Lantech

Web UI User's Manual

Industrial 3/5 Switches

Latest update: Sep 2018

Version: 1.53

Important Notice

Lantech Communications Global, Inc. reserves the right to modify the equipment, its specification or this manual without prior notice, in the interest of improving performance, reliability, or servicing. At the time of publication all data is correct for the operation of the equipment at the voltage and/or temperature referred to. Performance data indicates typical values related to the particular product.

No part of this documentation or information supplied may be divulged to any third party without the express written consent of Lantech Communications Global Inc. Products offered may contain software which is proprietary to Lantech Communications Global Inc. The offer or supply of these products and services does not include or infer any transfer of ownership.

Applied Models

This manual applies to Lantech industrial 3/5 managed switches, except the following models: IPGS/IGS-3204MSFP, IPGS/IGS-3008T, IPGS/IGS-3208MGSFP, IPGS/IGS-3208C.

The model list may be changed, Lantech Communications Global, Inc. reserves the right to modify the equipment, its specification or this manual without prior notice.

Content

1. About Web-based Management

There is an embedded HTML web site residing in flash memory on CPU board of the switch, which offers advanced management features and allows users to manage the switch from anywhere on the network through a standard browser such as Mozilla Firefox or Chrome. (note: Window IE is not supported)

The Web-Based Management supports Mozilla Firefox 54.X or later, or Chrome 59.X or later. The Web browser is a program that can read hypertext.

1.1 Preparing for Web Management

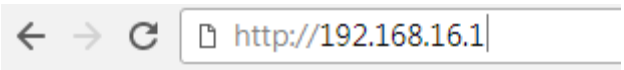
Before using the web management, install the industrial switch on the network and make sure that any one of the PCs on the network can connect with the industrial switch through the web browser.

The industrial switch default value of IP, subnet mask, username and password are listed as below:

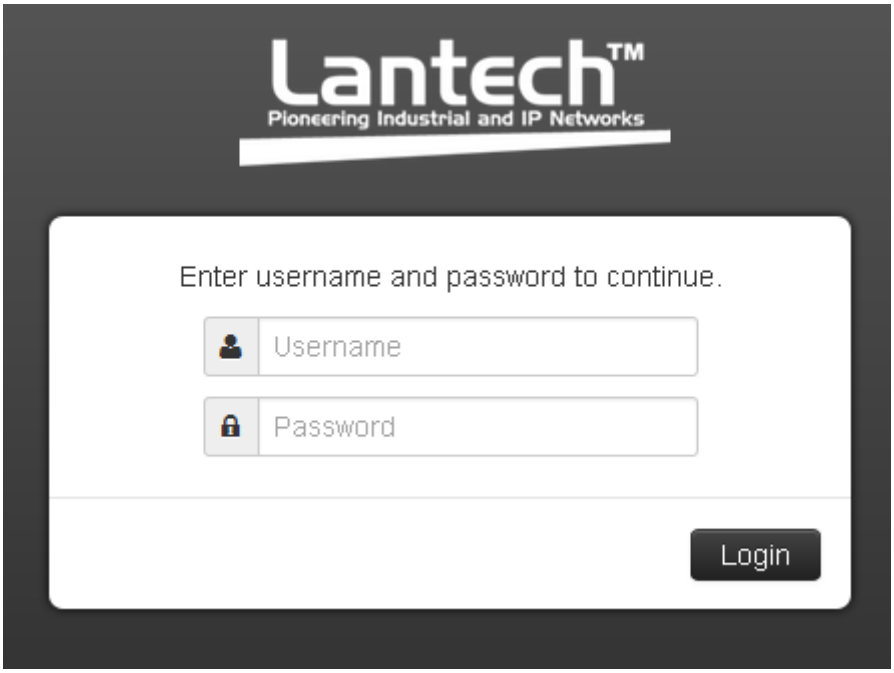
- IP Address: **192.168.16.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.16.254**
- User Name: **admin**
- Password: **admin**

1.2 System Login

1. Launch the Mozilla or Chrome browser on the PC
2. Key in “http:// “+” the IP address of the switch”, and then Press “**Enter**”.

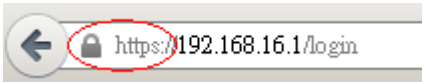


3. The login screen will appear right after



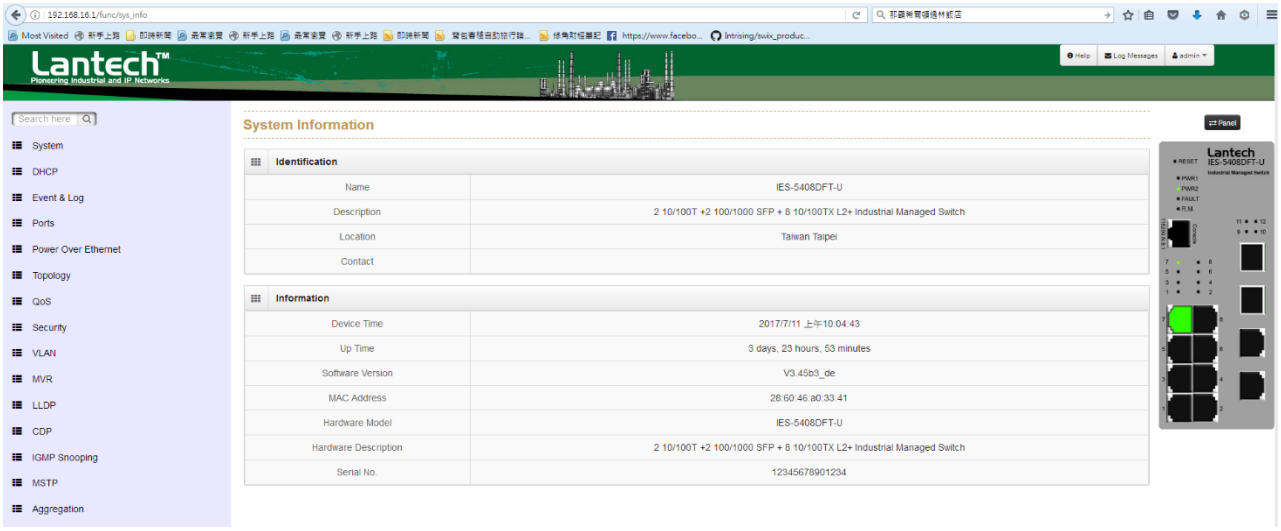
Login screen

4. Key in the user name and password. The default user name and password are the same as '**admin**'.
5. Press **Enter** or click the **OK** button, and then the home screen of the Web-based management appears.
6. The switch also support SSL security login, if you need SSL to protect your access account of switch, please key in "https://" + " the IP address of switch ", and press "Enter"



Note: The changes you make in the dialogs will be over-rode to the device when you click "Apply". Remember to save the setting before you power off or reboot the switch.

1.3 Introduction of the Web Interface



The menu section displays the menu items. Use mouse to select function where you want to set and press left button of mouse to enter the function.

2.System

The "System" submenu consists of the followings:

- System Configuration
- System Information
- IP Configuration
- System Time
- User Accounts
- AAA Configuration
- SNMP Configuration
- Fault Relay Alarm
- Digital Input/Output
- Environment Monitoring
- Auto Provision

2.1 System Configuration

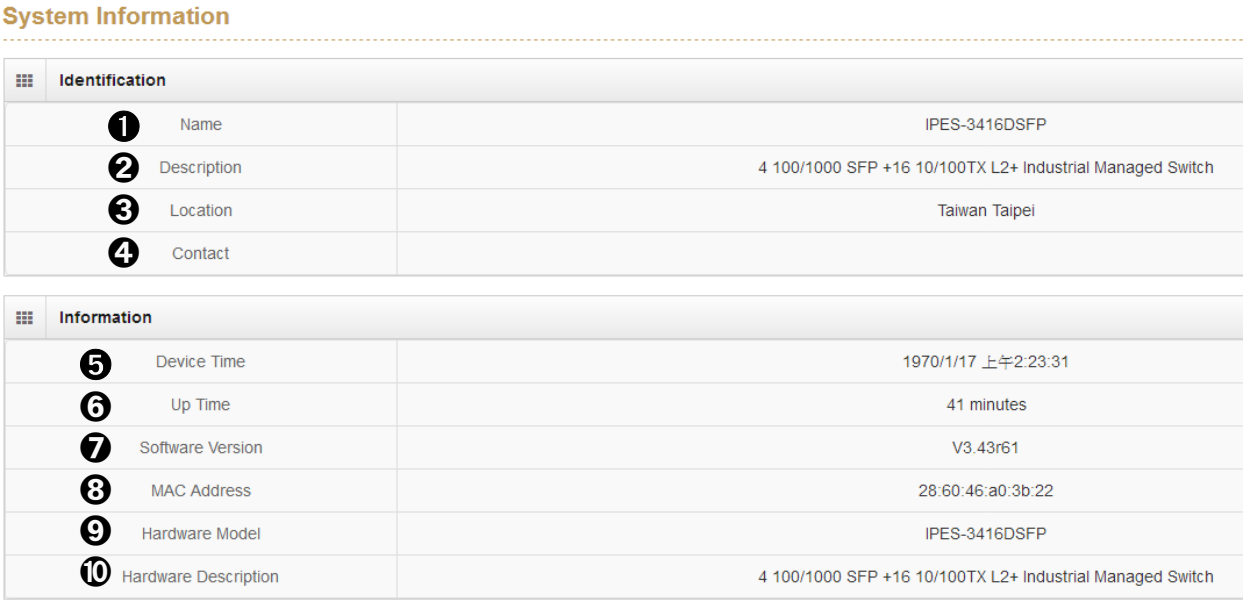
This section displays the system parameters of the device. You can change the following parameters:

- the system name
- the system description
- the location description
- the name of the contact person for this device
- the value of auto logout time

❶ **Name:**	An administratively assigned name which defined by system. It CAN'T be edit manually.
❷ **Description:**	Display the description of switch. The allowed string length is 0 to 255.
❸ **Location:**	The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
❹ **Contact:**	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
❺ **Auto Logout Time:**	Define how long the switch has not received any command from end user via web service, switch will cut off the session between web server with the client. 0 means to disable the auto logout service.

2.2. Switch Information

This function will show you the basic information of switch.



Identification

Name	Description
❶ **Name:**	System name of this device
❷ **Description:**	Description of this device
❸ **Location:**	Location of this device
❹ **Contact:**	The contact for this device

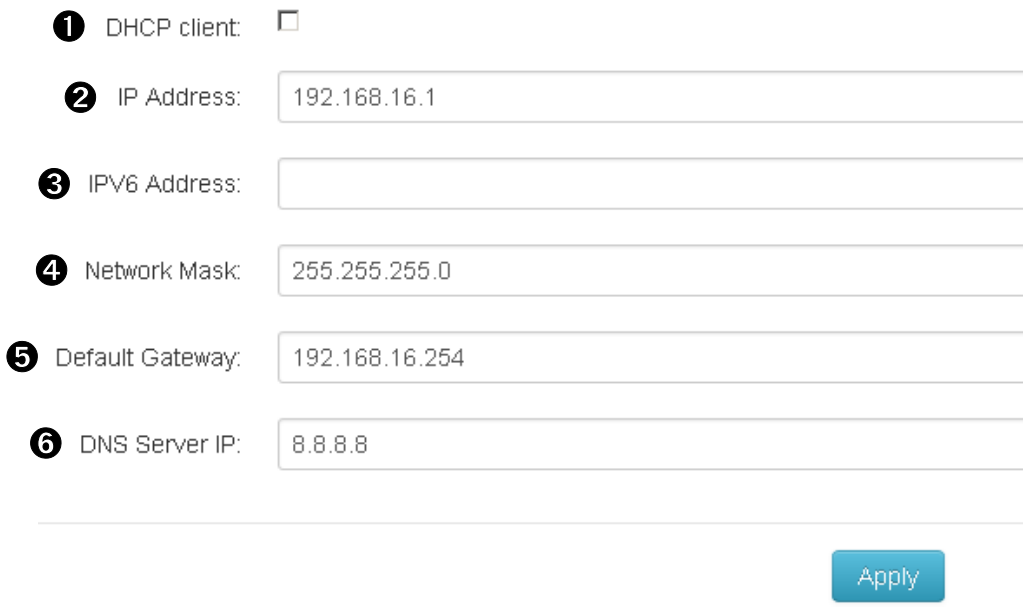
Information

Name	Description
❺ **Device Time:**	System time of switch
❻ **Up Time:**	Time that has elapsed since this device was restarted.
❼ **Software Version:**	Software version of switch system
❽ **MAC Address:**	Media Access Control address of switch

❾ **Hardware Model:**	Model name of switch
❿ **Hardware Description:**	Description of switch model

2.3. IP configuration

The IPv4 settings include the switch's IP address and subnet mask, as well as the IP address of the default gateway.



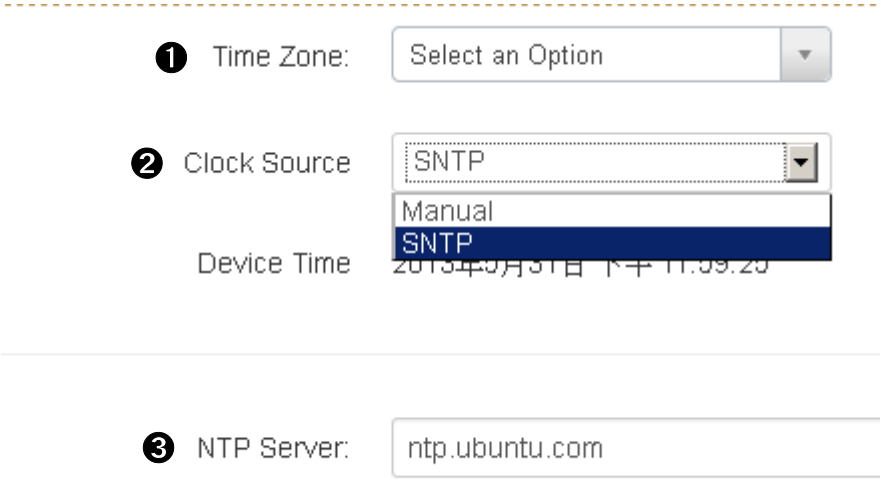
Name	Description
❶ **DHCP client:**	Set the switch as DHCP client, it will get the IP address from DHCP server.
❷ **IP Address:**	Input the IP address of switch
❸ **IPV6 Address:**	You can input the IP address of IPV6 standard.
❹ **Network Mask:**	The network mask of IP address.
❺ **Default Gateway:**	The IP address of network gateway, if you need switch to connect with internet, please input correct IP address.

❻ **DNS Server IP:**	The IP address of DNS server, if you need switch to enable internet service (like SNTP), please input correct IP address.

2.4. System Time

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC). It uses the intersection algorithm, to select accurate time servers and is designed to mitigate the effects of variable network latency. NTP can usually maintain time to within tens of milliseconds over the public Internet, and can achieve better than one millisecond accuracy in local area networks under ideal conditions. Asymmetric routes and network congestion can cause errors of 100 ms or more.

Note: This section is taken from Wiki at https://en.wikipedia.org/wiki/Network_Time_Protocol

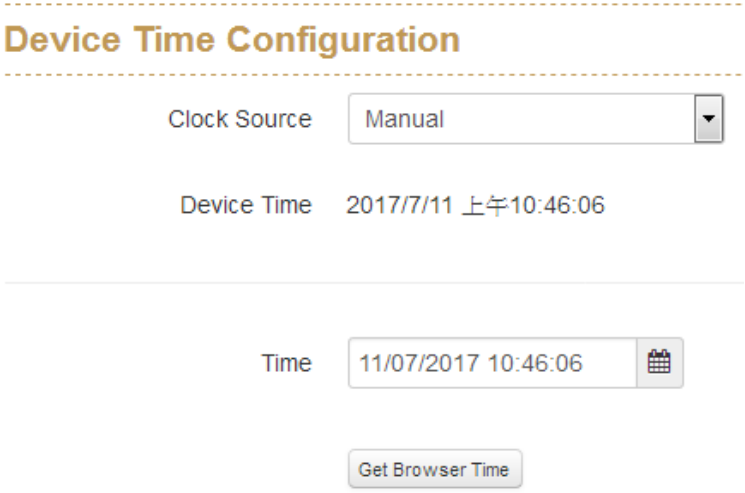


Name	Description
❶ **Time Zone:**	Universal Time Coordinated. Set the switch location time zone. The following table lists the different location time zone for your reference.

Variants	Default Setting

	Please refer to the "Table: Location Time Zone" below	None
❷ **Clock Source:**	You can set the time of switch manually or set SNTP server to let the switch synch the time with SNTP server via internet.	
	Variants	**Default Setting**
	Manual, SNTP	SNTP
❸ **SNTP server:**	The IP address of SNTP server.	

Manual Mode: If the switch can't access internet for security issue, you can set manual mode of clock source to correct system time of switch, just press "get browser time" then the system time of switch will be synchronized with your desktop via web browser.



Note: For the most accurate system time distribution possible, only use network components (routers, switches, hubs) which support SNTP in the signal path between the SNTP server and the SNTP client.

Table: Location Time Zone

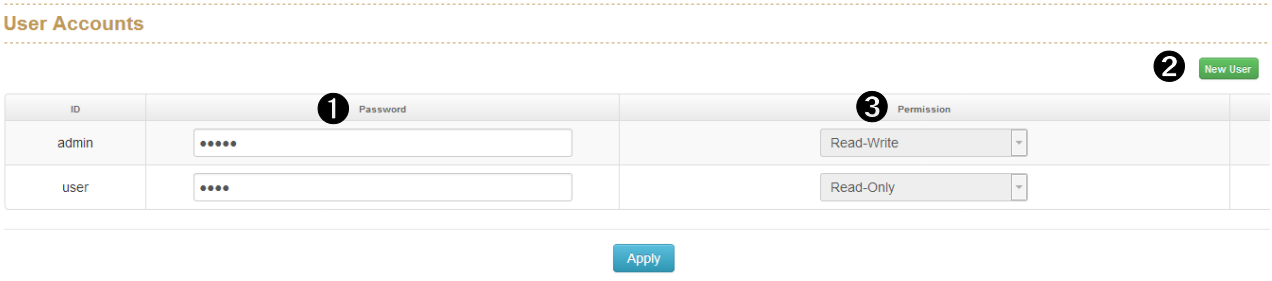
Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am

Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm

ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

2.5. User Accounts

This dialog gives you the option of changing the read and read/write passwords for access to the device via the Web-based interface and via the CLI. Please note that passwords are case-sensitive. Set different passwords for the read and the read/write so that a user that only has read access (user name "user") or read/write access (user name "admin"). If you set identical password for both that will incur a general error.

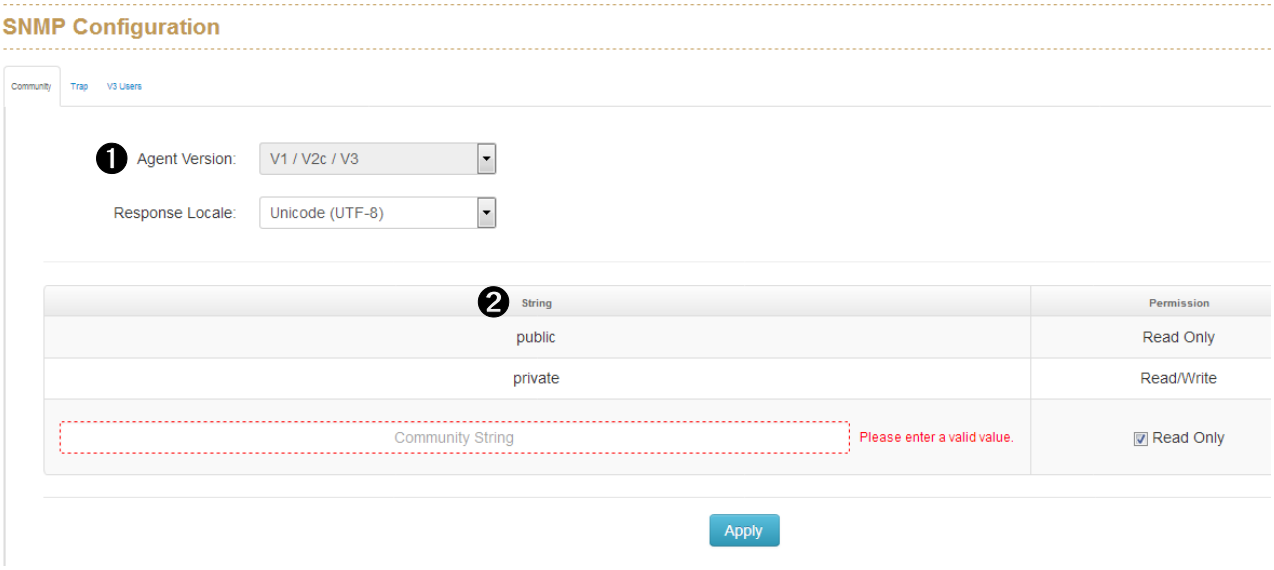


Name	Description
❶ **Password:**	Reset the password of an account
❷ **New User:**	Press to add new account
❸ **Permission:**	Set the permission level of an account

Variants	Default Setting
Read-Write, Read-Only	Read-Write

2.6. SNMP Configuration

Lantech switch supports SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string match for authentication in which the SNMP servers access all objects with read-only or read/write permissions using the community strings public and private by default. SNMP V3 requires you to select an authentication level of MD5 or SHA which is the most secure protocol. You can also enable data encryption to enhance data security.

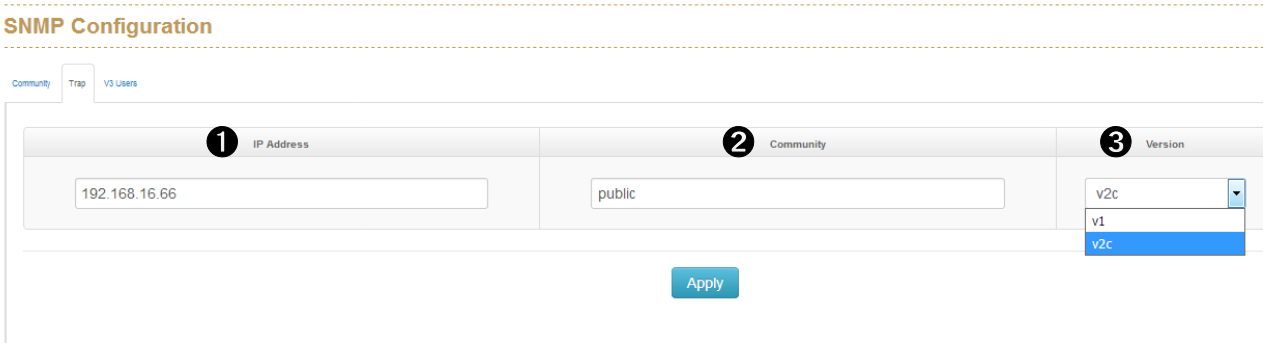


Community

Name	Description
❶ **Agent version:**	Detected by system automatically.

Variants	Default Setting
V1/ V2c/ V3	Detected by system automatically.

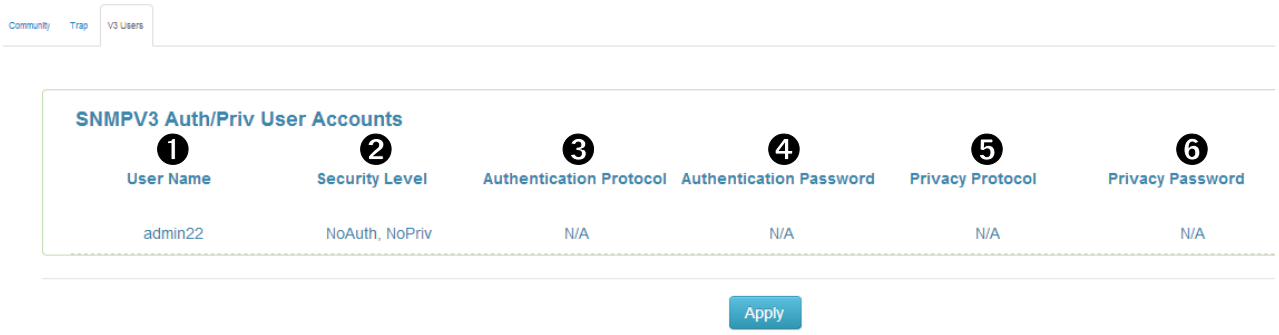
❷ **String:**	Set the community string of SNMP protocol with read only permission or read/write permission.



Trap

Name	Description
❶ **IP Address:**	The IP address of trap destination (usually will be the PC of IT manager).
❷ **Community:**	The community string of SNMP trap.
❸ **Version:**	Select the SNMP trap version.

