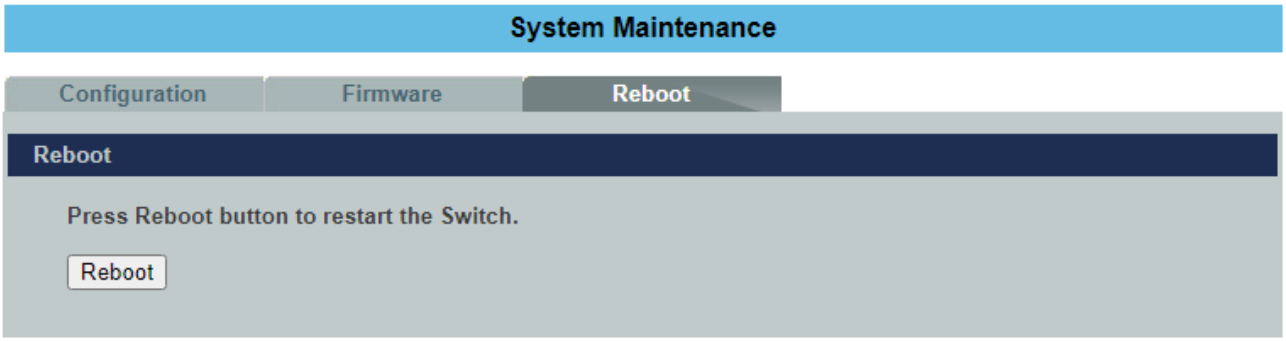
Item	Description
Save Configurations	
Save	Save the parameter settings of the Switch.
Upload and Download Configurations	
Choose File	Select the new configuration file which you want to upgrade it to the Switch.
Upload	Start the upgrade procedures.
Download	Download the current configurations to local host.
Reset Configuration	
Reset	Reset the system configurations to default values.

8.5.2 Firmware



Item	Description
Upgrade Firmware	
Choose File	select the new firmware which you want to upgrade it to the Switch.
Upgrade	start the upgrade procedures.

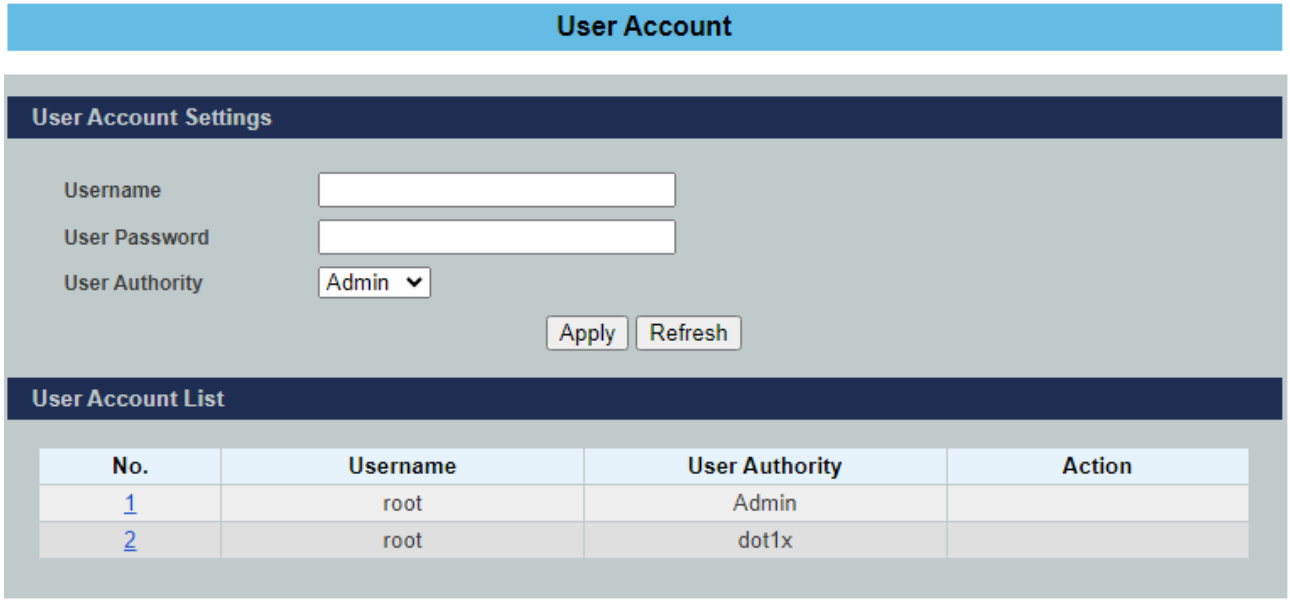
8.5.3 Reboot



Item	Description
Reboot	
Reboot	Reboots the switch

8.6 User Account

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



Item	Description
User Account Settings	
User Name	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.