Variants	Default Setting
V1 or V2c	V2c



V3 Users

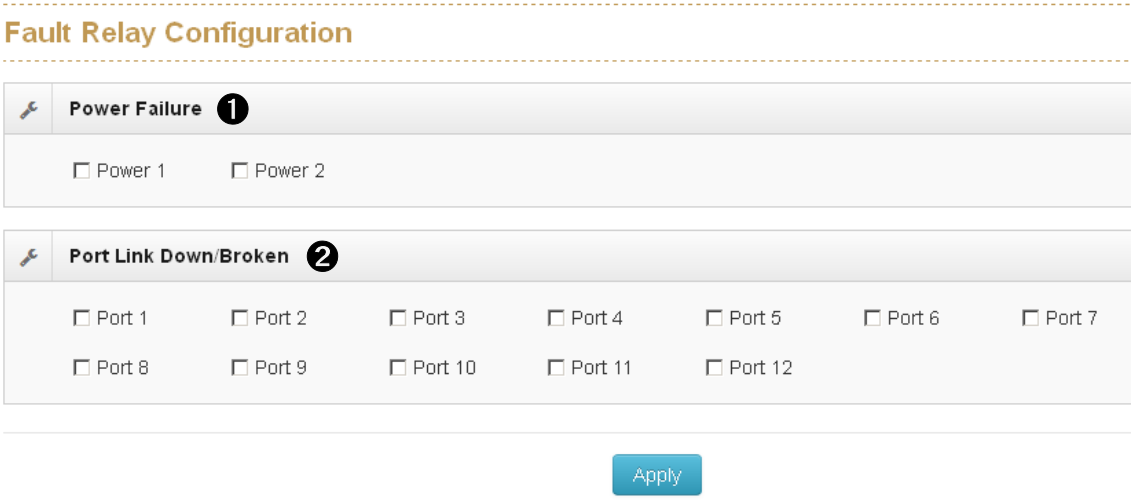
Name	Description
❶ **User name:**	Set the user name.
❷ **Security Level:**	Set up the access level, you can choose Authentication or Privacy or Both.
❸ **Authentication**	Set the authenticated way, the default value was MD5

Protocol:	
❹ **Authentication Password:**	Set the password of authentication.
❺ **Privacy protocol:**	Set the security way, the default value is DES.
❻ **Privacy Password:**	Set the password of Privacy.

Note: For security reasons, SNMPv3 encrypts the password. With the "SNMPv1" or "SNMPv2" setting in the dialog, Security: SNMPv1/v2 access, the switch transfers the password unencrypted that will be shown and readable.

2.7. Fault Relay Configuration

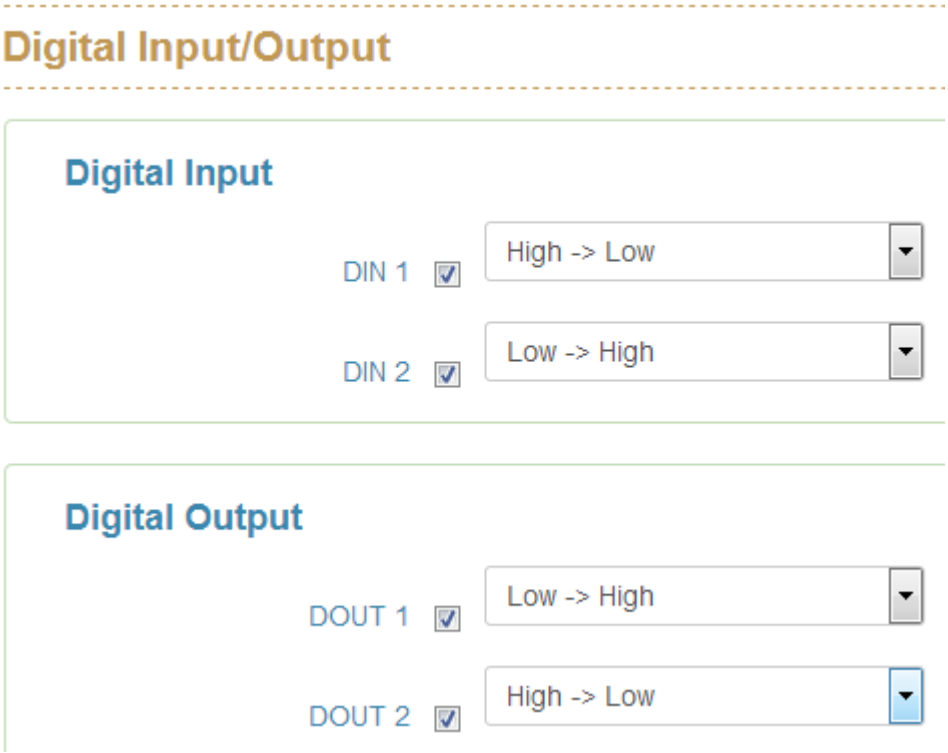
This section allows you to set the condition to trigger Alarm Relay of the switch, including power failure and the linking status of ports.



Name	Description
❶ **Power Failure:**	When you connect both the PWR1 and PWR2 with switch, should one of them fail, the alarm relay will be triggered.
❷ **Port Link Down/Broken:**	Choose the port (one or more) to trigger the alarm relay when the connection fails.

2.8. Digital Input/ Digital Output (DIDO)

This switch contains two digital outputs and two digital inputs. Outputs are open-collector transistor switches that may be controlled by the host computer. They provide messages, which can be applied to heaters, pumps, and other electrical equipment. The digital inputs may be read by the host computer and used to sense the state of a remote digital signal.



Digital Input

When First/Second Digital Input function is enabled, First Digital Input/Second Digital Input will then be available respectively. Digital Input: Choose the transition type to trigger DI0/DI1.

Name	Description
Low->High:	Having focused this radio button, DI0/DI1 will only report the status when the external device's voltage changes from low to high.
High->Low:	Having focused this radio button, DI0/DI1 will only report the

	status when the external device's voltage changes from high to low.
Event Description:	Please fill in the description for the event.

Digital Output

When First/Second Digital Output function is enabled, First Digital Output/Second Digital Output will then be available respectively.

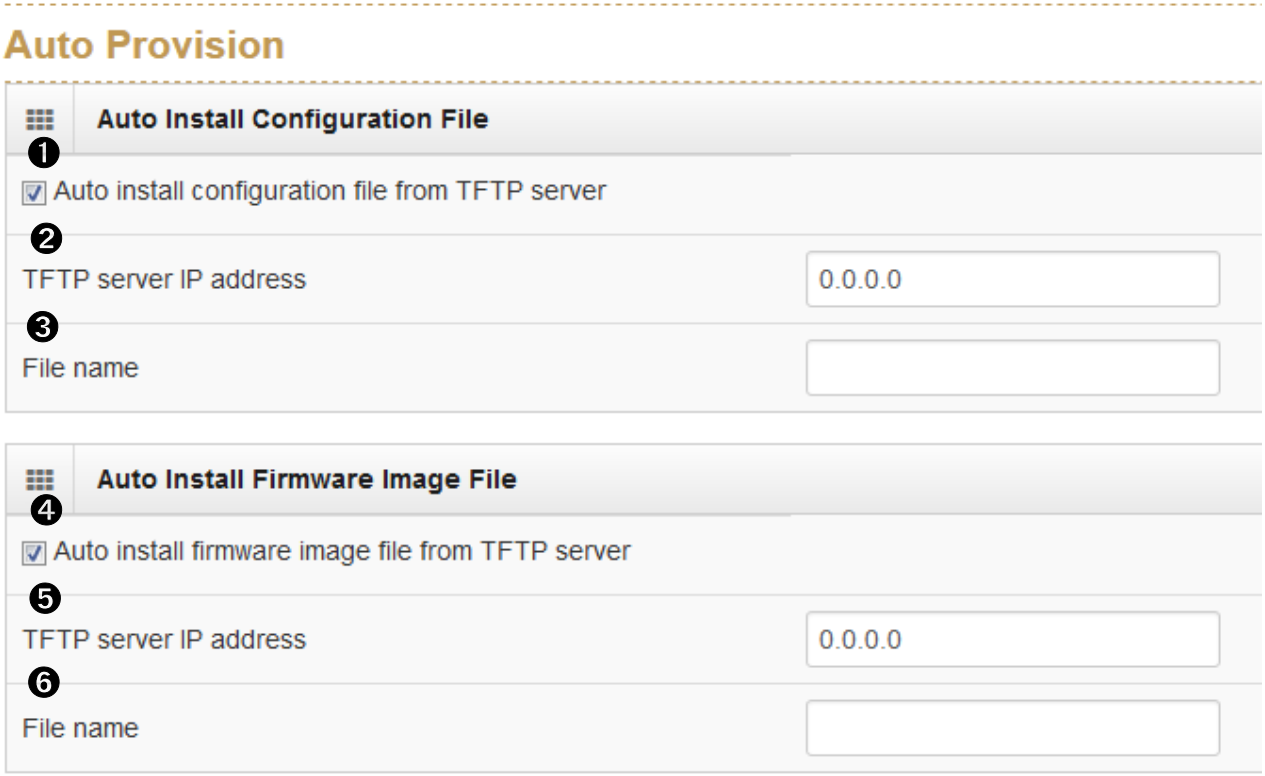
Name	Description
Action:	Choose the output type of electrical signal.
Low->High:	Having focused this radio button, DO0/DO1 will output an electrical signal of Low-to-High when the condition of the ticked checkbox is met (port/power failure occurs).
High->Low:	Having focused this radio button, DO0/DO1 will output an electrical signal of Low-to-High when the condition of the ticked checkbox is met (port/power failure occurs).

2.9. Environmental Monitoring

This function is optional and only support M series.

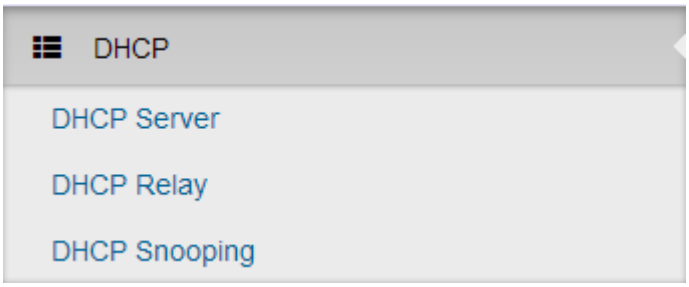
2.10. Auto Provision

Auto provision can help switch to obtain new configuration or upgrade firmware remotely by TFTP protocol.



Name	Description
❶ **Auto install configuration file from TFTP server:**	Enable switch Auto Provision to get configuration remotely.
❷ **TFTP server IP address:**	IP address of TFTP server.
❸ **File name**	File name of configuration file.
❹**Auto install firmware image file from TFTP server:**	Enable switch Auto Provision to upgrade firmware remotely.
❺ **TFTP server IP address:**	IP address of TFTP server.
❻ **File name**	File name of firmware.

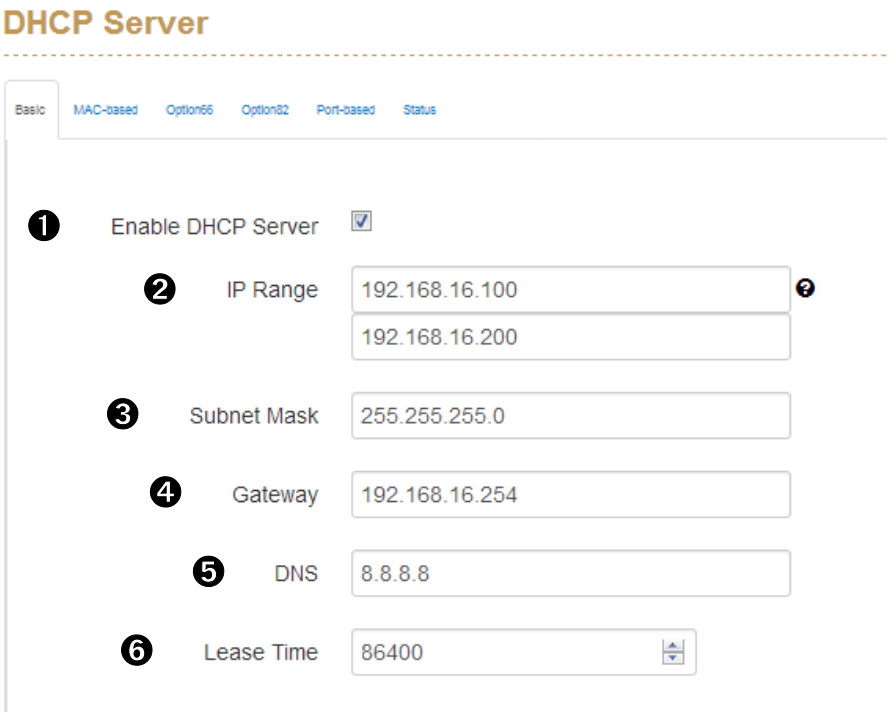
3. DHCP



This section contains the dialogs, displays and tables for:

- Basic DHCP Server
- Mac-based DHCP
- DHCP Option 66
- DHCP Option 82
- Port-based DHCP
- DHCP Status
- DHCP Snooping

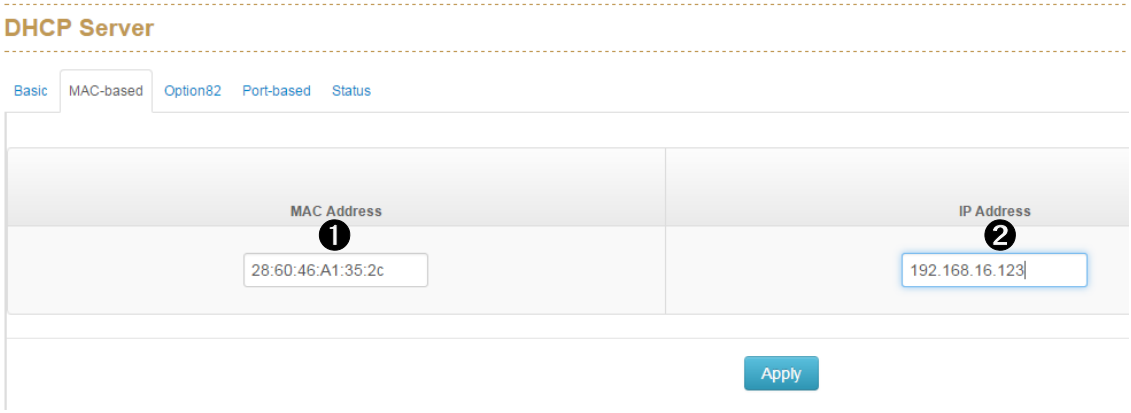
3.1. Basic DHCP Server



Name	Description
❶ **Enable DHCP Server:**	Click to enable the DHCP server function of switch.
❷ **IP Range:**	Define the IP range which will assign to DHCP client from switch.
❸ **Subnet Mask:**	Define the Subnet Mask which will be assigned to DHCP client.
❹ **Gateway:**	Define the gateway which will be assigned to DHCP client.
❺ **DNS:**	Define the DNS which will be assigned to DHCP client.
❻ **Lease Time:**	Define the effective time of assigned IP address; the DHCP client will apply the IP again from DHCP server when the time is over.

3.2. Mac-based DHCP

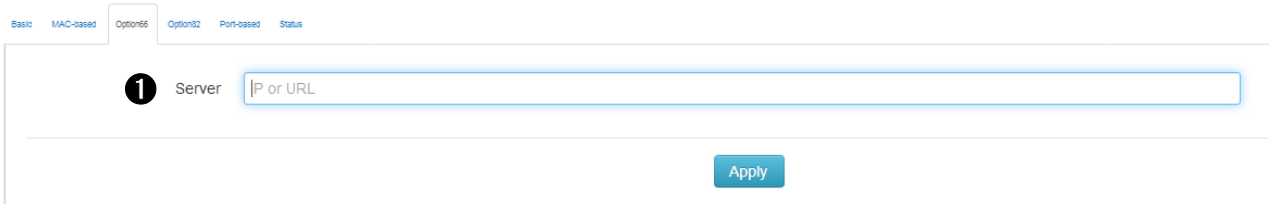
Assign dedicated IP address to the client with dedicated MAC address via DHCP service.



Name	Description
❶ **Mac Address:**	MAC address of dedicated device which you want to assign dedicated IP.
❷ **IP Address:**	Dedicated IP address assigned by DHCP server

3.3. DHCP Option 66

Assign dedicated IP of TFTP server under DHCP option66 standard.



Name	Description
❶ **Server:**	IP address of TFTP server

3.4. DHCP Option 82

Assign dedicated IP address under DHCP option82 standard; you need to assign one Lantech switch as option82 server and other Lantech switches as DHCP relay.

Name	Description
❶ **Remote ID:**	ID of remote DHCP option82 relay switch
❷ **Current ID:**	ID of port of remote DHCP option82 relay switch
❸ **IP Range:**	IP address range will be assigned via current ID
❹ **Netmask:**	Assigned netmask
❺ **Gateway:**	Assigned gateway
❻ **DNS:**	Assigned DNS
❼ **Lease Time:**	Lease time of released DHCP IP address

With Option 82, a DHCP relay agent (Lantech Switch) receiving a DHCP request without Option 82 field will add an "Option 82" field to the request.

3.5. Port-based DHCP

Assign dedicated IP address by port that is connected to the device.

Name	Description
❶ **Port No.:**	Switch port number connecting to the device
❷ **Desired IP:**	Dedicated IP address which will be assigned via this port
❸ **Do not offer IP:**	This port will not assign IP address to ending device

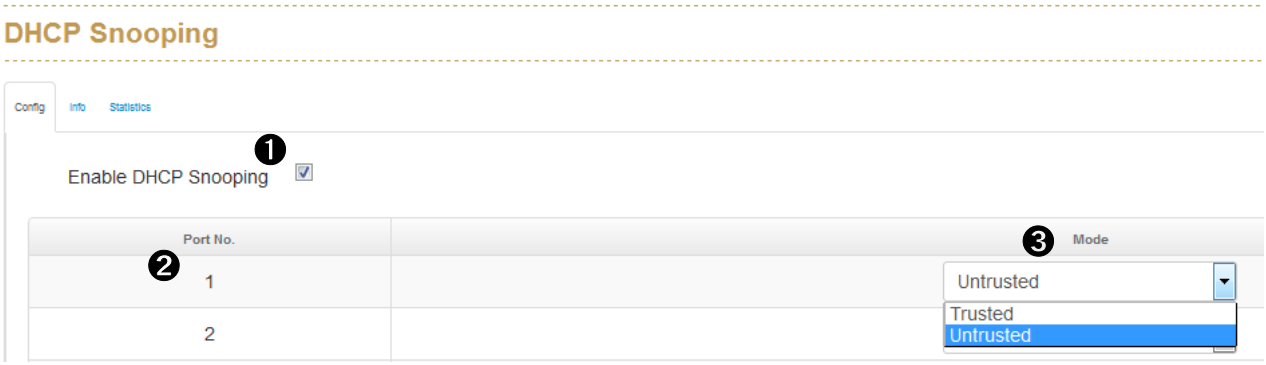
3.6. DHCP Status

It will show you what IP address has been assigned to client.

Name	Description
❶ **Port No.:**	Switch port number
❷ **Mac Address:**	MAC address of ending device
❸ **IP Address:**	IP address of ending device
❹ **Name:**	Host name of ending device
❺ **Available Leased Time:**	How long this IP address will be renewed with DHCP server.

3.7. DHCP Snooping

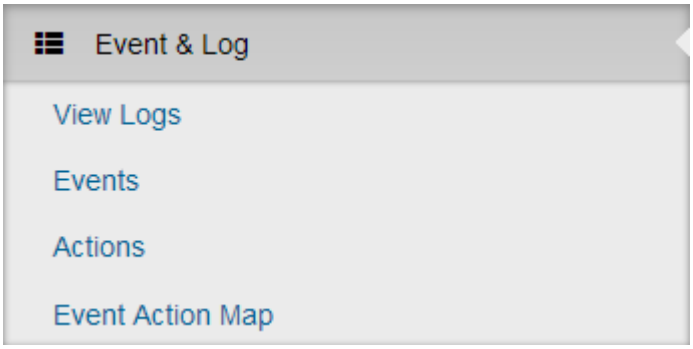
Set dedicated port to forward DHCP packets or block malicious DHCP traffic.



Name	Description
❶ **Enable DHCP Snooping:**	Activate DHCP Snooping function
❷ **Port No.:**	Switch port number
❸ **Mode:**	Trusted: This port will forward DHCP packets. Untrusted: This port will block DHCP packets.

Variants	Default Setting
Trusted, Untrusted	Untrusted

4. Event & Log

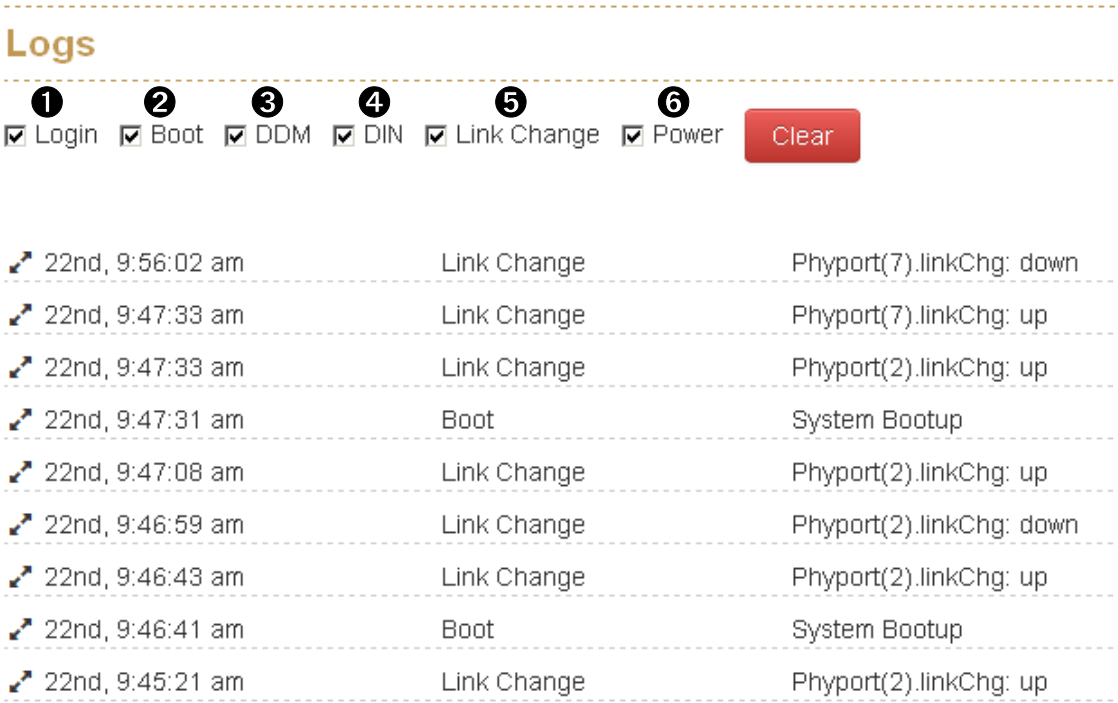


The Event & Log displays the following information

- Occur time
- Event type
- Event description

4.1. View Logs

The section shows the system log entry includes the following action types:



Name	Description
❶ **Login:**	User Login

❷ **Boot:**	System Boot
❸ **DDM:**	DDM information from SFP module
❹ **Din:**	Digital Input Event is triggered
❺ **Link Change:**	Port link up or down
❻ **Power:**	Power condition

Note: The maximum log entry is 1000. When the log exceeds 1000, it will reshuffle from the oldest entry.

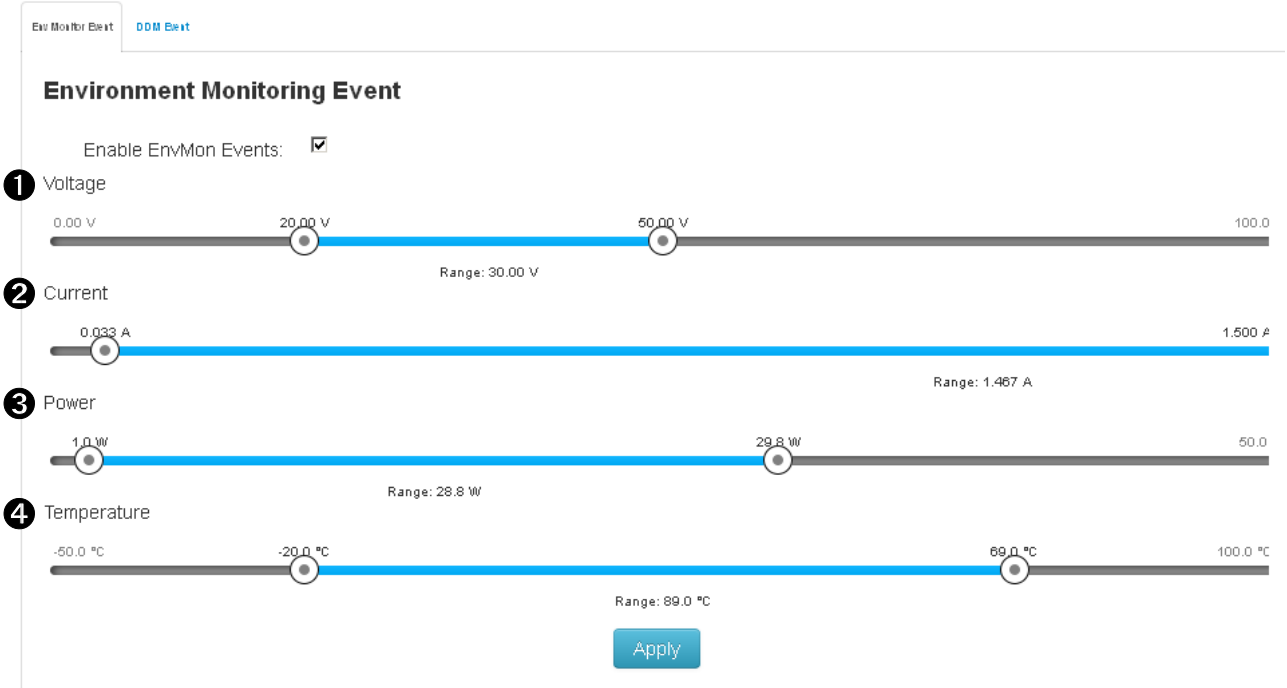
4.2. Events

This function will help you to check the status of the following items.

- Environment Monitoring Event
- SFP Digital Diagnostic Monitor Event

4.2.1. Environment Monitoring Event

You can set the desired triggered range of each event, for example, when you set the blue bar in the range from 20V to 50V, should the voltage of power input is over 50VDC or below 20VDC, it will trigger the event system.

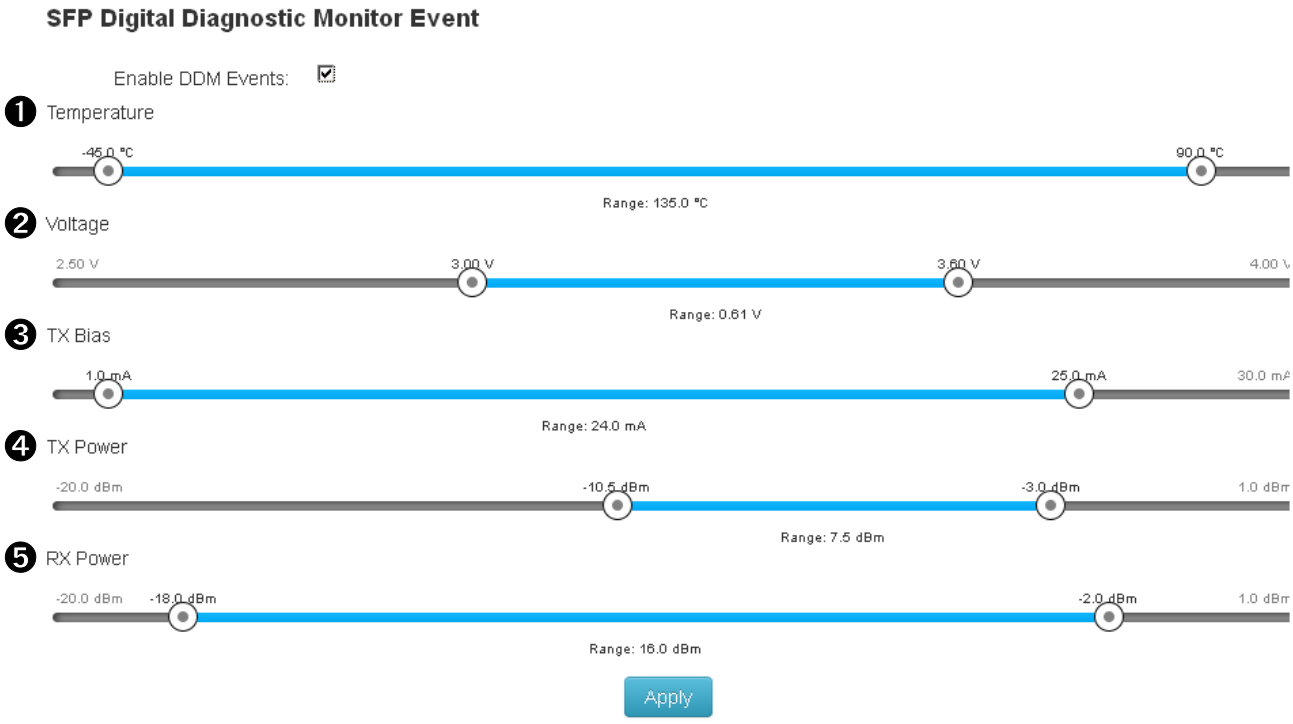


Name	Description
❶ **Voltage:**	Voltage of power input
❷ **Current:**	Current of power input
❸ **Power:**	Power consumption of switch
❹ **Temperature:**	Internal ambient temp. of switch PCB

Notice: This function only works with the model which has built in Environment Monitoring module.

4.2.2. SFP Digital Diagnostic Monitor Event

You can set the trigger range of each SFP DDM event.



Name	Description
❶ **Temperature:**	Working Temp. of SFP
❷ **Voltage:**	Working voltage of SFP
❸ **TX Bias:**	Bias of SFP
❹ **TX Power:**	Tx power of SFP
❺ **RX Power:**	Rx power of SFP

Notice: This function only works for the SFP module with DDM spec.

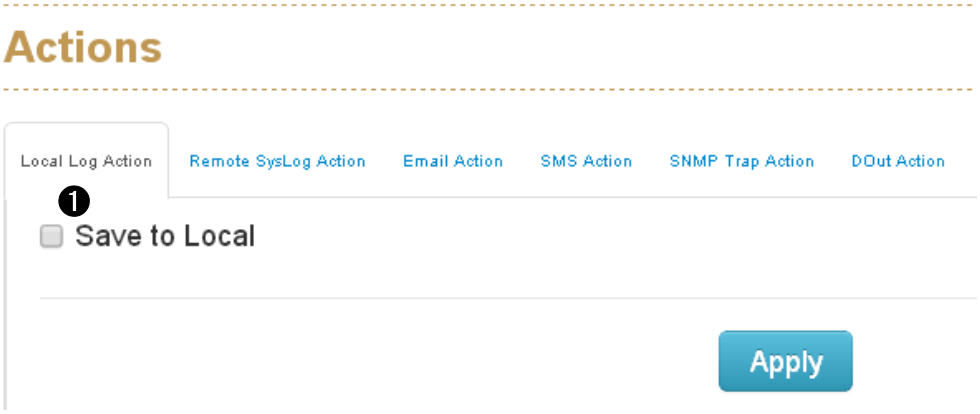
4.3. Actions

When switch find event, it will trigger the follow-by action pre-set.

You can find all reactive actions as follows:

- Local Log Action
- Remote Syslog Action
- Email Action
- SNMP Trap Action
- SMS Action
- DOUT Action

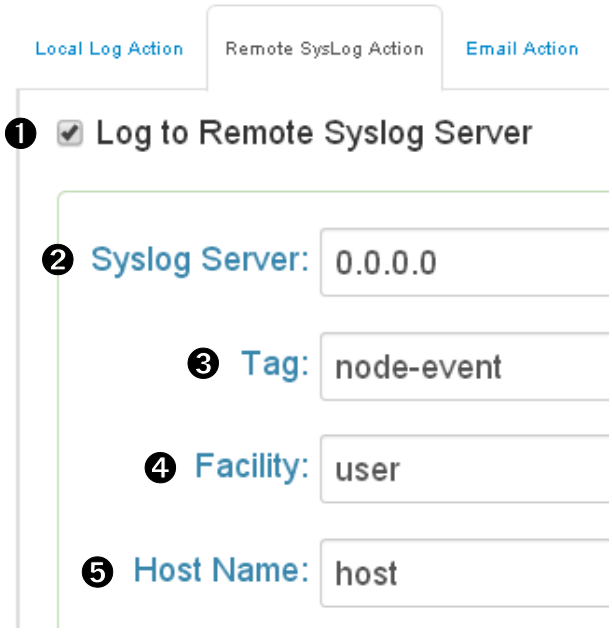
4.3.1. Local Log Action



Name	Description
❶ **Save to Local:**	Click to save log to local switch

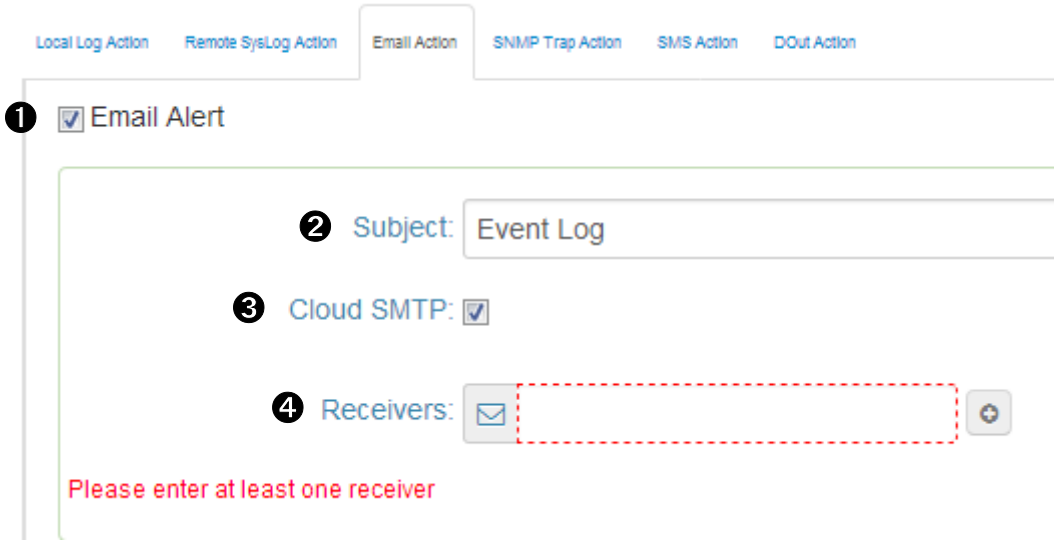
4.3.2. Remote Syslog Action

The "Syslog" dialog enables you to additionally send event to one or more syslog servers locating local or remote. You can switch the function on or off.



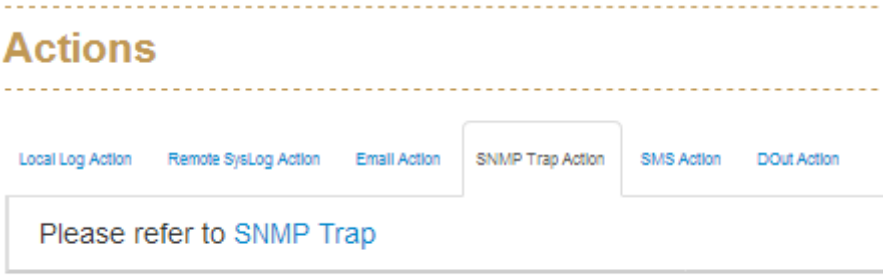
Name	Description
❶ **Log to Remote Syslog Server:**	Click to save log to Syslog Server
❷ **Syslog Server:**	IP address of Syslog server
❸ **Tag:**	Tag of event
❹ **Facility:**	Facility of event
❺ **Host Name:**	Host name of event

4.3.3. Email Action



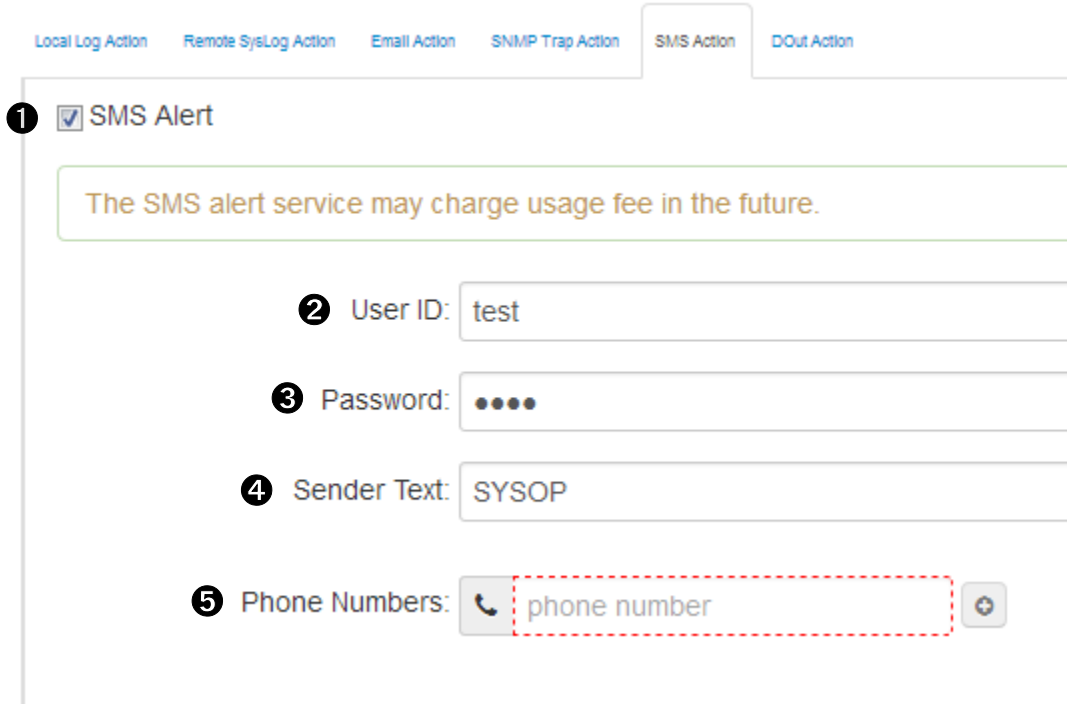
Name	Description
❶ **Email Alert:**	Click to sent log alert via Email
❷ **Subject:**	Subject of email
❸ **Cloud SMTP:**	Send Email via Lantech Cloud SMTP server
❹ **Receivers:**	Email address of event receiver

4.3.4. SNMP Trap Action



Name	Description
SNMP Trap Action:	The setting page of this function will be redirect to SNMP configuration of System.

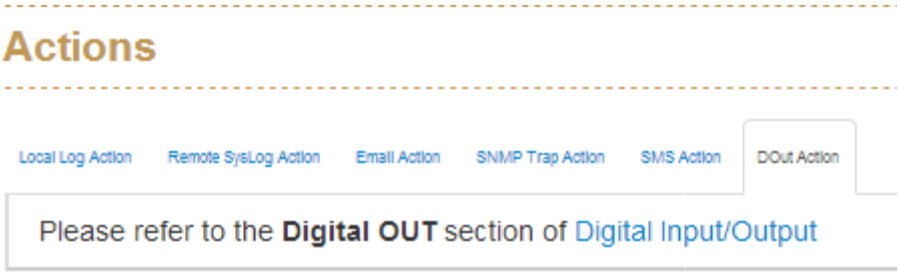
4.3.5. SMS Action



Name	Description
❶ **SMS Alert:**	Click to send log alert via SMS service.
❷ **User ID:**	User name of SMS account
❸ **Password:**	Password of SMS account
❹ **Sender Text:**	Content of SMS message
❺ **Phone Numbers:**	Cell-phone number of recipient

Note: The switch must connect with internet and define the SMS server to activate this service. Currently the SMS service is offered by Lantech in Taiwan.

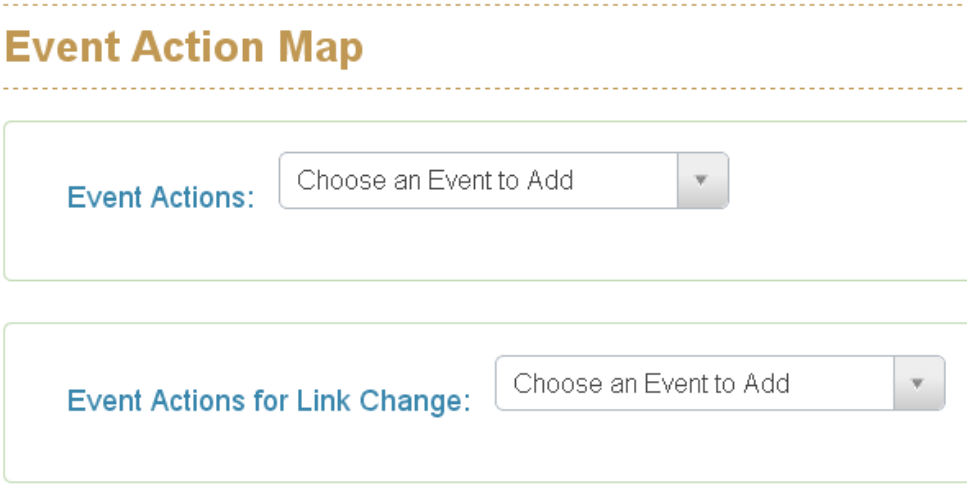
4.3.6. DOUT Action



Name	Description
DOUT Action:	The setting page of this function will be redirect to Digital Input/Output configuration

4.4 Event Action Map

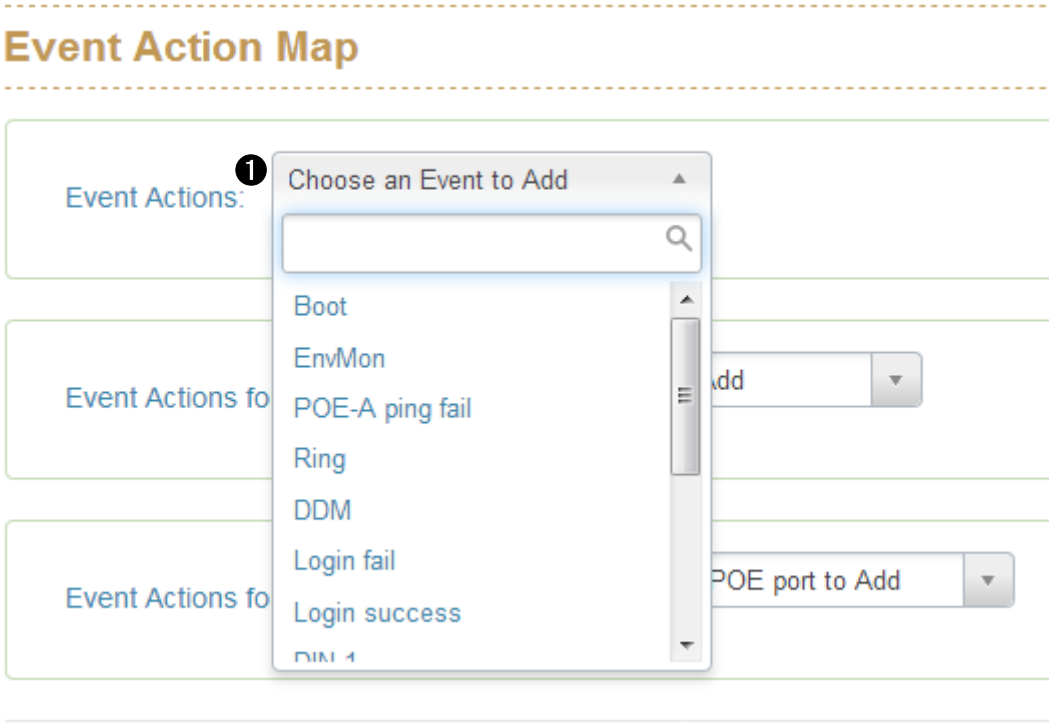
You can combine event and action setting here.



Event Actions:

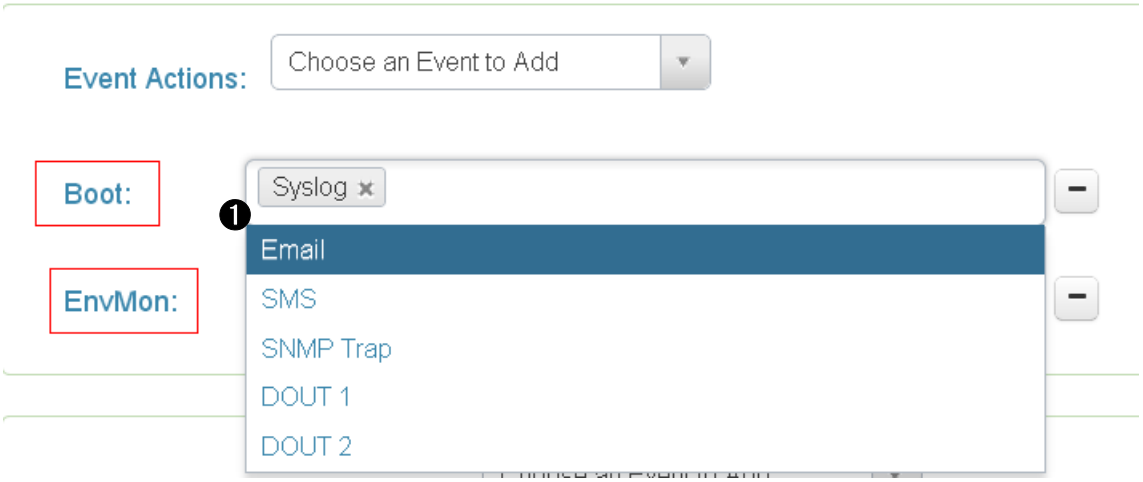
Please follow the steps below to set the event actions:

A. Choose the event which you want to activate.



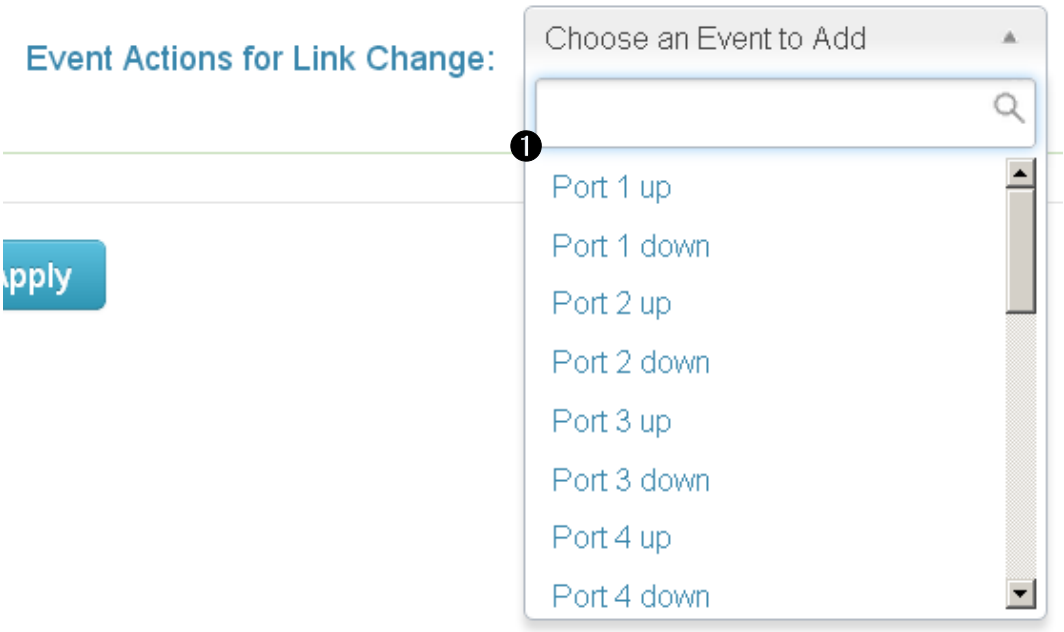
Name	Description	Variants	Default setting
❶ **Event Actions**:	Which event will be combined with desired action	Boot EnvMon POE-A ping fail Ring DDM Login fail Login success DIN1 DIN2 Power1 on Power1 off Power2 on Power2 off	None

B. You will find the selected event to be shown as follows, then choose forwarding method to define how to forward this event to manager side.



Name	Description	Variants	Default setting
❶ **Forwarding method:**	Which action will be combined with this event	Email SMS SNMP Trap DOUT 1 DOUT 2	None

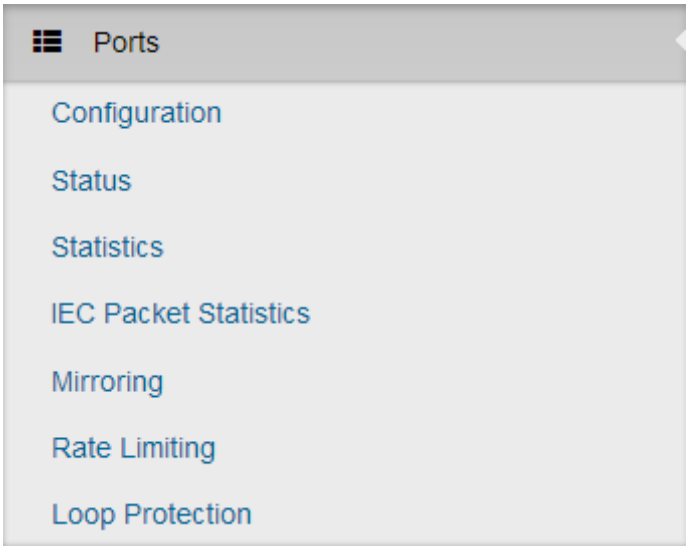
C. You can set the forwarding method of port up/down event here.



Name	Description	Variants	Default setting
❶ **Event**	Select dedicated port link or	Port 1 up	None

Actions for Link Change:	down event to combine action	Port 1 down Port 2 up Port 2 down Port 3 up Port 3 down Port 4 up Port 4 down ……etc

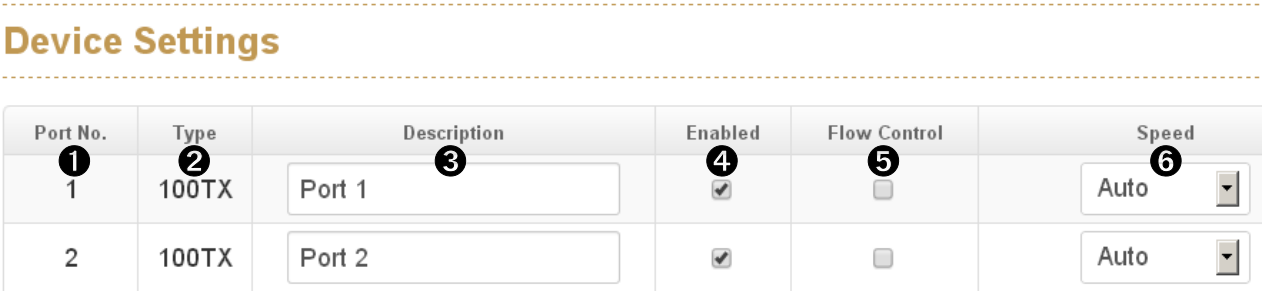
5.Ports



This section guides how to control and manage the ports of switch.

5.1 Configuration

Device Settings panel shows port configurations and each port can be configured here.



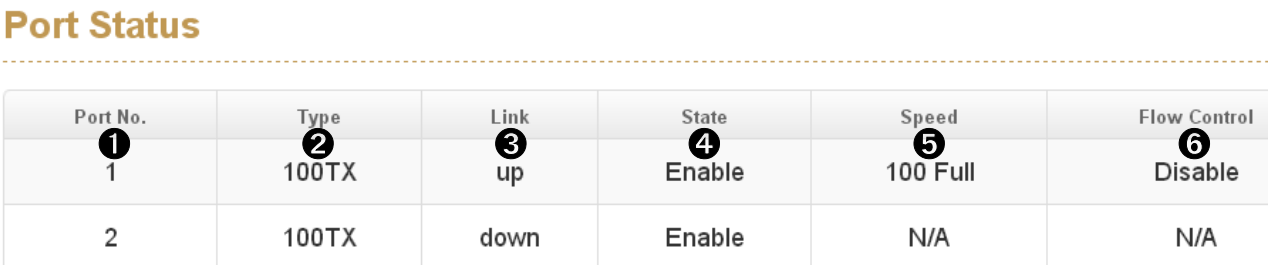
Name	Description
❶ **Port No.:**	Number of the port.
❷ **Type:**	Media type of the port (100Tx/1000T/GSFP/DSFP).
❸ **Description:**	Enter up to 47 characters to describe the port for better identification.
❹ **Enabled:**	Enabled or disable port transmission.

❺ Flow Control: Enabled or disable flow control.

❻ Speed: Select the speed of the port. Only supported speed would be shown as an option.

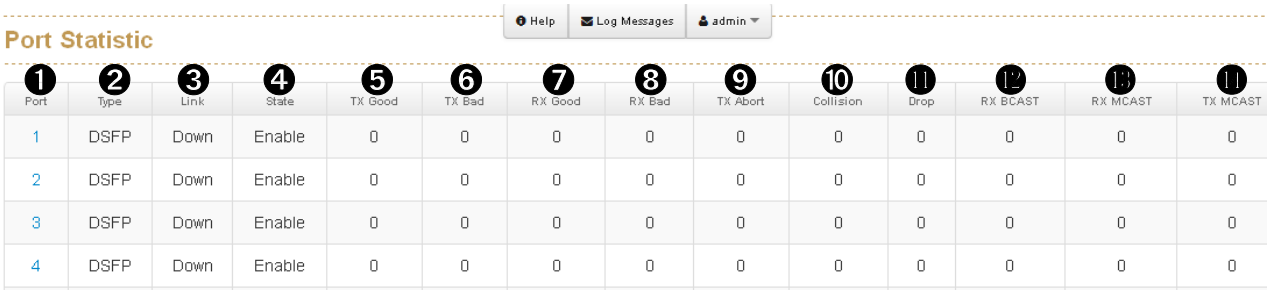
Options	Default Setting
Disabled – Deactivate the port. Auto – Let the port to negotiate the speed with the linking device and reach the maximum speed that is possible. 10Mbps HDX - Forces the cu port in 10Mbps half duplex mode. 10Mbps FDX - Forces the cu port in 10Mbps full duplex mode. 100Mbps HDX - Forces the cu port in 100Mbps half duplex mode. 100Mbps FDX - Forces the cu port in 100Mbps full duplex mode. 1Gbps FDX - Forces the cu port in 1Gbps full duplex mode.	Auto

5.2 Status



Name	Description
❶ **Port No:**	Number of the port.
❷ **Type:**	Media type of the port (100Tx/1000T/GSFP/DSFP).
❸ **Link:**	Link status: up or down.
❹ **State:**	State of port linking status.
❺ **Speed:**	The speed of link (detailed description may refer to page 32 Possible Options).
❻ **Flow Control:**	Status of Flow Control. *Flow Control is only available when the speed of port is set to Auto and therefore its efficiency is subject to the negotiation between the port and the linking device.

5.3 Statistics



Name	Description
❶ **Port:**	Number of each port.
❷ **Type:**	Media type of each port (100Tx/1000T/GSFP/DSFP).
❸ **Link:**	Link status: Up or Down.

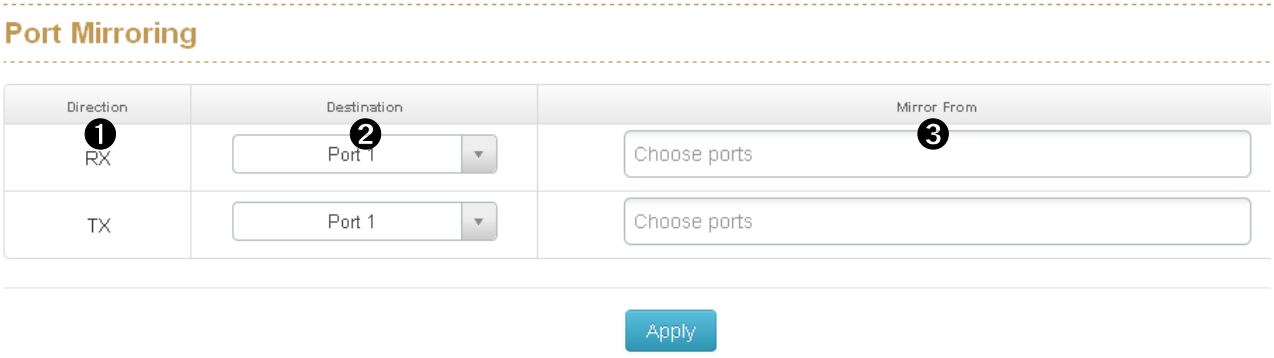
❹ **State:**	Port status: Enable or not
❺ **Tx Good Packet:**	The counts of transmitting good packets via this port.
❻ **Tx Bad Packet:**	The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
❼ **Rx Good Packet:**	The counts of receiving good packets via this port.
❽ **Rx Bad Packet:**	The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
❾ **Tx Abort Packet:**	The aborted packet while transmitting.
❿ **Packet Collision:**	The counts of collision packet.
⓫ **Packet Dropped:**	The counts of dropped packet.
⓬ **Rx Bcast Packet:**	The counts of broadcast packet.
⓭ **Rx Mcast Packet:**	The counts of multicast packet.
⓮ **Tx Mcast:**	The counts of transferring multicast packet.

5.4 Mirroring

Port Mirroring is a method of monitoring network traffic. With port mirroring enabled, the switch sends a copy of all network packets seen on some ports (Source Port) to another port (Destination Port), where the packet can be analyzed.

Source Port: The port(s) that is/are to be monitored. The monitored port(s) traffic will be copied to Destination Port.

Destination Port: There is only one port can be assigned as Destination Port for monitoring both RX and TX traffic which come from source port(s).



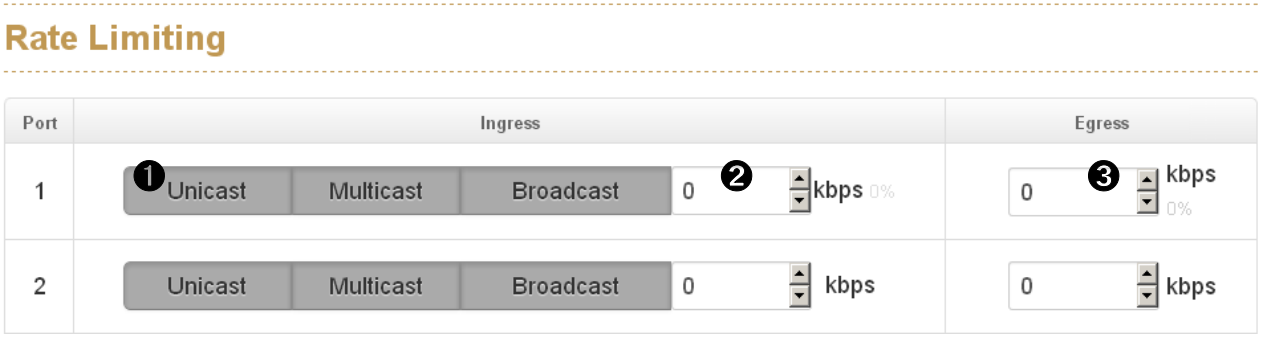
Name	Description
❶ **Direction:**	Choose to monitor only the packets coming in (RX) or sending out (TX) via the port.
❷ **Destination:**	Choose the port which receives monitoring packets.
❸ **Mirror From:**	Choose the port(s) which to be monitored.

5.5 Rate Limiting

Rate Limiting allows setting limit of each port's ingress/ egress rate.

Ingress control supports limit of packet type and rate, there are 4 packet types for selection: All, Unicast, Multicast and Broadcast.

Egress control supports limit of rate only.



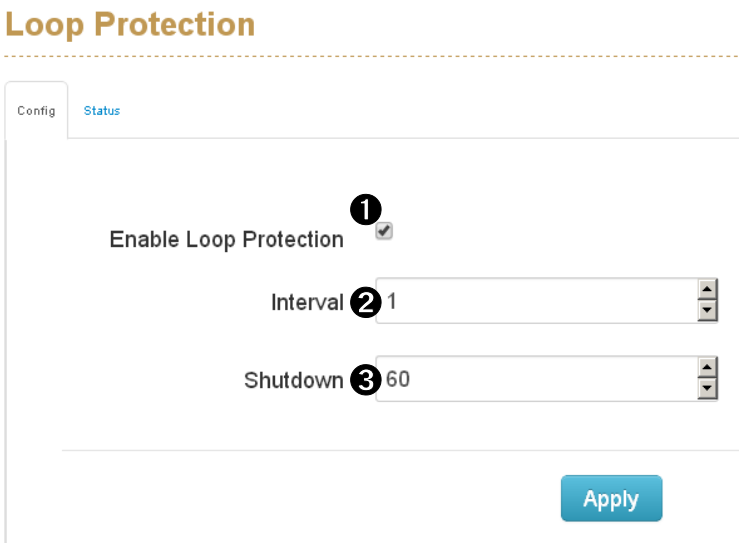
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>❶ Band Width:</td><td>All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set its effective egress rate is 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate.
<table>
<tr><th>Packet Types</th><th>Default Setting</th></tr>
<tr><td>1. All
2. Unicast
3. Multicast
4. Broadcast</td><td>All</td></tr>
</table>
</td></tr>
<tr><td>❷ Ingress:</td><td>Enter the limit of ingress rate (The default value is "0"</td></tr>
<tr><td>❸ Egress:</td><td>Enter the limit of egress rate (The default value is "0"</td></tr>
</table>

Note: Rate Limiting works exclusively on layer 2 to serve the purpose of limiting the impact of flooding packets. Therefore, this function ignores any protocol information of higher layers like IP or TCP.

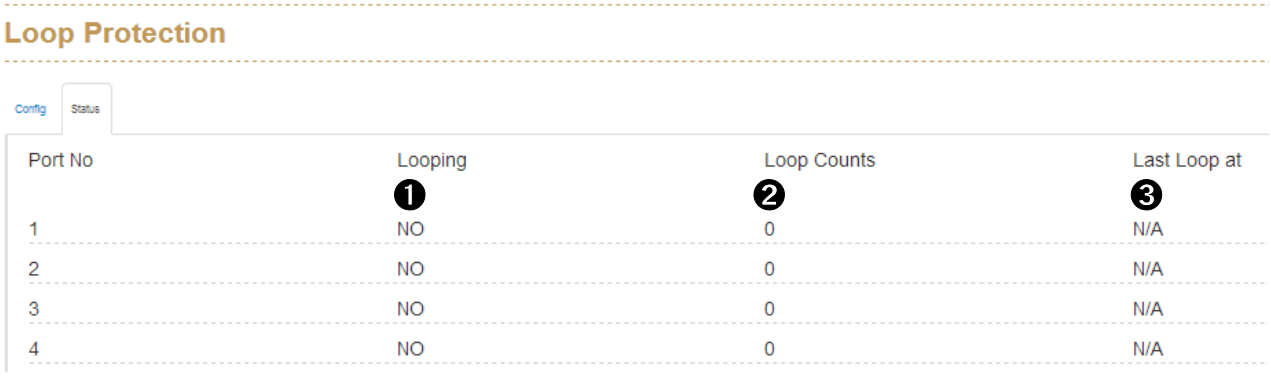
Note: Ports that are included in a Link Aggregation are excluded from the rate limitation, regardless of the entries in the "Rate Limiting" dialog.

5.6 Loop Protection

Loop Protection helps to prevent the broadcast storm which caused by loop connection.

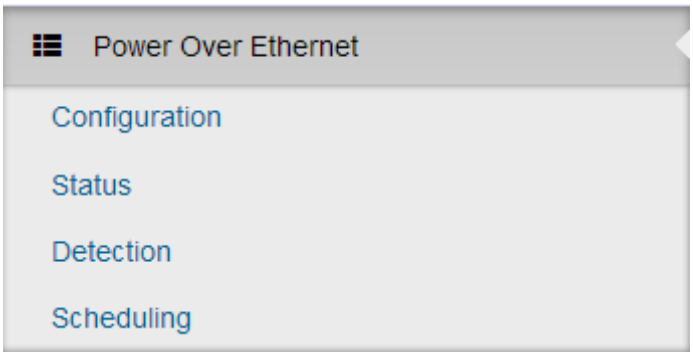


Name	Description
❶ **Enable Loop Protection:**	Enable or disable loop protection.
❷ **Interval** (second):	Define how often the switch will check the loop status of each port.
❸ **Shutdown** (second):	Define how long the port will be blocked when it is looping.



Name	Description
❶ **Looping:**	Loop status of the port.
❷ **Loop Counts**:	Show how many loops happened to the port.
❸ **Last Loop at:**	Show the time of the last loop happened.

6. Power over Ethernet



Power over Ethernet (PoE) is a way to transmit power over Ethernet cable to PD (Powered devices). The standards are IEEE 802.3at/af with different power output. The IEEE802.3af can transmit max 15.4W per port while IEEE802.3at, also known as PoE+, transmit 30W per port. In the physical connection of PoE technology, please consider power loss over the length of cable. The minimum power available is 12.95Watts per port over IEEE802.3af and 25.5Watts per port over IEEE802.3at standard.

There are several common techniques for transmitting power over Ethernet cabling. Two of them have been standardized by IEEE 802.3 since 2003. These standards are known as *Alternative A* and *Alternative B*. For 10BASE-T and 100BASE-TX, only two of the four data/signal pairs in typical CAT-5 cable are used. **Alternative B** separates the data and the power conductors, making troubleshooting easier. It also makes full use of all four twisted pair, copper wires. The positive voltage runs along pins 4 and 5, and the negative along pins 7 and 8.
Note: This part is taken from Wiki at
https://en.wikipedia.org/wiki/Power_over_Ethernet

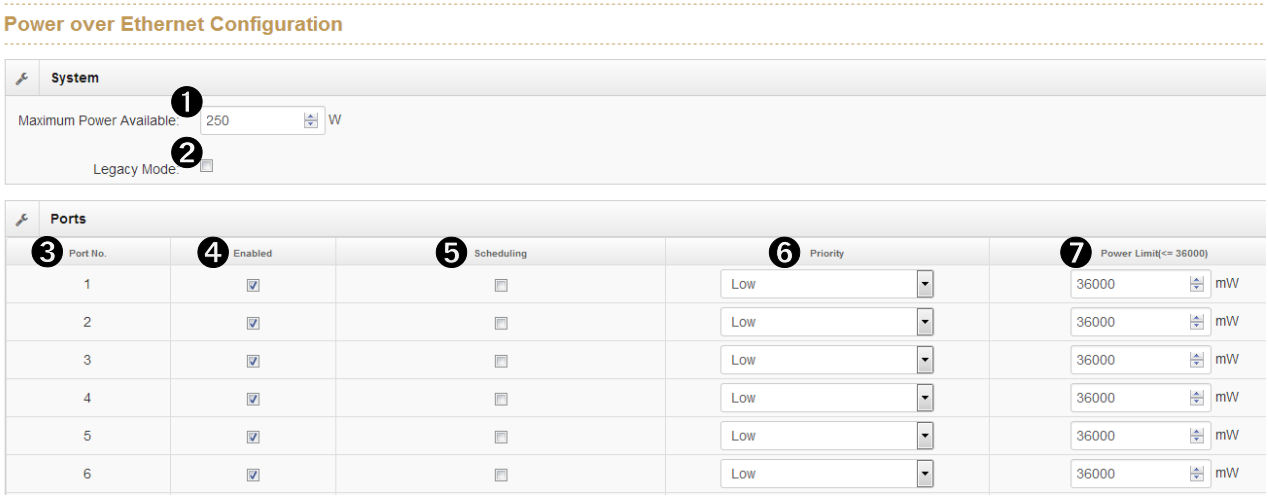
Lantech supports most PoE switch as PSE (power sourcing equipment) using Alternative A technique. Only a couple of models support Alternative B technique.

Lantech PoE models have options with different input range including 12/24V→48V boost up, 72V →48V step down and high voltage 85~265VAC/ 110~300VDC. Furthermore, Lantech managed PoE switches offer PD detection and PoE scheduling

for advanced PoE management.

Note: PoE is an optional hardware function, Lantech PoE switch (PSE Power Sourcing Device) supports different input voltage to feed 48V PoE output with different PoE budget, please check your model for correct input range and PoE budget before you connect to PDs.

6.1 Configuration



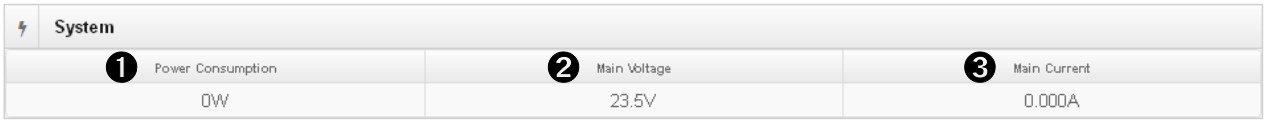
Name	Description
❶ **Maximum Power Available:**	Define the limit of total power consumption.
❷ **Legacy mode:**	Force switch to supply power to legacy PD.
❸ **Port No.:**	Number of the PoE port.
❹ **Scheduling:**	The PoE port is under control with PoE scheduling function.
❺ **Enable:**	Enable or disable PoE function of the port.
❻ **Priority:**	Set the priority of power supply. If the total power consumption of all PoE ports meets the maximum power limit, then the switch will supply power by priority setting.

Priority Options	Default Setting

	Low / High/ Critical	Low
❼ **Power Limit:**	Define the maximum power of the PoE port.	

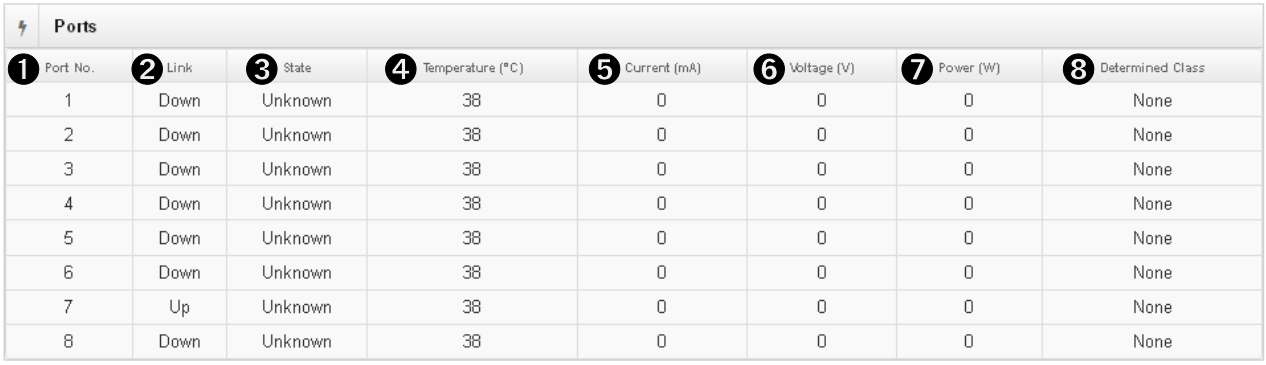
6.2 Status

System



Name	Description
❶ **Power Consumption:**	Total power consumption of all PoE ports
❷ **Main Voltage:**	The output voltage of each PoE port.
❸ **Main Current:**	The output current of each PoE port.

Ports



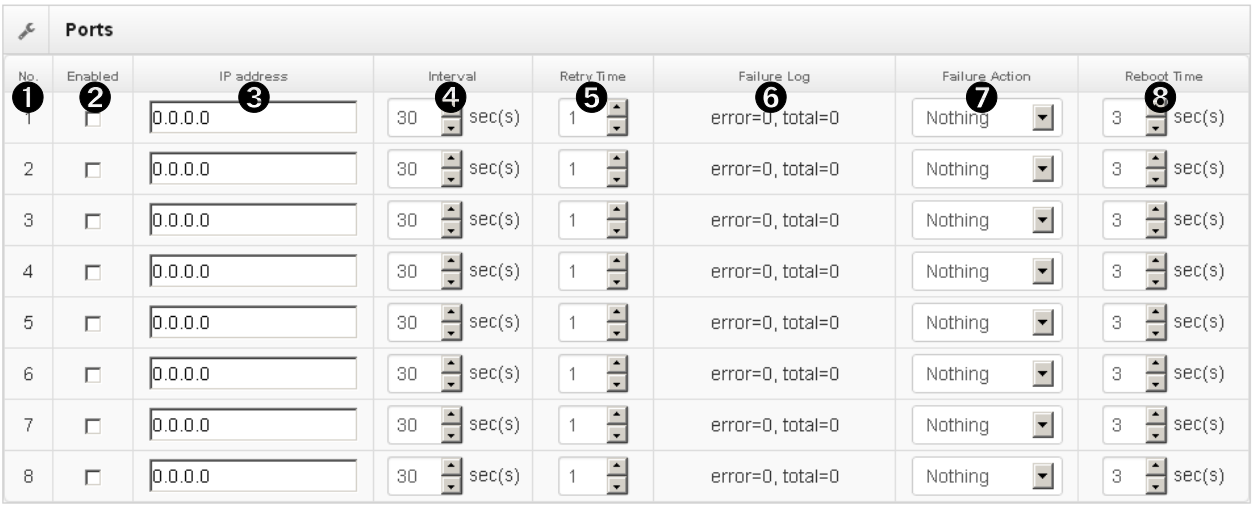
Ports

❶ Port No.	❷ Link	❸ State	❹ Temperature (°C)	❺ Current (mA)	❻ Voltage (V)	❼ Power (W)	❽ Determined Class
1	Down	Unknown	38	0	0	0	None
2	Down	Unknown	38	0	0	0	None
3	Down	Unknown	38	0	0	0	None
4	Down	Unknown	38	0	0	0	None
5	Down	Unknown	38	0	0	0	None
6	Down	Unknown	38	0	0	0	None
7	Up	Unknown	38	0	0	0	None
8	Down	Unknown	38	0	0	0	None

Name	Description
❶ **Port No.:**	Number of each PoE port.
❷ **Link:**	Connection status of each PoE port.
❸ **State:**	PoE status of each connected PD (Unknown means the connected device is non-PD).
❹ **Temperature (℃):**	Temperature of PoE chipset surface.
❺ **Current (mA):**	Output current of each PoE port.
❻ **Voltage (V):**	Power consumption of each PoE port.
❼ **Power (W):**	PoE class of each connected PD.
❽ **Determined Class:**	Number of each PoE port.

6.3 Detection

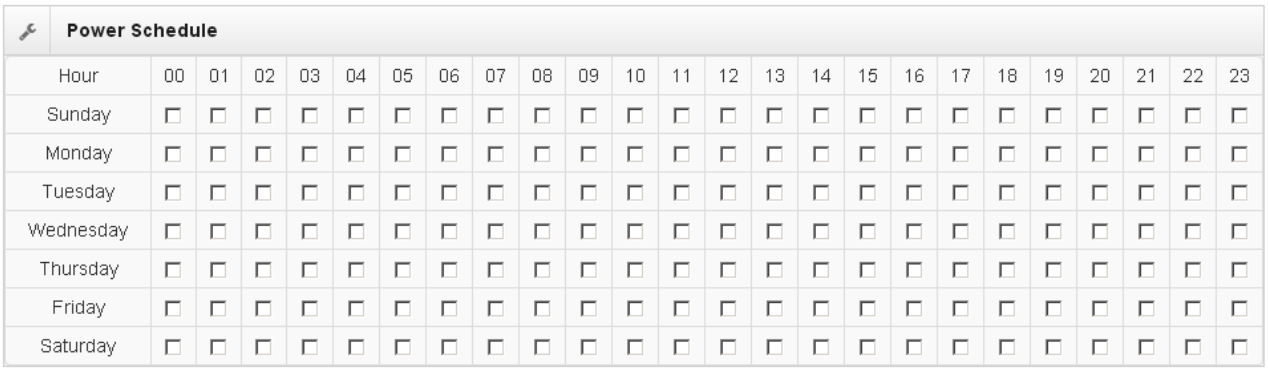
Device Detection



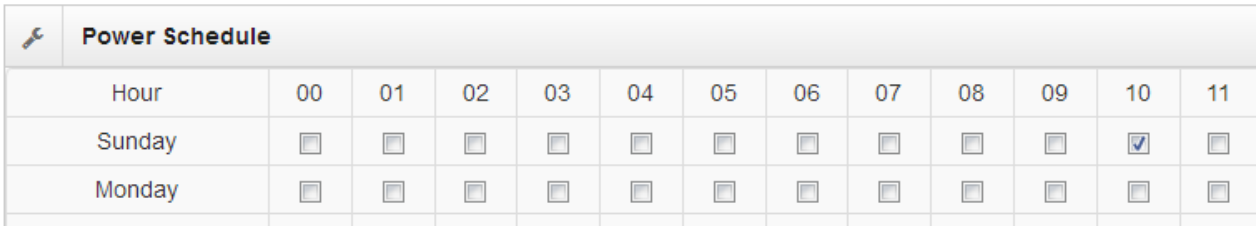
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>❶ No.:</td><td>Number of the PoE port.</td></tr>
<tr><td>❷ Enabled:</td><td>Enable or disable PoE detection.</td></tr>
<tr><td>❸ IP address:</td><td>IP address of the connected PD.</td></tr>
<tr><td>❹ Interval:</td><td>Define how often to ping the connected PD.</td></tr>
<tr><td>❺ Retry Time:</td><td>Define how many times of ping failure will be determined as the PD failed.</td></tr>
<tr><td>❻ Failure Log:</td><td>Failure record of PD detection.</td></tr>
<tr><td>❼ Failure Action:</td><td>Action to be taken when PD fails.
<table>
<tr><th>Actions</th><th>Default Setting</th></tr>
<tr><td>■ Nothing: No action.
■ Power Down: Shutdown the power of the PoE port.
■ Power On: Keep the power on with the PoE port.
■ Restart Forever: Reset the power of the PoE port continuously.
■ Restart Once: Reset once</td><td>Nothing</td></tr>
</table>
</td></tr>
</table>

	only with the PoE Port.	
❽ **Reboot Time:**	If the action is set to be Restart Forever, then Reboot Time can define how often the switch will reset the power.	

6.4 Scheduling

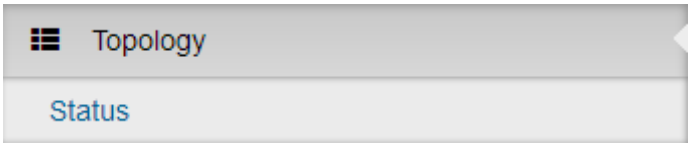


Set the PoE power-on schedule of a week.



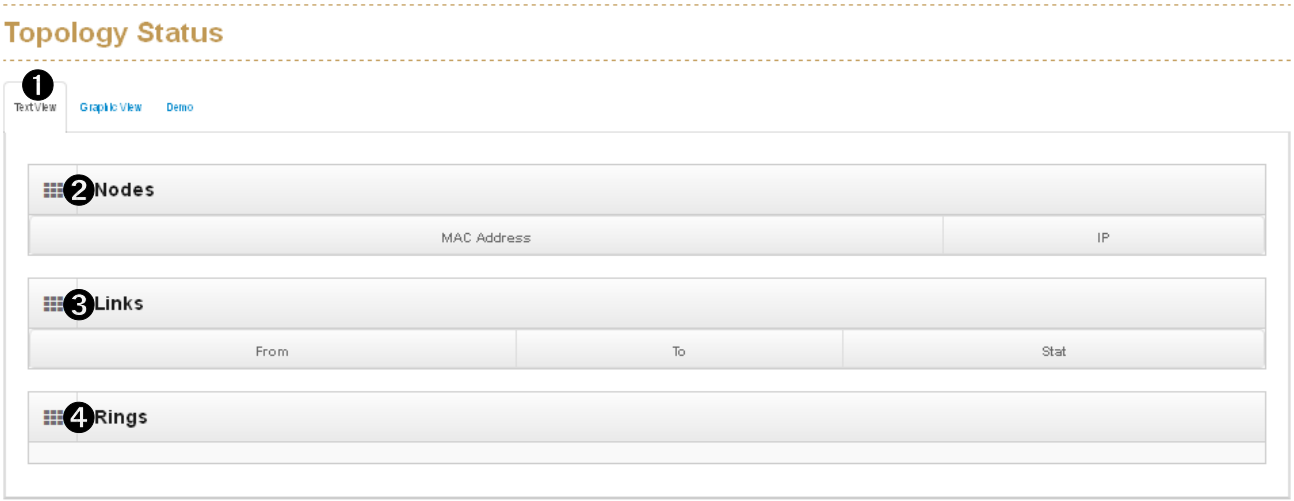
Refer to above screenshot, Sunday at 10 o'clock is ticked which means the switch will power the PD from AM10:00 to AM10:59 on Sunday.

7.Topology

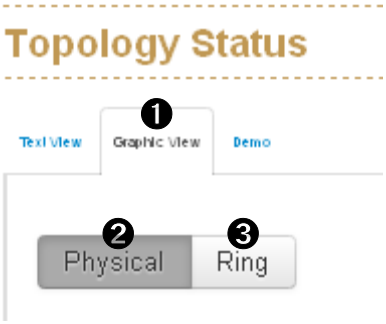


This function gives user a graphical overview of the entire network topology. However, the LLDP function of all the connected switches must be activated to work this out.

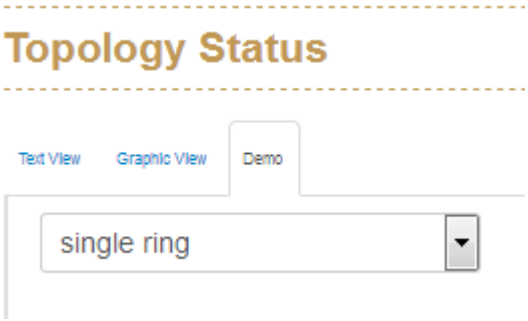
Topology Status



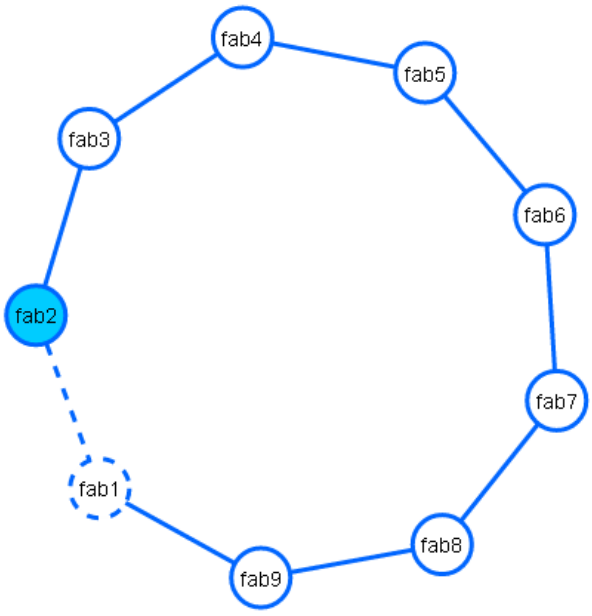
Name	Description
❶ **Text View:**	Display LLDP information of each switch by text.
❷ **Nodes:**	Show the detailed information of each node (switch), such as MAC address and IP address.
❸ **Links:**	Show the status of each connection.
❹ **Rings:**	Show the information from ITU-Ring.



Name	Description
❶ **Graphic View:**	Display graphical overview of network topology which built by the LLDP information.
❷ **Physical**:	Show only physical connections of the network.
❸ **Ring**:	Show both of physical and ITU-Ring connections of the network.



Topology Status will show the example of different topologies.



8.QoS

Quality of service (QoS) is the description or measurement of the overall performance of a service, such as a telephony or computer network or a Cloud computing service, particularly the performance seen by the users of the network. To quantitatively measure quality of service, several related aspects of the network service are often considered, such as error rates, bit rate, throughput, transmission delay, availability, jitter, etc.

In the field of computer networking and other packet-switched telecommunication networks, quality of service refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

Quality of service is particularly important for the transport of traffic with special requirements. In particular, developers have introduced technology to allow computer networks to become as useful as telephone networks for audio conversations, as well as supporting new applications with even stricter service demands.

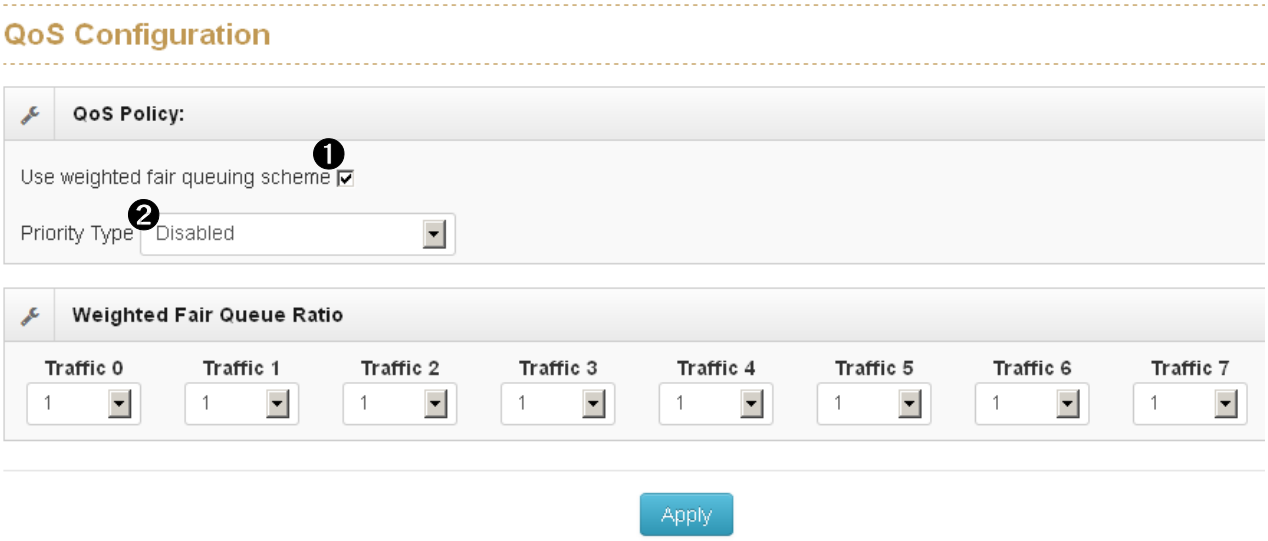
Note: This section is taken from Wiki at
https://en.wikipedia.org/wiki/Quality_of_service

QoS Policy

The hardware of Lantech switches has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the Lantech switch without being delayed by lower priority traffic. As each packet arrives in the Lantech switch, it passes through any ingress processing, and is then sorted into the appropriate queue. The switch then forwards packets from each queue. Lantech

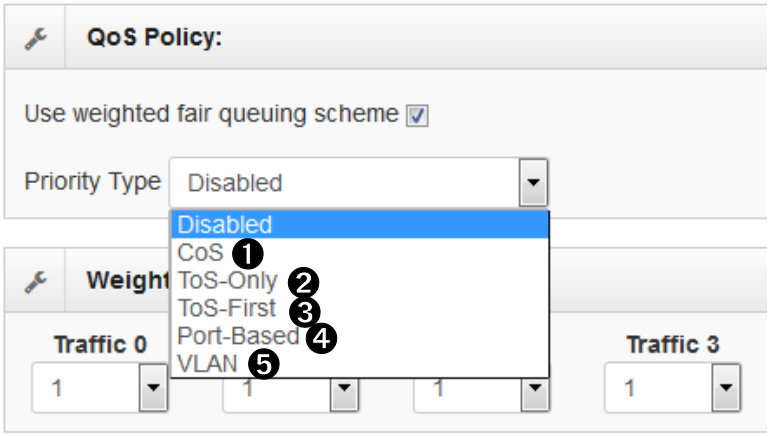
switches support two different queuing mechanisms:

- Weighted Fair Queue Ratio: This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, the Weighted Fair Queue Ratio gives high priority precedence over low priority, but in the event that high priority traffic does not reach the link capacity, lower priority traffic is not blocked.
- Strict: This method services high traffic queues first; low priority queues are delayed until no more high priority data needs to be sent. The Strict method always gives precedence to high priority over low priority.



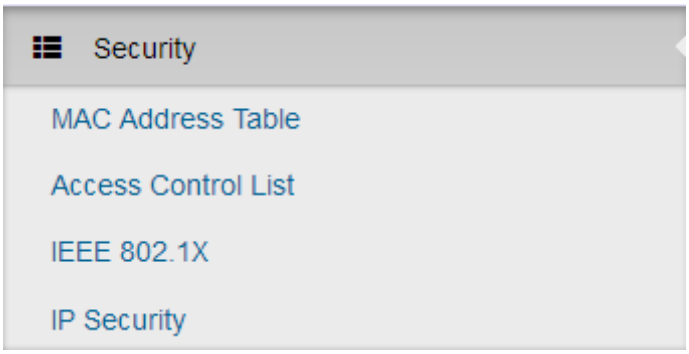
Name	Description
❶ **Using the weight fair queue scheme:**	The switch will follow 8:7:6:5:4:3:2:1 rate to process priority queue from High to lowest queue.
❷ **Priority Type:**	■ **Port-base:** the port priority will follow the default port priority that you have assigned - High, center, low, or lowest. ■ **CoS:** the port priority will only follow the CoS priority that you have assigned. ■ **ToS only:** the port priority will only follow the ToS priority that you have assigned. ■ **ToS first:** the port priority will follow the ToS priority first, and the other priority rule.

- **Port-based:** Set the priority of traffic by per port.
- **VLAN:** Set the priority of traffic by VLAN.



Name	Description
❶ **Cos:**	Set the CoS priority level 0~7.
❷ **ToS-Only:**	System provides 0~63 ToS priority level.
❸ **ToS-First:**	System provides 0~63 ToS priority level. Each level has 8 type of priority - 0~7. The default value is "1" priority for each level. When the IP packet is received, the system will check the ToS level value in the IP packet has received. For example: user set the ToS level 25 is 7. The port 1 is following the ToS priority policy only. When the packet received by port 1, the system will check the ToS value of the received IP packet. If the ToS value of received IP packet is 25 (priority = 7), and then the packet priority will have highest priority.
❹ **Port Based:**	Define the priority by switch port.
❺ **VLAN Based:**	Define the priority by VLAN tag.

9.Security



The "Security" menu contains the dialogs, displays and tables for configuring the security settings:

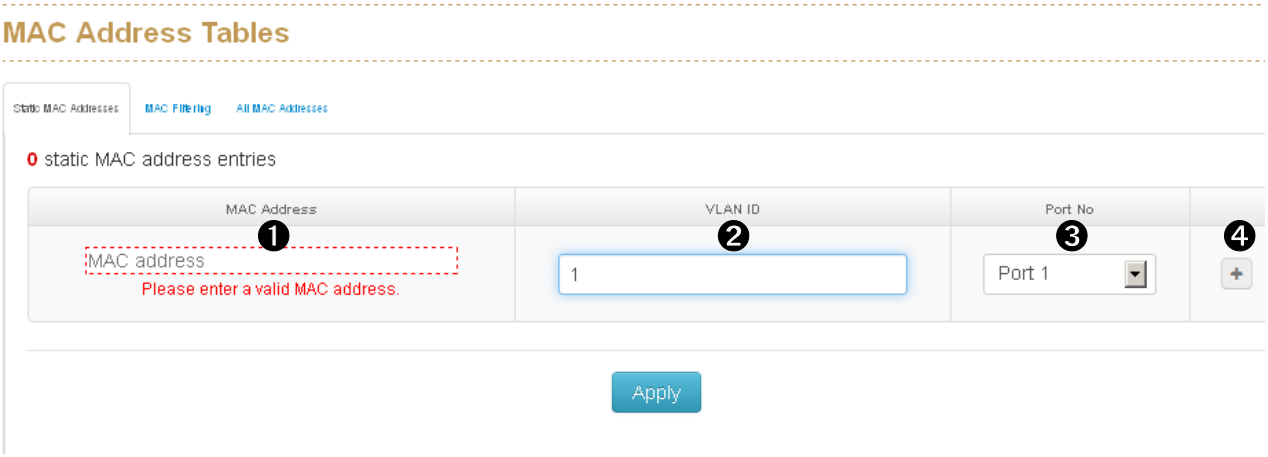
- Mac Address Tables
- Access Control List
- IEEE 802.1X Radius Server
- IP Security

9.1 MAC Address Tables

Use the MAC address table to ensure the port security.

Static MAC Address

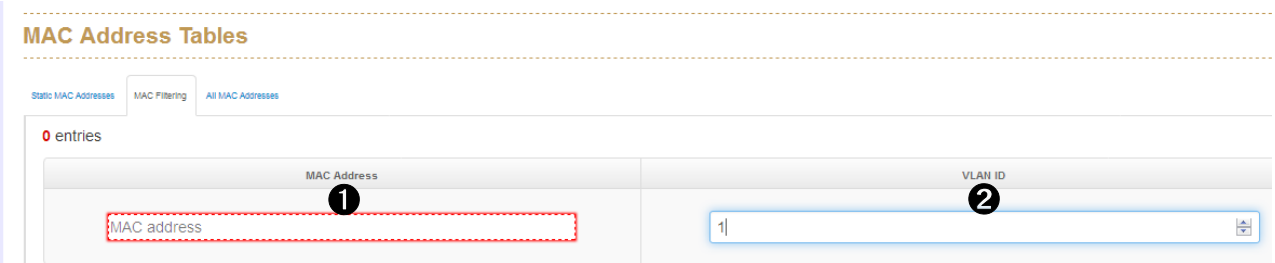
You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address.



Name	Description
❶ **Mac Address:**	Enter the MAC address of the port that should permanently forward traffic.
❷ **VLAN ID:**	Enter the corresponding VLAN ID.
❸ **Port No.:**	Drop down menu for selecting the port.
❹ **+:**	Add a new entry in static MAC address table

MAC Filtering

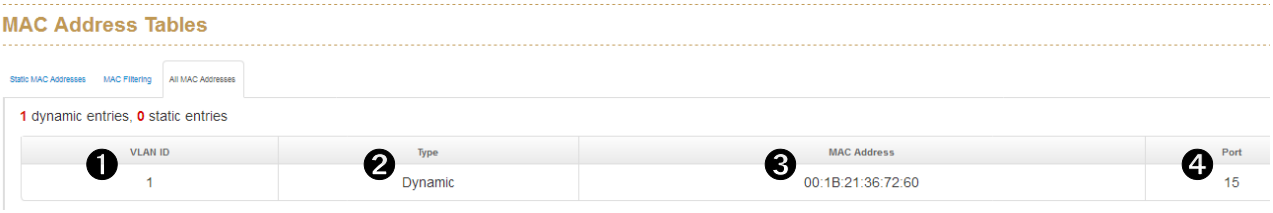
MAC Filtering helps to filter pre-configured MAC address and therefore enhances safety. You can add and delete filtering MAC address.



Name	Description
❶ **Mac Address:**	Enter the MAC address to be filtered.
❷ **VLAN ID:**	Enter the corresponding VLAN ID.

All MAC Addresses

This panel shows the source MAC address and its corresponding port of all the passing through packets.



Name	Meaning
❶ **VLAN ID:**	Show the VLAN ID.
❷ **Type:**	Dynamic or Static
❸ **Mac Address:**	MAC address of connected device or other network equipment.
❹ **Port:**	The corresponding port of the MAC address.

9.2 Access Control List

ACL can be used to deny the access from the specified IP address or MAC address.

Name	Description
❶ **Index:**	Index number of ACL rule.
❷ **Ingress/Egress:**	Set ACL is to be applied to Ingress or Egress traffic. **Options**: Ingress/Egress **Default Setting**: Ingress
❸ **Directio:**	Set ACL to check the Source or Destination address of packets. **Options**: Source/Destination **Default Setting**: Destination
❹ **Type:**	Set ACL to check the IP address or MAC address of packets.

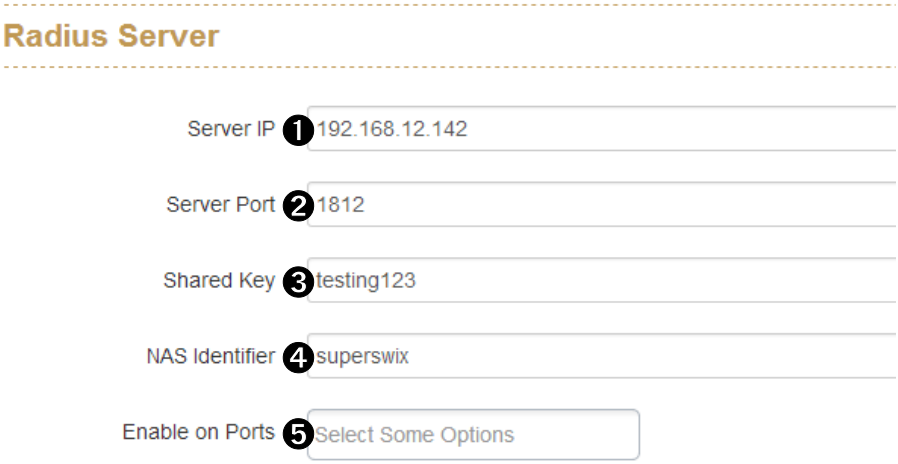
	Options	Default Setting
	IP/MAC	IP

❺ **Address:**	Set the address (MAC or IP) to be processed by ACL.
❻ **Mask:**	Set Subnet Mask.
❼ **Action:**	Action to be taken by ACL.

Actions	Default Setting
Deny/Permit	Permit

9.3 IEEE 802.1X Radius Server

IEEE 802.1X defines a protocol for client/server-based access control and authentication. The protocol restricts unauthorized clients from connecting to a LAN through ports that are open to the Internet, and which otherwise would be readily accessible. The purpose of the authentication server is to check each client that requests access to the port. The client is only allowed access to the port if the client's permission is authenticated.

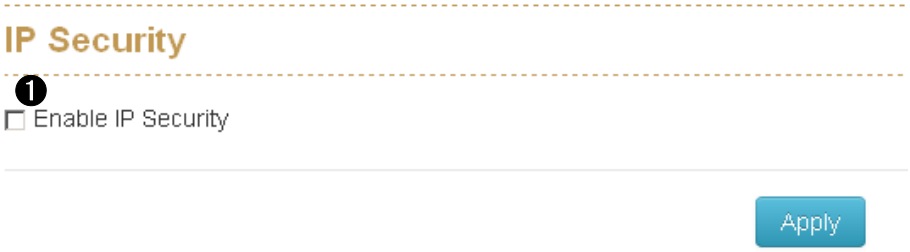


Name	Description
❶ **Server IP:**	IP address of the authentication server.
❷ **Server Port:**	UDP port number used by the authentication server to authenticate.
❸ **Shared Key:**	Key of server for authentication

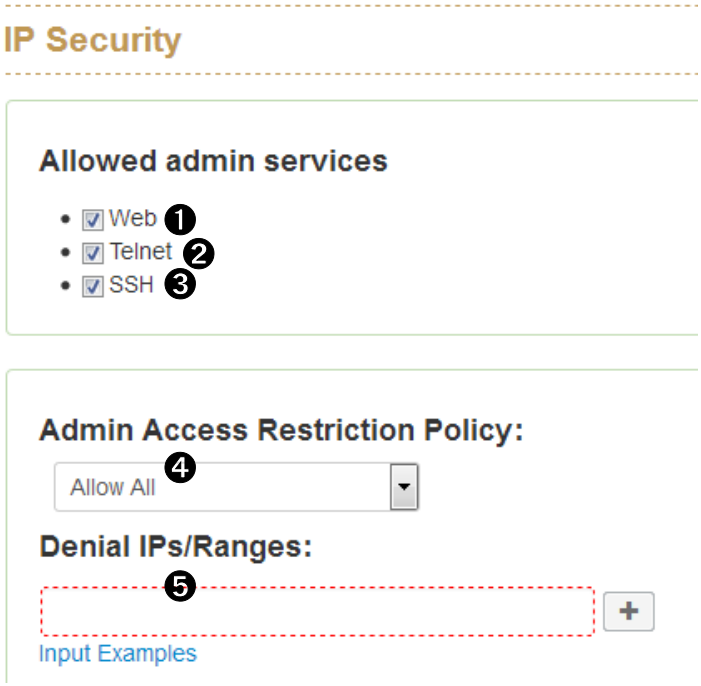
❹ **NAS Identifier:**	A string used to identify this switch.
❺ **Enable on Ports:**	Select specific port and configure the authorization state.

9.4 IP Security

IP security function allows user to assign 20 specific IP addresses that have permission to access the switch through the web browser for the securing switch management.

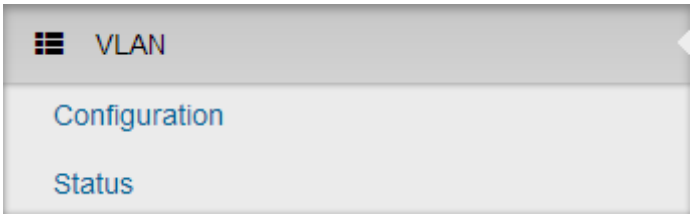


Name	Description
❶ **Enable IP Security:**	When IP Security is activated, the options (Web, Telnet and SSH) of Allowed admin services will be available.



<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>❶ Web:</td><td>Check this option to make web access available for further setting.</td></tr>
<tr><td>❷ Telnet:</td><td>Check this option to make Telnet access available for further setting.</td></tr>
<tr><td>❸ SSH:</td><td>Check this option to make SSH access available for further setting.</td></tr>
<tr><td>❹ Admin Access Restriction Policy:</td><td>Following IP list should be allowed or denied with web/Telnet/SSH access.
<table>
<tr><th>Actions</th><th>Default Setting</th></tr>
<tr><td>Allow All/Deny All</td><td>Allow All</td></tr>
</table>
</td></tr>
<tr><td>❺ IPs/ Ranges:</td><td>Assign up to 20 specific IP addresses to be allowed or denied to access the admin service(s).</td></tr>
</table>

10. VLAN



A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic. VLANs work through tags within network packets and tag handling in networking systems - recreating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks. In this way, VLANs can keep networks separate despite being connected to the same network, and without requiring multiple sets of cabling and networking devices to be deployed.

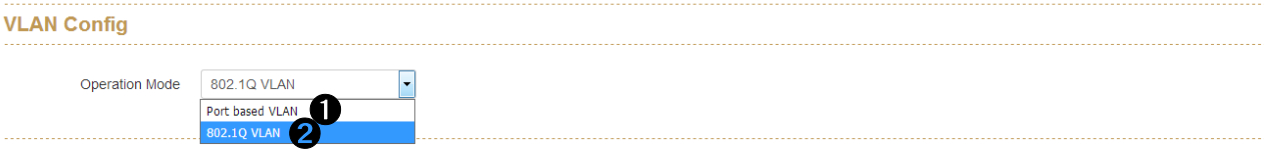
VLANs allow network administrators to group hosts together even if the hosts are not on the same network switch. This can greatly simplify network design and deployment, because VLAN membership can be configured through software. Without VLANs, grouping hosts according to their resource needs necessitates the labor of relocating nodes or rewiring data links. It also has benefits in allowing networks and devices that must be kept separate to share the same physical cabling without interacting, for reasons of simplicity, security, traffic management, or economy. For example, a VLAN could be used to separate traffic within a business due to users, and due to network administrators, or between types of traffic, so that users or low priority traffic cannot directly affect the rest of the network's functioning. Many Internet hosting services use VLANs to separate their customers' private zones from each other, allowing each customer's servers to be grouped together in a single network segment while being located anywhere in their datacenter. Some precautions are needed to prevent traffic "escaping" from a given VLAN, an exploit known as VLAN hopping.

The VLAN membership configuration for the switch can be monitored and modified here. Up to 4094 VLANs are supported. This panel allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

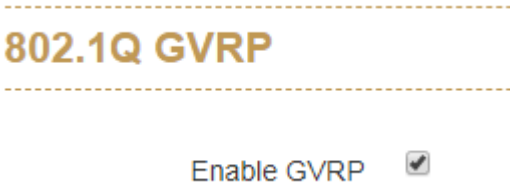
Note: This section is taken from Wiki at https://en.wikipedia.org/wiki/Virtual_LAN

10.1 Operation Mode

Set Port based VLAN or 802.1Q VLAN



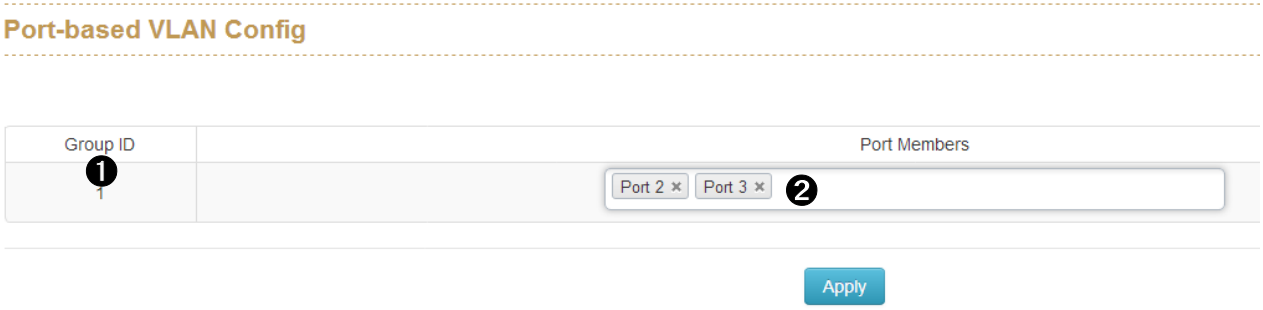
Name	Description
❶ **Port based VLAN:**	Set isolated VLAN group by port
❷ **802.1Q VLAN:**	Set isolated VLAN group by VLAN tag



GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network . GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices.

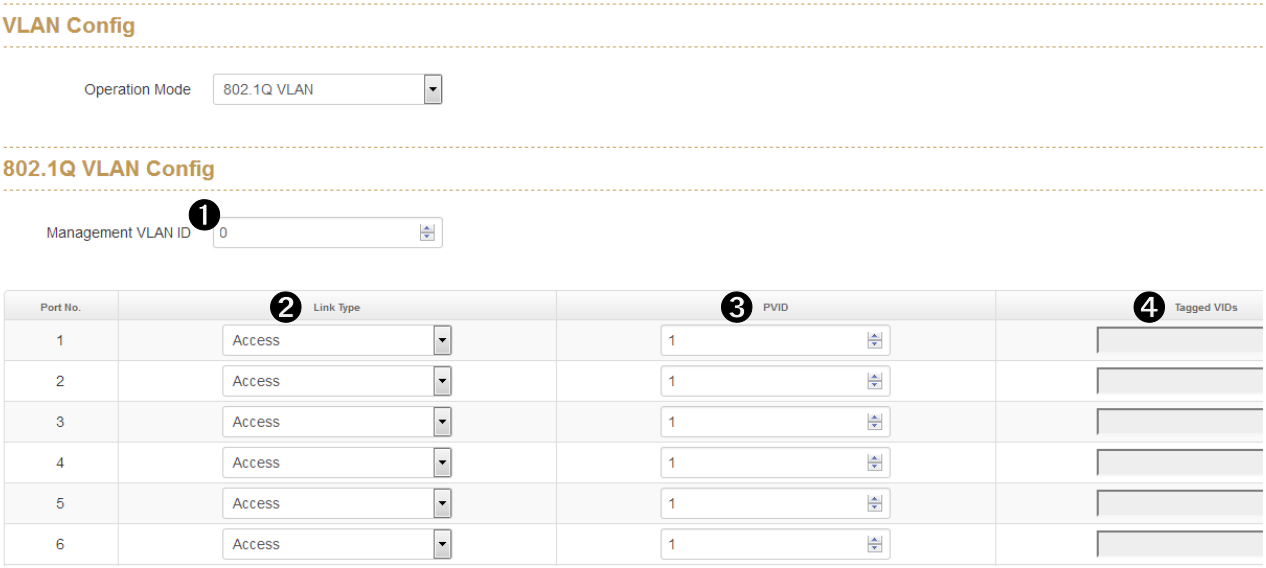
Enable GVRP option with all switches, those switch will synchronize the setting of VLAN trunk port with each other.

10.2 Port-based VLAN Config



Name	Description
❶ **Group ID:**	ID of VLAN Group
❷ **Port Members:**	Select switch ports to build isolated VLAN group

10.3 802.1Q VLAN Config



Name	Description
❶ **Management VLAN ID:**	Define which VLAN group member can access the switch, 0 means all VLAN group
❷ **Link Type:**	There are 3 types of link type: 1. **Access Link:** A segment which provides the link path for one

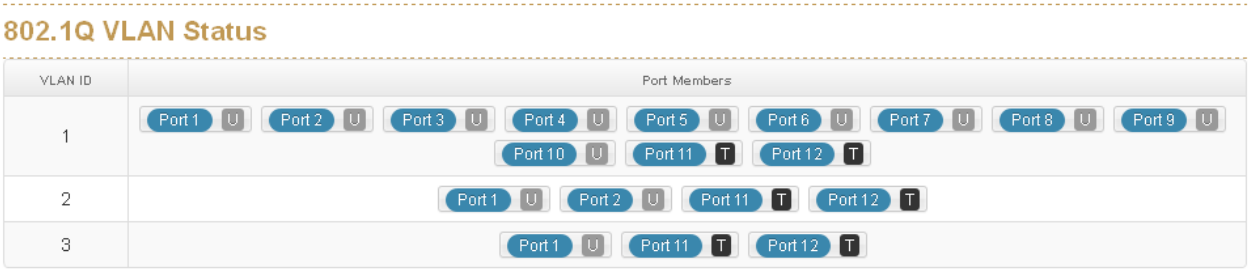
or more stations to the VLAN-aware device. An Access Port (untagged port), connected to the access link, has an untagged VID (also called PVID). After an untagged frame gets into the access port, the switch will insert a four-byte tag in the frame. The contents of the last 12-bit of the tag is untagged VID. When this frame is sent out through any of the access port of the same PVID, the switch will remove the tag from the frame to recover it to what it was. Those ports of the same untagged VID are regarded as the same VLAN group members.

2. **Trunk Link:** A segment which provides the link path for one or more VLAN-aware devices (switches). A Trunk Port, connected to the trunk link, has an understanding of tagged frame, which is used for the communication among VLANs across switches. Which frames of the specified VIDs will be forwarded depends on the values filled in the Tagged VID column field. Please insert a comma between two VIDs.
3. **Hybrid Link:** A segment which consists of Access and Trunk links. The hybrid port has both the features of access and trunk ports. A hybrid port has a PVID belonging to a particular VLAN, and it also forwards the specified tagged-frames for the purpose of VLAN communication across switches.
4. **QinQ Tunnel:** A Q-in-Q VLAN tunnel enables a service provider to segregate the traffic of different customers in their infrastructure, while still giving the customer a full range of VLANs for their internal use by adding a second 802.1Q tag to an already tagged frame.
5. **QinQ Trunk:** When Q-in-Q tunneling is enabled, trunk interfaces are assumed to be part of the service provider or data center network. Access interfaces are assumed to be customer-facing and accept both tagged and untagged frames.

	Note: *Because the access port doesn't have an understanding of tagged frame, the column field of Tagged VID is not available.* ***Note:*** *A trunk port doesn't insert tag into an untagged frame, and therefore the untagged VID column field is not available. It's not necessary to type '1' in the tagged VID. The trunk port will forward the frames of VLAN 1. The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.*
❸ **PVID:**	Indicates the VLAN ID of this particular VLAN.
❹ **Tagged VID:**	This column will be editable when Link Type is set to Trunk Link or Hybrid Link. Assign a number in the range between 1 with 4094.

802.1Q VLAN Status

Display the status of each VLAN group.



Icon	Description
U	VLAN untagged port (Access port)
T	VLAN trunk port

10.4 QinQ TPID Table

802.1Q adds a 32-bit field between the source MAC address and the EtherType fields of the original frame. The minimum frame size is left unchanged at 64 bytes. The maximum frame size is extended from 1,518 bytes to 1,522 bytes. Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI). The TCI field is further divided into PCP, DEI, and VID.

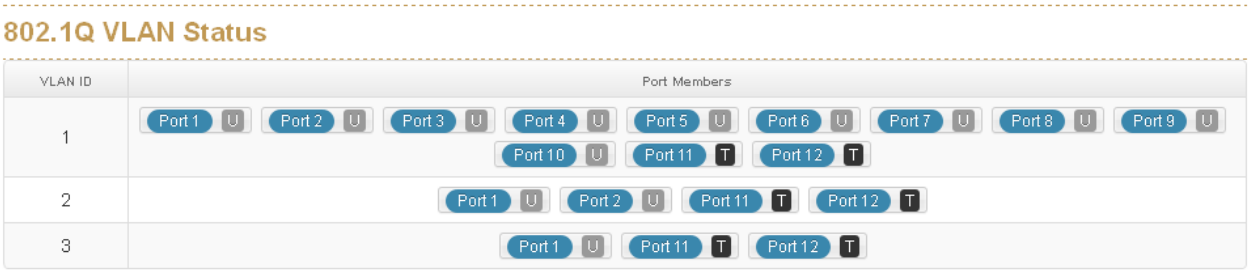
802.1Q tag format

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID

Usually we would suggest to set TPID as 88a8.

10.5 802.1Q VLAN Status

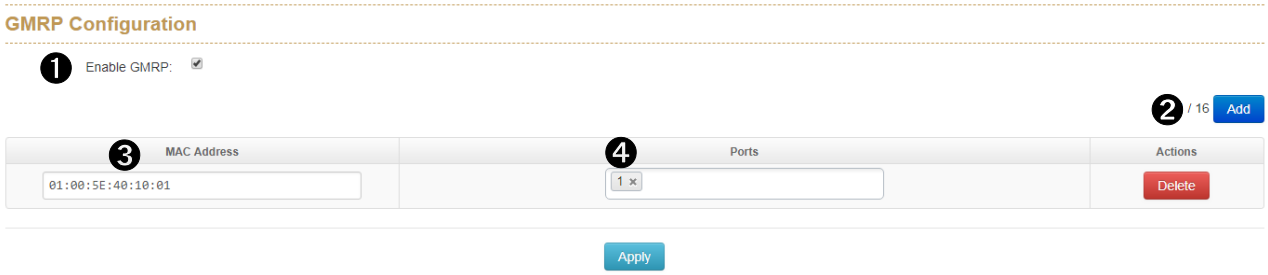
Display the status of each VLAN group.



Icon	Description
U	VLAN untagged port (Access port)
T	VLAN trunk port

11. GMRP

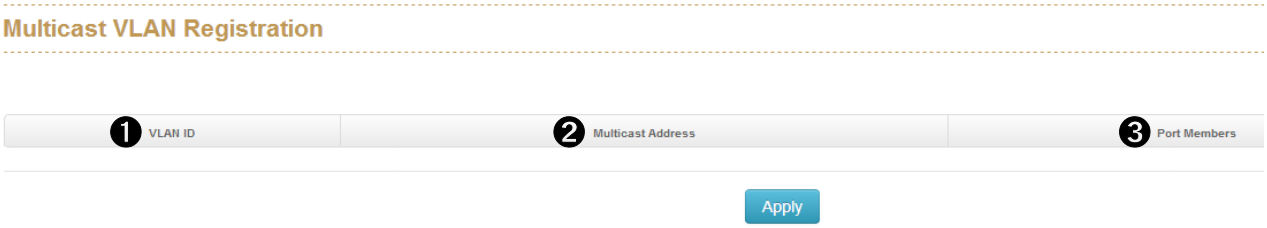
GARP was defined by the IEEE 802.1 working group to provide a generic framework allowing bridges (or other devices like switches) to register and de-register attribute values, like VLAN identifiers and multicast group membership. GARP defines the architecture, rules of operation, state machines and variables for the registration and de-registration of attribute values. GARP was used by two applications: GARP VLAN Registration Protocol (GVRP) for registering VLAN trunking between multilayer switches, and by the GARP Multicast Registration Protocol (GMRP). The latter two were both mostly enhancements for VLAN-aware switches per definition in IEEE 802.1Q.



Name	Description
❶ **Enable GMRP:**	Enable GMRP option.
❷ **Add:**	Press Add to edit new entry of GMRP table
❸ **MAC address:**	MAC address of dedicated Multicast stream.
❹ **Ports**	Dedicated port which will be responsible to redirect dedicated Multicast stream.

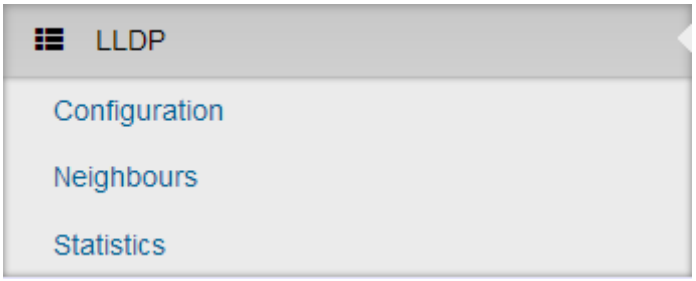
12. Multicast VLAN Registration (MVR)

MVR allows static multicast forwarding table to process the multicast stream from legacy device which doesn't support IGMP protocol.



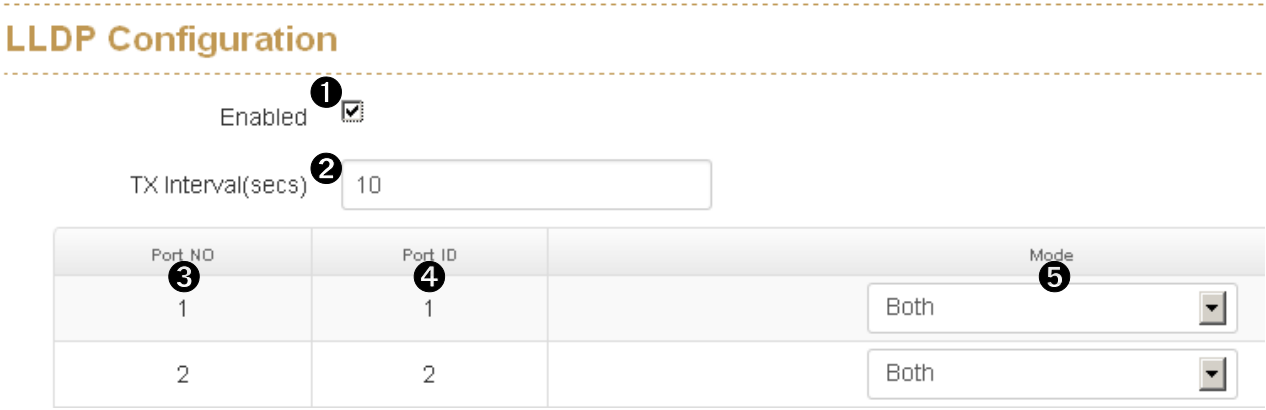
Name	Description
❶ **VLAN ID:**	Specify the Multicast VLAN ID.
❷ **Multicast Addresses:**	Multicast stream of the address is to be forwarded to Port Members.
❸ **Port Members:**	Ports that will receive multicast stream.

13. LLDP



The Link Layer Discovery Protocol (LLDP) is a link layer protocol in the Internet Protocol Suite used by switches to propaganda their identity, capabilities, and neighbors on wired Ethernet network. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in IEEE 802.1AB and IEEE 802.3-2012 section 6 clause 79.

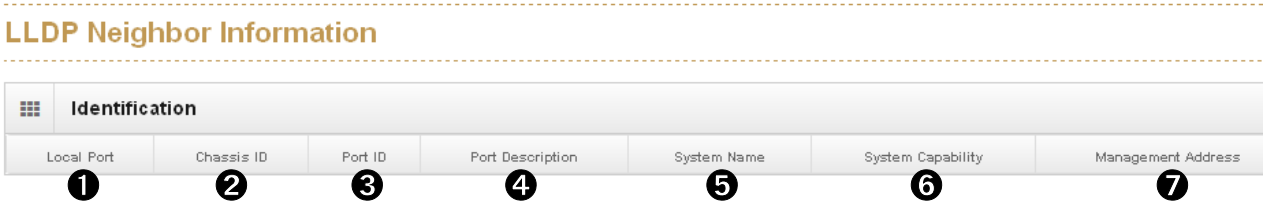
13.1 LLDP Configuration



Name	Description
❶ **Enabled:**	Enabled the switch to send out LLDP information, and will analyze LLDP information received from neighbours.
❷ **Tx Interval:**	The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-dated. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 3600 seconds.

❸ **Port No:**	The switch port number for LLDP mode.
❹ **Port ID:**	Input identification number of LLDP port.
❺ **Mode:**	Select LLDP mode. ■ **Rx only:** The switch port will only get LLDP information from neighbors. ■ **Tx only:** The switch port will only send out LLDP information to neighbors. ■ **Disabled:** The switch port will not send out LLDP information, and will drop LLDP information received from neighbors. ■ **Both:** The switch port will send out LLDP information, and will analyze LLDP information received from neighbors.

13.2 LLDP Neighbor Information



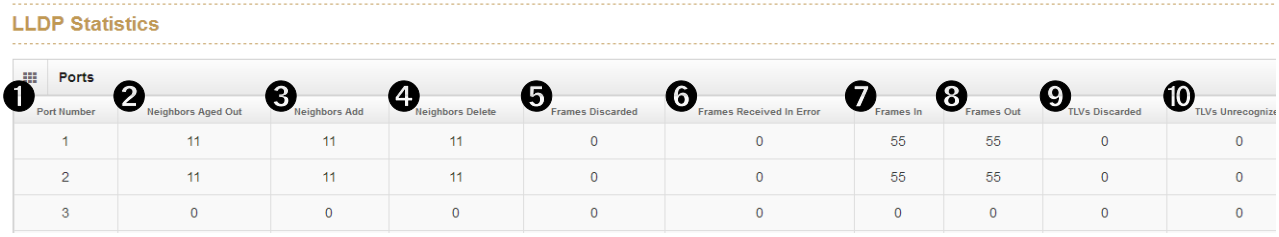
This page provides a status-quo for all LLDP neighbors. The table shows the LLDP neighbor information that contains the followings:

Name	Description
❶ **Local Port:**	The port which the LLDP frame was received.
❷ **Chassis ID:**	The identification of the neighbor's LLDP frames.
❸ **Port ID:**	The identification number of the neighbor port.
❹ **Port Description:**	The description that is advertised by the neighbor unit.
❺ **System Name:**	The name advertised by the neighbor unit.
❻ **System**	It describes the neighbor unit's capabilities which include the

Capabilities:	followings: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is shown (+). If the capability is disabled, the capability is shown (-).
❼ **Management Address:**	Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

13.3 LLDP Neighbor Information

This page provides an overview of all LLDP traffic.

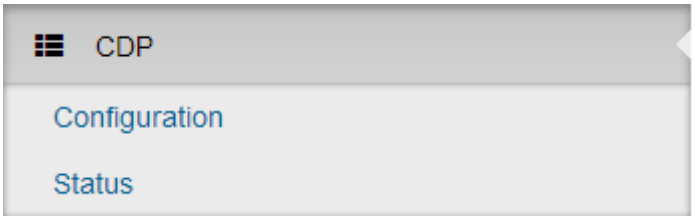


There are two types of counters are shown. **Total** is the counters that refer to the whole stack, switch, while **Ports** refer to per port counters for the selected switch.

Name	Description
❶ **Port Number:**	The port which LLDP frames are received or transmitted.

❷ **Neighbors Aged Out:**	Shows the number of entries deleted due to Time-To-Live expiration
❸ **Neighbors Added:**	Shows the number of new entries added since switch reboot.
❹ **Neighbors Deleted:**	Shows the number of new entries deleted since switch reboot.
❺ **Frames Discarded:**	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and will be discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.
❻ **Frames Received In Error:**	The number of received LLDP frames contains some kind of error.
❼ **Frames In:**	The number of LLDP frames received on the port.
❽ **Frames Out:**	The number of LLDP frames transmitted on the port.
❾ **TLVs Discarded:**	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
❿ **TLVs Unrecognized:**	The number of well-formed TLVs, but with an unknown type value.

14. Cisco Discovery Protocol (CDP)



Cisco Discovery Protocol (CDP) is a proprietary Data Link Layer protocol developed by Cisco Systems. It is used to share information about other directly connected Cisco equipment, such as the operating system version and IP address. CDP can also be used for On-Demand Routing, which is a method of including routing information in CDP announcements so that dynamic routing protocols do not need to be used in simple networks.

Cisco devices send CDP announcements to the multicast destination address 01-00-0c-cc-cc-cc, out each connected network interface. These multicast frames may be received by Cisco switches and other networking devices that support CDP into their connected network interface. This multicast destination is also used in other Cisco protocols such as Virtual Local Area Network (VLAN) Trunking Protocol (VTP). By default, CDP announcements are sent every 60 seconds on interfaces that support Subnetwork Access Protocol (SNAP) headers, including Ethernet, Frame Relay and Asynchronous Transfer Mode (ATM). Each Cisco device that supports CDP stores the information received from other devices in a table that can be viewed using the show cdp neighbors command. This table is also accessible via Simple Network Management Protocol (SNMP). The CDP table information is refreshed each time an announcement is received, and the holdtime for that entry is reinitialized. The holdtime specifies the lifetime of an entry in the table - if no announcements are received from a device for a period in excess of the holdtime, the device information is discarded (default 180 seconds).

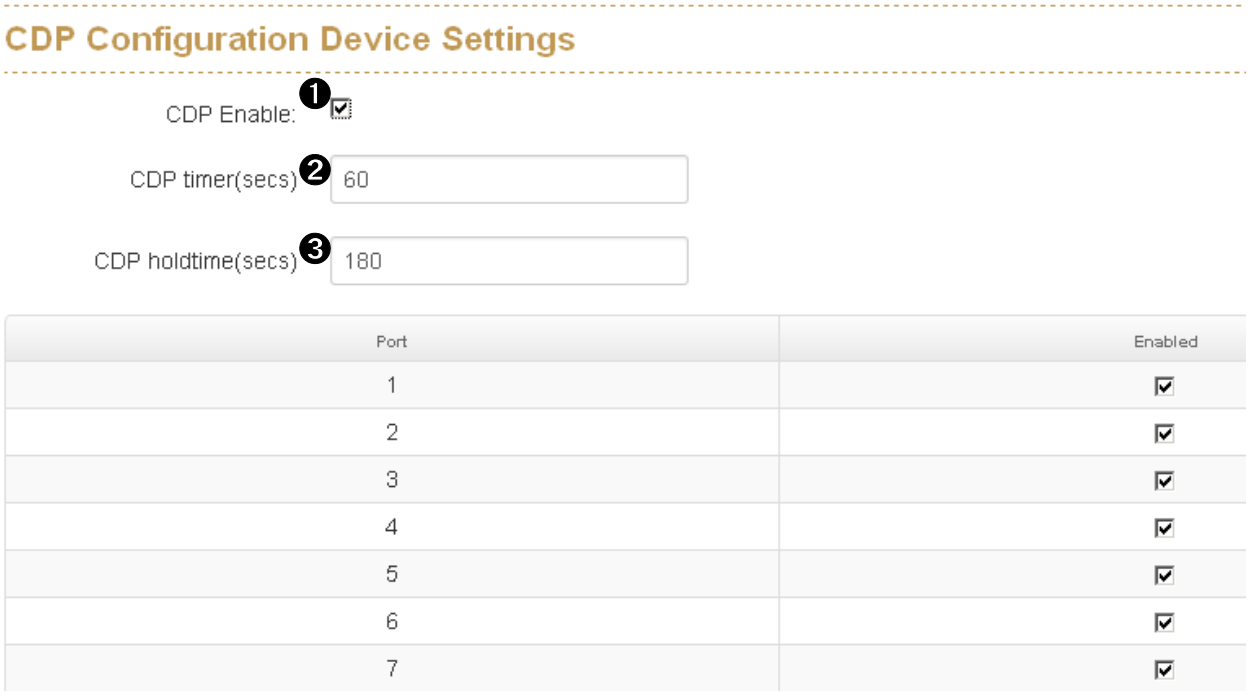
The information contained in CDP announcements varies by the type of device and the version of the operating system running on it. This information may include the operating system version, hostname, every address (i.e. IP address) from all protocol(s) configured on the port where CDP frame is sent, the port identifier from

which the announcement was sent, device type and model, duplex setting, VTP domain, native VLAN, power draw (for Power over Ethernet devices), and other device specific information. The details contained in these announcements are easily extended due to the use of the type-length-value (TLV) frame format.

Note: Cisco is registered trademarks of Cisco Systems in the United States and/or other countries.

The above info is taken from Wiki at
https://en.wikipedia.org/wiki/Cisco_Discovery_Protocol

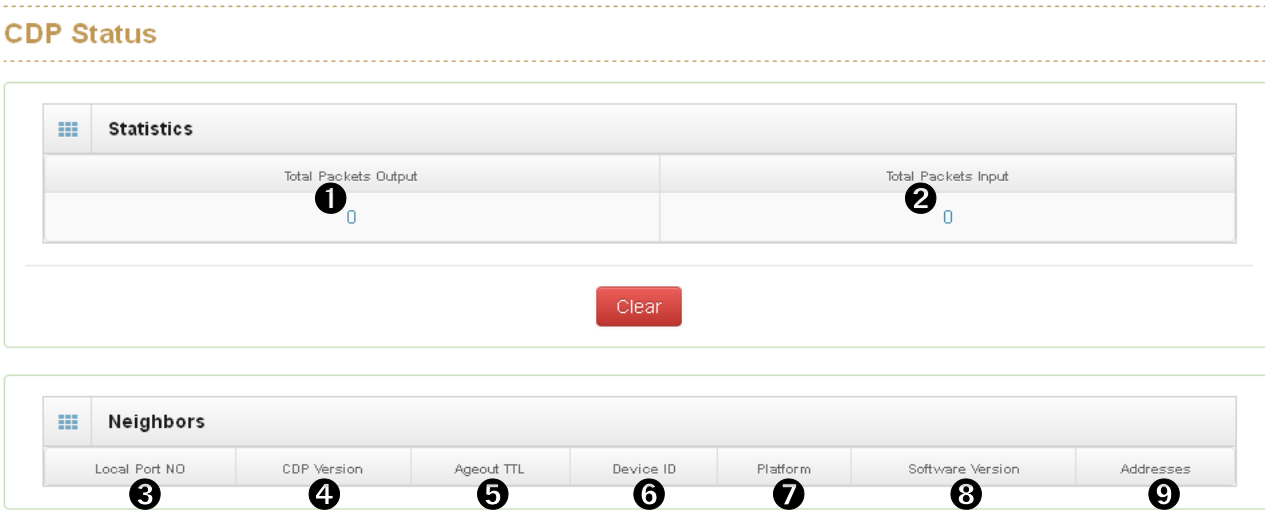
14.1 CDP Configuration Device Settings



Name	Description
❶ **CDP Enabled:**	Enabled the switch to send out CDP information, and will analyze CDP information received from neighbors.
❷ **CDP Timer (secs):**	The switch periodically transmits CDP frames to its neighbours for having the network discovery information up-to-dated. The interval between each CDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 3600 seconds.

❸ **CDP Holdtime (secs):**	Each CDP frame contains information about how long the information in the CDP frame shall be considered valid. The hold-time between each CDP frame is determined by the **Tx Holdtime** value. Valid values are restricted to 5 - 3600 seconds.

14.2 CDP Status



14.2.1. Statistics

Name	Description
❶ **Total Packets Output:**	The number of CDP frames transmitted on the switch.
❷ **Total Packets Input:**	The number of CDP frames received on the switch.

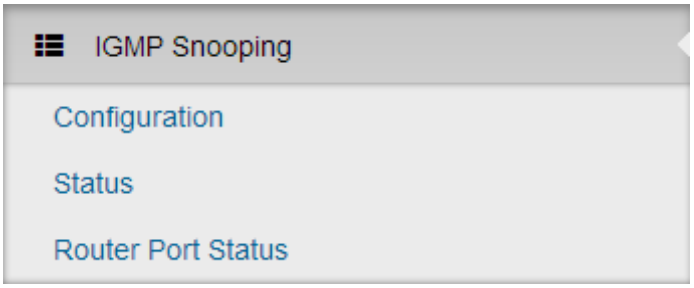
14.2.2. Neighbors

This page provides a status-quo for all CDP neighbors. The table shows the CDP neighbor information that contains the followings:

Name	Description
❸ **Local Port NO:**	The port on which the CDP frame was received.

❹ **CDP Version:**	CDP version advertised by the neighbor unit.
❺ **Ageout TTL:**	The ageout Time-To-Live advertised by the neighbor unit.
❻ **Device ID:**	The identification number of the neighbor's CDP frames.
❼ **Platform:**	The description advertised by the neighbor unit.
❽ **Software Version:**	The software version advertised by the neighbor unit.
❾ **Addresses:**	The neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

15. IGMP Snooping

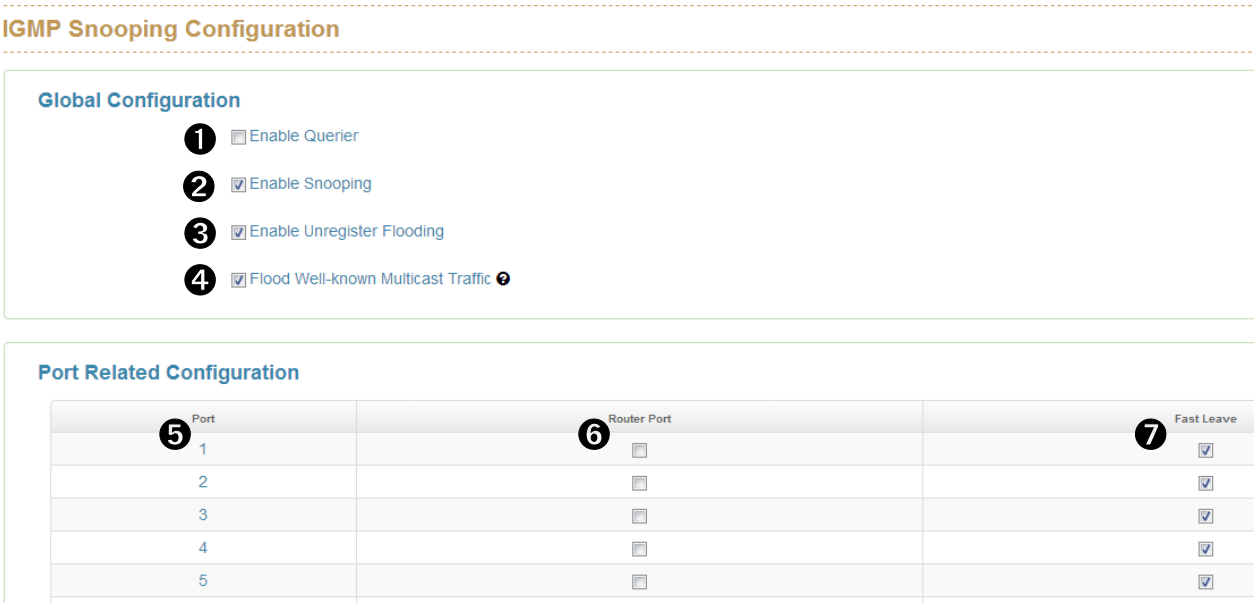


By default, all Multicast traffic should be blocked until requested by a Multicast group member. (Default behavior depends on switch manufacturer.) The master of the IGMP filter lists is the router or switch that is configured to act as the IGMP Querier. The responsibility of the Querier is to send out IGMP group membership queries on a timed interval, to retrieve IGMP membership reports from active members, and to allow updating of the group membership tables.

Without IGMP Querying/Snooping, Multicast traffic is treated in the same manner as a Broadcast transmission, which forwards packets to all ports on the network. With IGMP Querying/Snooping, Multicast traffic is only forwarded to ports that are members of that Multicast group. IGMP Snooping generates no additional network traffic, which significantly reduces the Multicast traffic passing through your switch.

Lantech switches support IGMP Snooping that can snoop IGMP Query, report, and leave (IGMP version 2) between Multicast switches and Multicast hosts to determine the Multicast group membership. IGMP snooping function is able to check IGMP packets passing through the network, generate the table holding the member ports for each a multicast group.

15.1 IGMP Snooping Configuration



15.1.1. Global Configuration

Name	Description
❶ **Enabled Querier:**	Enable IGMP Querier with switch.
❷ **Enabled Snooping:**	Enable IGMP Snooping with switch.
❸ **Enable Unregister Flooding:**	Set switch to flood all unregistered Multicast data.
❹ **Flood Well-known Multicast Traffic:**	Set switch to flood all dedicated Multicast data. Please refer to help file for info about dedicated Multicast data

Help file of IGMP Snooping Configuration

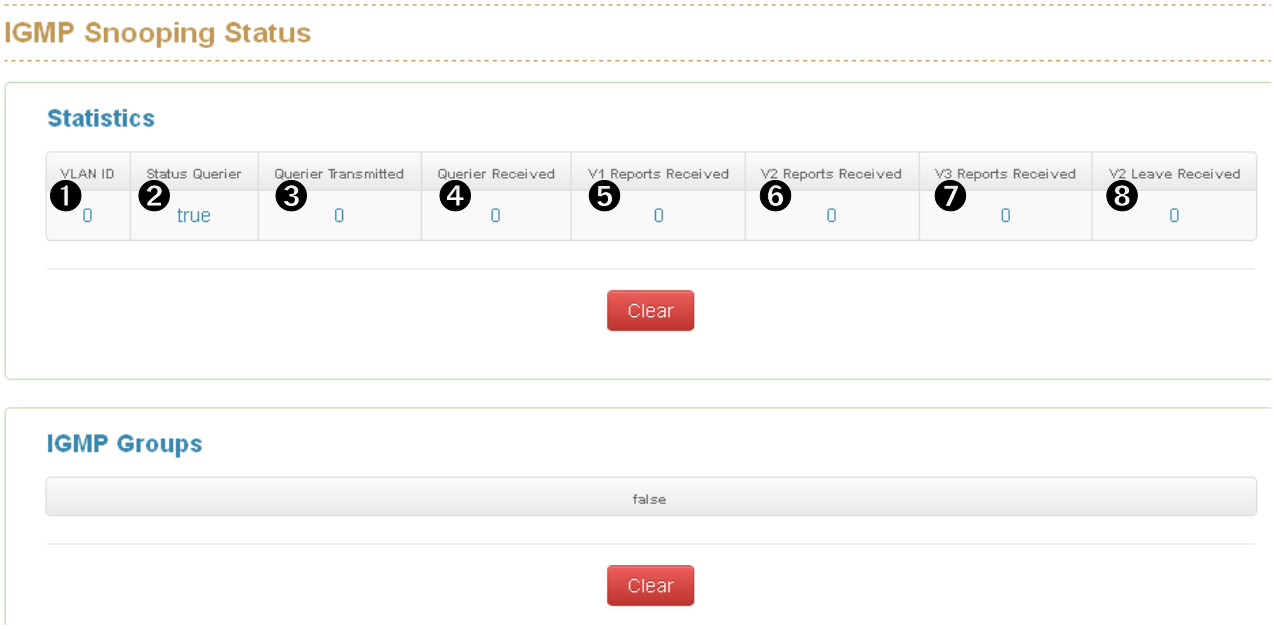
15.1.2. Port Related Configuration

Name	Description
❺ **Port:**	The switch port number
❻ **Router Port:**	Switch will forward all Multicast stream to router port
❼ **Fast Leave:**	Enable the fast leave on the port.

Fast Leave: A device sends IGMP leave packet (IGMP v2) to switch, the switch then sends a group query to confirm if any device (host) is left without response.

15.2 IGMP Snooping Status

This page provides IGMP Snooping status.



15.2.1. Statistics

Name	Description
❶ **VLAN ID:**	The VLAN ID of the entry.
❷ **Status Querier:**	Shows the Querier status is "ACTIVE" or "IDLE".
❸ **Queries Transmitted:**	The number of Transmitted Queries.
❹ **Queries Received:**	The number of Received Queries.
❺ **V1 Reports Received:**	The number of Received IGMP V1 Reports.
❻ **V2 Reports Received:**	The number of Received IGMP V2 Reports.
❼ **V3 Reports Received:**	The number of Received IGMP V3 Reports.

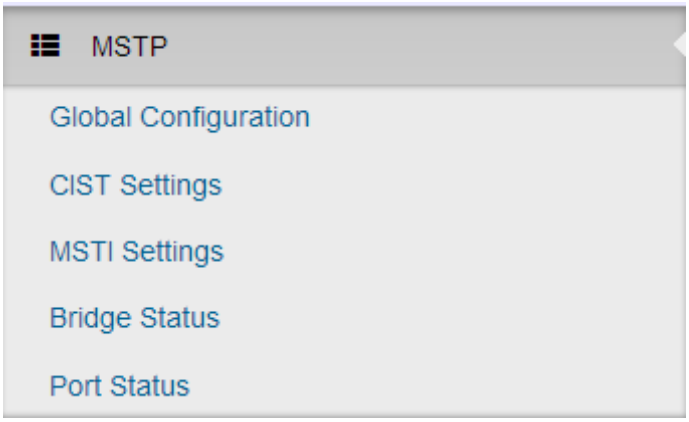
❽ **V2 Leaves Received:**	The number of Received IGMP V2 Leaves.

15.2.2. IGMP Groups

Entries in the IGMP group table is shown on this page

Name	Description
❶ **VLAN ID:**	VLAN ID of the IGMP group
❷ **Multicast Addresses:**	Multicast address of the IGMP group
❸ **Port Members:**	Ports under this IGMP group
❹ **Membership Interval:**	The IGMP table refresh time. The default interval time is 260 seconds

16. MSTP



The Spanning Tree Protocol (STP) is a network protocol that builds a logical loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails. This is done without the danger of bridge loops, or the need for manual enabling or disabling of these backup links.

STP creates a spanning tree within a network of connected layer-2 bridges, and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

Within STP, the detection and reconfiguration of network topology (connection lost, add a new switch etc) will takes some time – like 30-50 seconds. However, many time-sensitive applications cannot tolerate such delay of network down time, Rapid Spanning Tree Protocol (RSTP) was conceived to overcome this problem (RSTP takes 5-6 seconds to update and re-configure the new network topology/ routes).

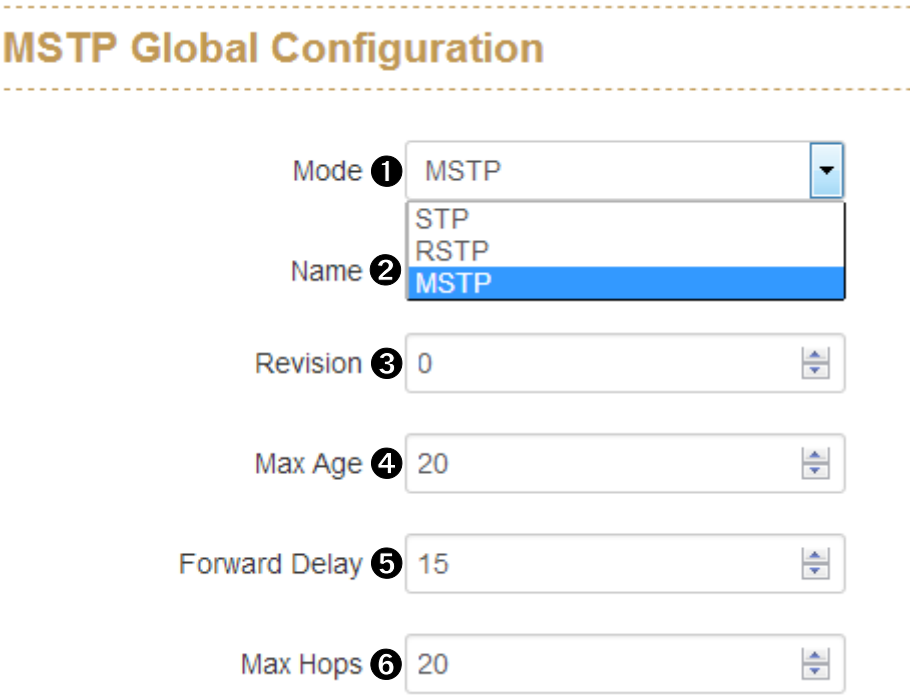
In RSTP, link status of each port is monitored pro-actively (instead of waiting for the BPDU messages) to detect network topology changes for achieving faster reaction. RSTP is backward compatible with STP switches.

MSTP (Multiple Spanning Tree Protocol) can map a group of VLAN's into a single Multiple Spanning Tree instance (MSTI), i.e. the Spanning Tree Protocol is applied

separately for a set of VLAN's instead of the whole network. Different root switches and different STP parameters can be individually configured for each MSTI, so one link can be active for one MSTI and the other link active for the second MSTI, this enables some degree of load-balancing and in general two MSTI's are used in the network for easier implementation.

Note: This section is taken from Wiki at https://en.wikipedia.org/wiki/Spanning_Tree_Protocol

16.1 MSTP Global Configuration



Name	Description
❶ **Mode:**	Select STP or RSTP or MSTP redundancy protocol for network.

Variants	Default Setting
STP, RSTP, MSTP	MSTP

❷ **Name:**	MSTP name for purpose of identifying VLAN to MSTI mapping. Bridges must match the name and revision, as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name column is up to 32 characters.

❸ **Revision:**	The revision of the MSTP configuration named above. This must be an integer between 0 and 65535.
❹ **Max Age:**	The maximum age time of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.
❺ **Forward Delay:**	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
❻ **Max Hop :**	The initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

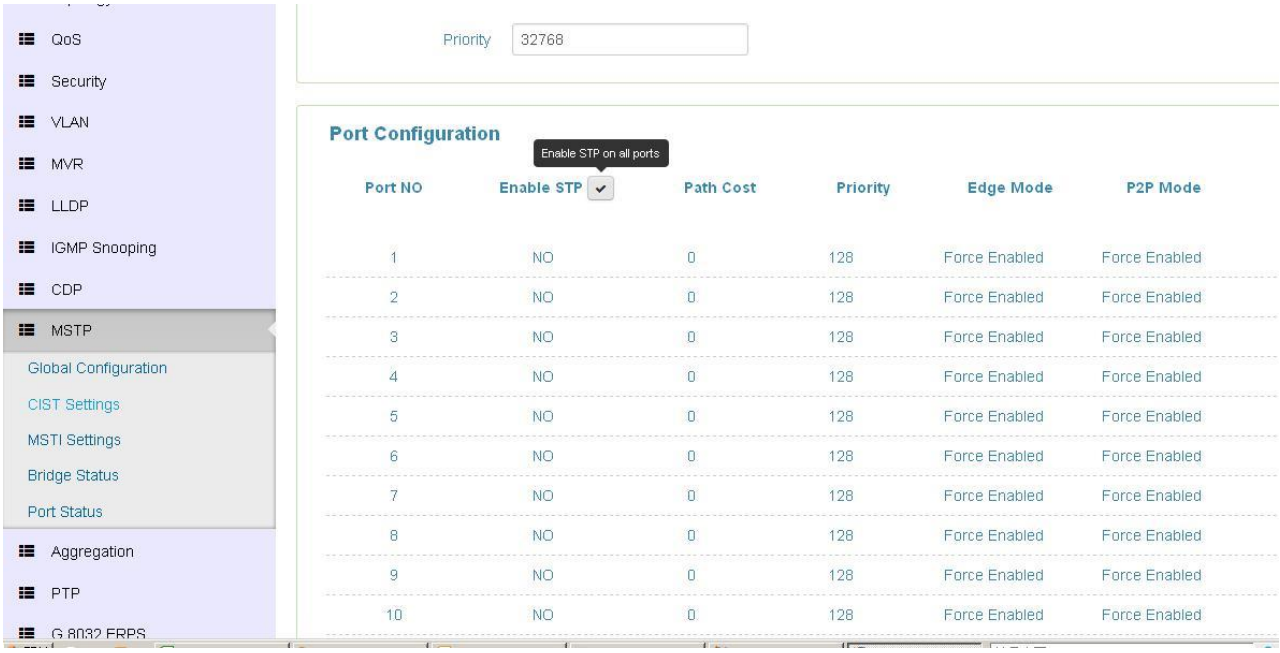
16.2 CIST Settings

How to enable STP/RSTP

A. Select STP or RSTP in MSTP Global Configuration

B. Press icon to enable STP under CIST Settings

Note: The default was disabled with all ports.

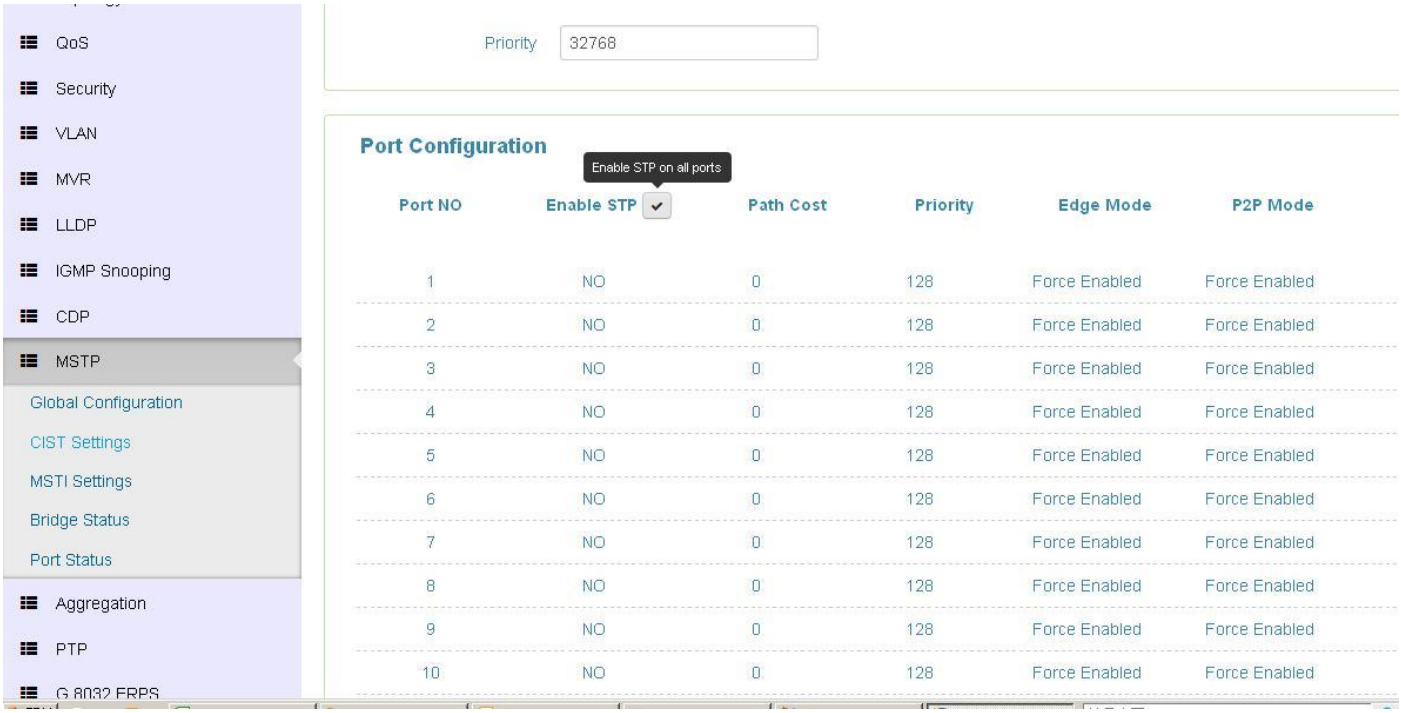


How to enable MSTP

A. Select MSTP in MSTP Global Configuration

B. Press icon to enable STP under CIST Settings

Note: The default was disabled with all ports.

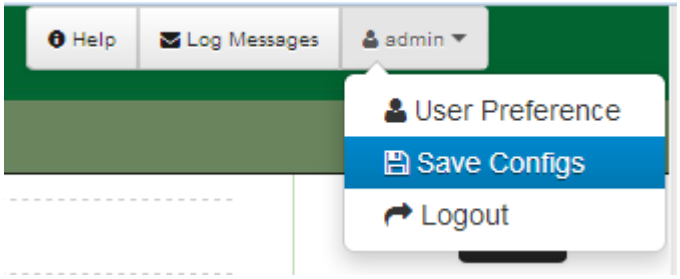


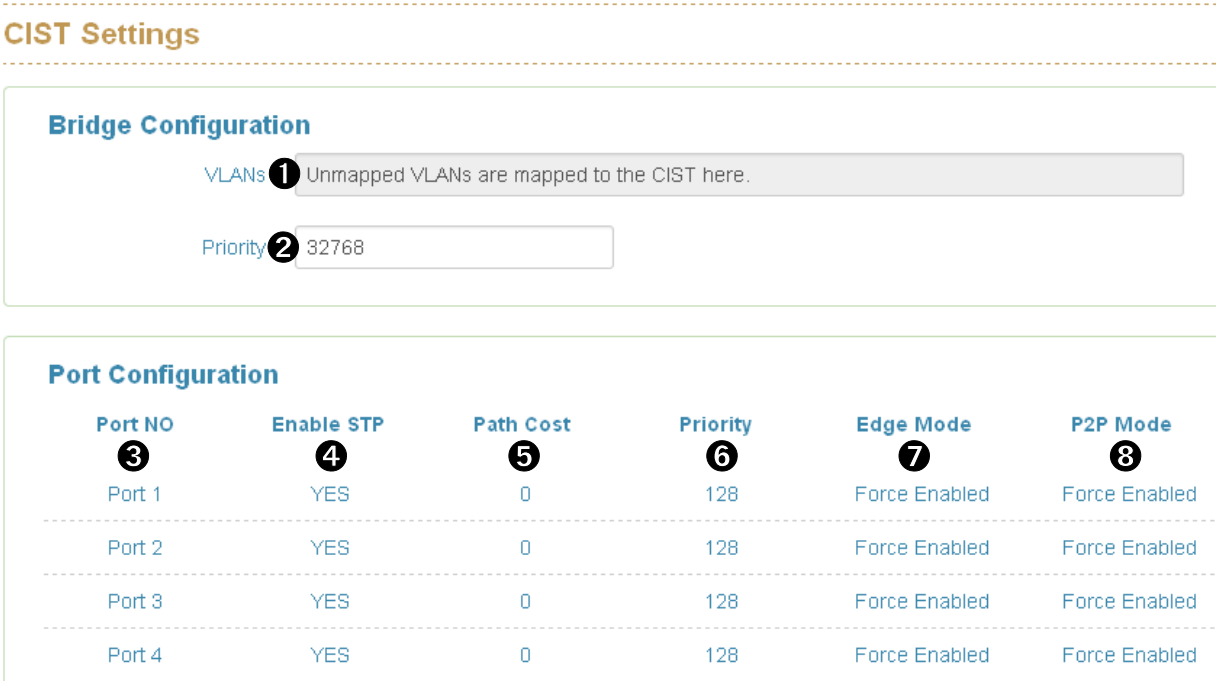
C. Check the status of STP, all ports should change to "Yes"

D. Remember to press "Apply"

Apply

E. Save setting





16.2.1. Bridge configuration

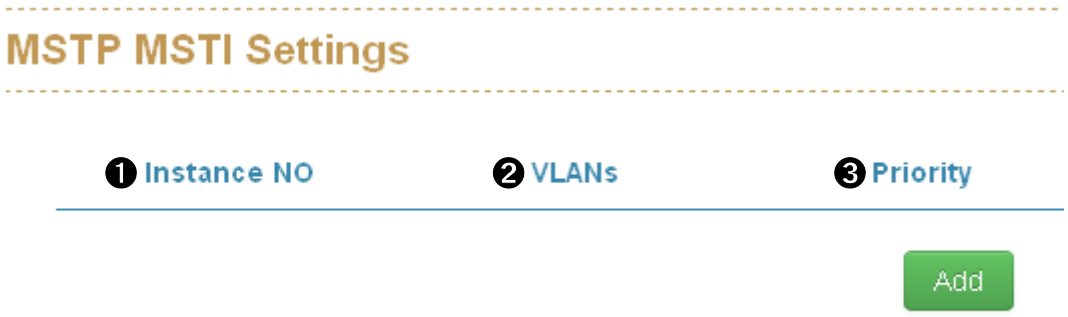
Name	Description
❶ **VLANs :**	The list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Unmapped VLANs are mapped to the CIST. (The default bridge instance).
❷ **Priority:**	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number,

	concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

16.2.2. Port Configuration

Name	Description
❸ **Port No:**	The switch port number of STP.
❹ **Enabled STP:**	Controls whether STP is enabled with this switch port.
❺ **Path Cost:**	Controls the path cost incurred by the port. The Auto setting will set the path cost appropriate by the physical link speed, using the 802.1D recommended values.
❻ **Priority:**	Controls the port priority. This can be used to control priority of ports having identical path cost. (See above).
❼ **edge_mode:**	The port which connects with ending device
❽ **p2p_mode:**	The port which connects with another switch

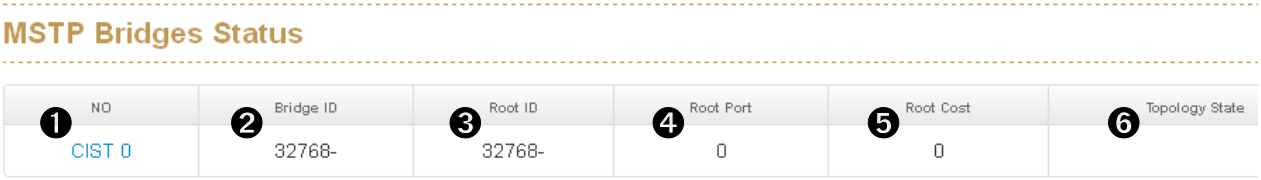
16.3 MSTP MSTI Settings



Name	Description
❶ **Instance No:**	Index number of MSTP instance
❷ **VLANs:**	The list of VLANs mapped to the MSTI. A VLAN can only be mapped to one MSTI. Unmapped VLANs are mapped to the CIST. (The default bridge instance).

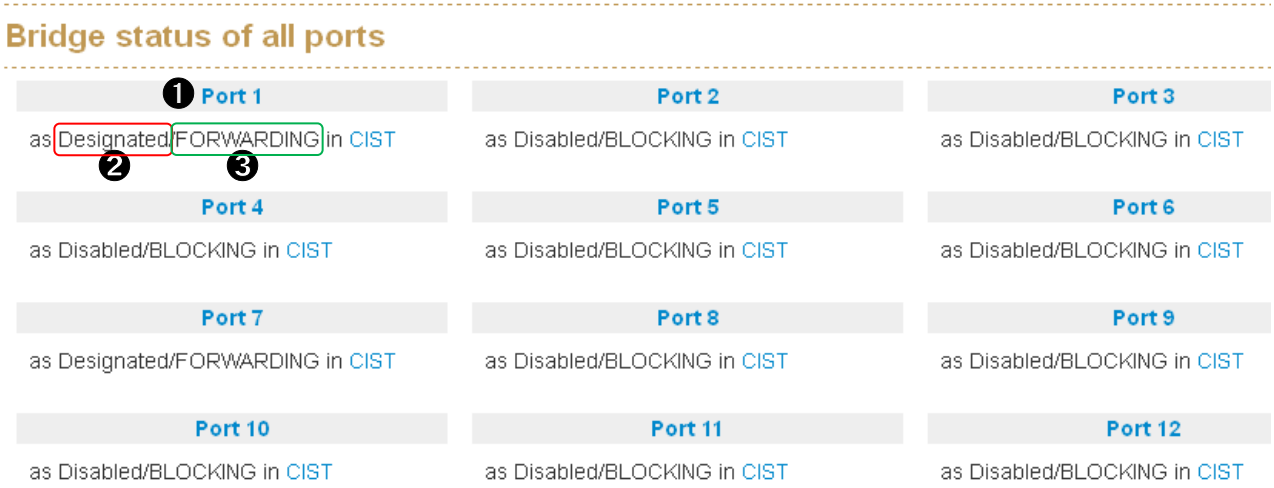
❸ **Priority:**	Controls the bridge priority. Lower numeric values have better priority.

16.4 MSTP Bridges Status



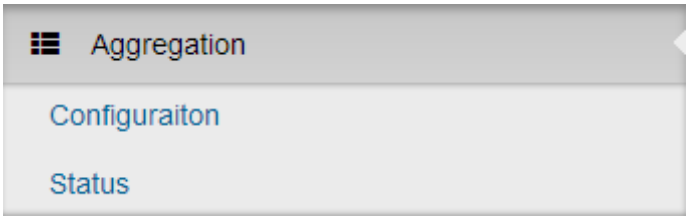
Name	Description
❶ **NO:**	The number of MSTP instance
❷ **Bridge ID:**	The ID of this Bridge instance.
❸ **Root ID:**	The ID of the currently elected root bridge.
❹ **Root Port:**	The switch port as the root port role.
❺ **Root Cost:**	Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
❻ **Topology State:**	The current state of the Topology.

16.5 Bridge status of all ports



<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>❶ Port:</td><td>The switch port number of STP port.</td></tr>
<tr><td>❷ Role:</td><td>The current STP port role of the port. The port role can be one of the following Variants:
<table>
<tr><th>Variants</th><th>Default Setting</th></tr>
<tr><td>AlternatePort, BackupPort, RootPort, DesignatedPort, Disabled</td><td>Per current status</td></tr>
</table>
</td></tr>
<tr><td>❸ State:</td><td>The current STP port state of the port. The port state can be one of the following Variants:
<table>
<tr><th>Variants</th><th>Default Setting</th></tr>
<tr><td>Discarding, Learning, Forwarding, Blocking</td><td>Per current status</td></tr>
</table>
</td></tr>
</table>

17. Link Aggregation

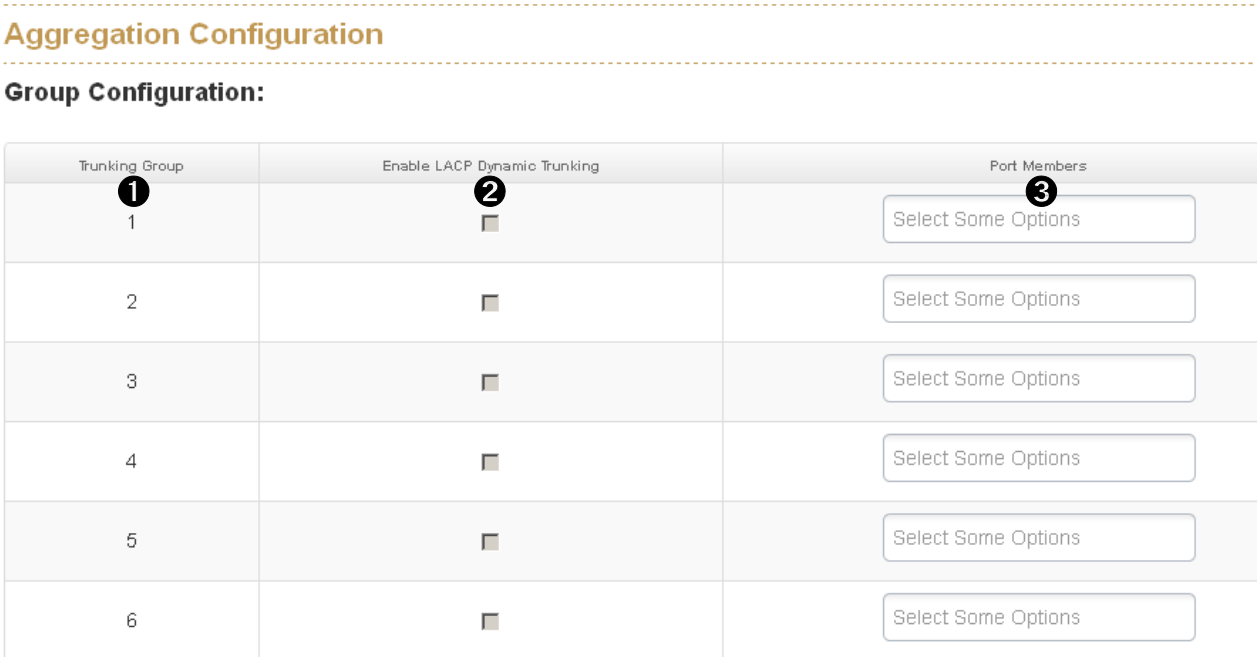


In computer networking, the term link aggregation applies to various methods of combining (aggregating) multiple network connections in parallel in order to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links should fail. A Link Aggregation Group (LAG) combines a number of physical ports together to make a single high-bandwidth data path, so as to implement the traffic load sharing among the member ports in the group and to enhance the connection reliability.

Other umbrella terms used to describe the method include port trunking ,link bundling, Ethernet/network/NIC bonding ,or NIC teaming. These umbrella terms encompass not only vendor-independent standards such as Link Aggregation Control Protocol (LACP) for Ethernet defined in IEEE 802.3ad standard, but also various proprietary solutions.

Note: This section is taken from Wiki at https://en.wikipedia.org/wiki/Link_aggregation

17.1 Aggregation Configuration



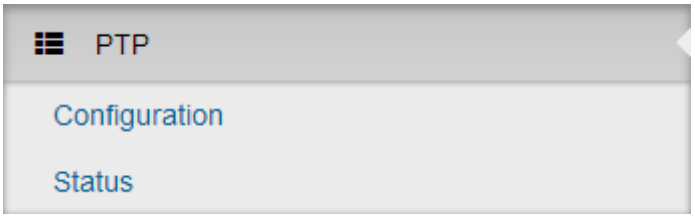
Group Configuration

Name	Description
❶ **Trunking Group:**	Number of trunk group
❷ **Enable LACP Dynamic Trunking**:	Enable LACP Dynamic Trunk function by clicking the box
❸ **Port Members:**	Select which ports you want to aggregate with

17.2 LACP Group Status

Name	Description
❶ **Trunking Group**	Number of trunk group
❷ **LACP**	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or the port link is down.
❸ **System ID**	The ID of each Trunk group
❹ **Port Members**	Switch ports which bind the trunk group

18. PTP



The Precision Time Protocol (PTP) is a protocol used to synchronize clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems.

PTP was originally defined in the IEEE 1588-2002 standard, officially entitled "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems" and published in 2002. In 2008, IEEE 1588-2008 was released as a revised standard; also known as PTP Version 2, it improves accuracy, precision and robustness but is not backward compatible with the original 2002 version.

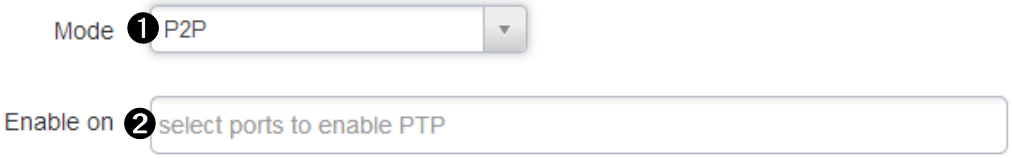
"IEEE 1588 is designed to fill a niche not well served by either of the two dominant protocols, NTP and GPS. IEEE 1588 is designed for local systems requiring accuracies beyond those attainable using NTP. It is also designed for applications that cannot bear the cost of a GPS receiver at each node, or for which GPS signals are inaccessible."

Note: this section is taken from WIKI at https://en.wikipedia.org/wiki/Precision_Time_Protocol

There are two modes in IEEE1588 PTP, Two-step PTP and One-step PTP. Two-step PTP will add the time-stamp value on synchronized massage via CPU to slave while One-step PTP sends a synchronized message straight to slave by hardware PHY without going through CPU.

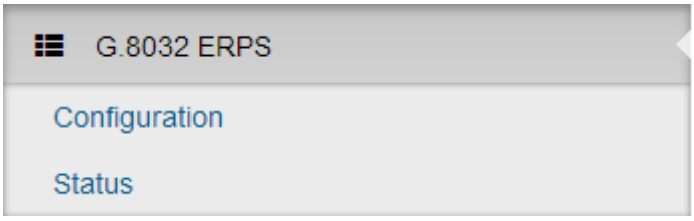
Note: PTP is an optional hardware function for Lantech switch. Please check your model if it supports PTP.

PTP Transparent Clock Configuration



Name	Description
❶ **Mode:**	Currently switch only support P2P mode **Variants**: E2E/P2P; **Default Setting**: P2P
❷ **Enable on:**	Select switch port(s) which you want to active PTP mode. Note : PTP mode is supported only on Gigabit port, please check the model specification for supported PTP Gigabit port by Cooper or Fiber or Both

19. G.8032 Ethernet Ring Protection (ERPS)



Ethernet Ring Protection Switching, or ERPS, is an effort at ITU-T under G.8032 Recommendation to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer. G.8032v1 supported a single ring topology and G.8032v2 supports multiple rings/ladder topology.

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 particular 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 for blocking 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 Neighbour Node, may also participate in blocking or unblocking its end of the RPL.

The event of an Ethernet Ring failure results in protection switching of the traffic. This is achieved under the control of the ETH_FF functions on all Ethernet Ring Nodes. An APS protocol is used to coordinate the protection actions over the ring.

Note: This section is taken from WIKI at https://en.wikipedia.org/wiki/Ethernet_Ring_Protection_Switching

Lantech ERPS ring consists of five (5) modes including Auto, Basic, Enhanced, Multiple-VLAN, Multiple-Train modes. Only the Basic and Multiple-VLAN modes are compatible with most of 3rd party switch that supports ERPS. The Auto, Enhanced

and Multiple-Train modes are Lantech proprietary protocols and can only be supported by Lantech 3 series and above switches. The ERPS ring modes may be varied in different switch models, please check the specification before use.

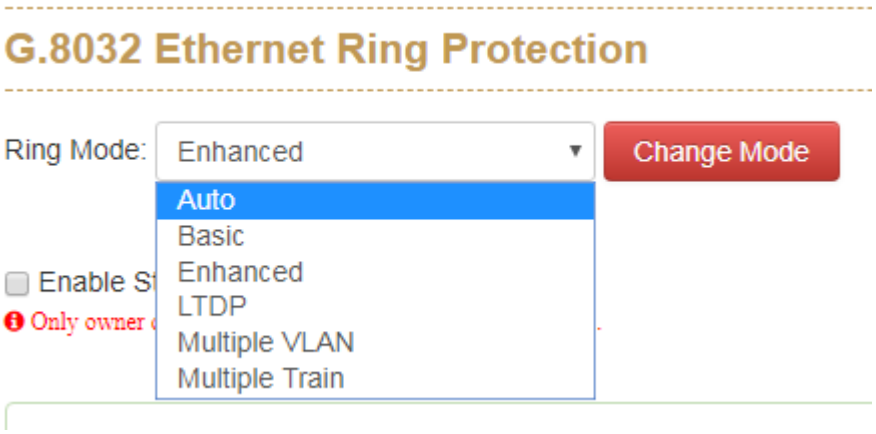
Lantech Auto, Enhanced and Multiple-Train ring are adapted to protect IGMP and data packets with faster recovery scheme, so if the network is in heavy duty of IGMP application, we suggest using those ring modes to achieve better redundancy.

Notice:

1. Building ITU-Ring requires all uplink connections to use the same media, i.e.: all fiber ports or all copper ports. Inconsistent uplink media may cause ITU-Ring to fail.

2. Apart from consistent uplink media, the speed of uplink ports must be consistent too, i.e.: all 10/100 or all 10/100/1000. Inconsistent speed may cause ITU-Ring misjudgment and loop.

19.1 Introduction of Ring modes



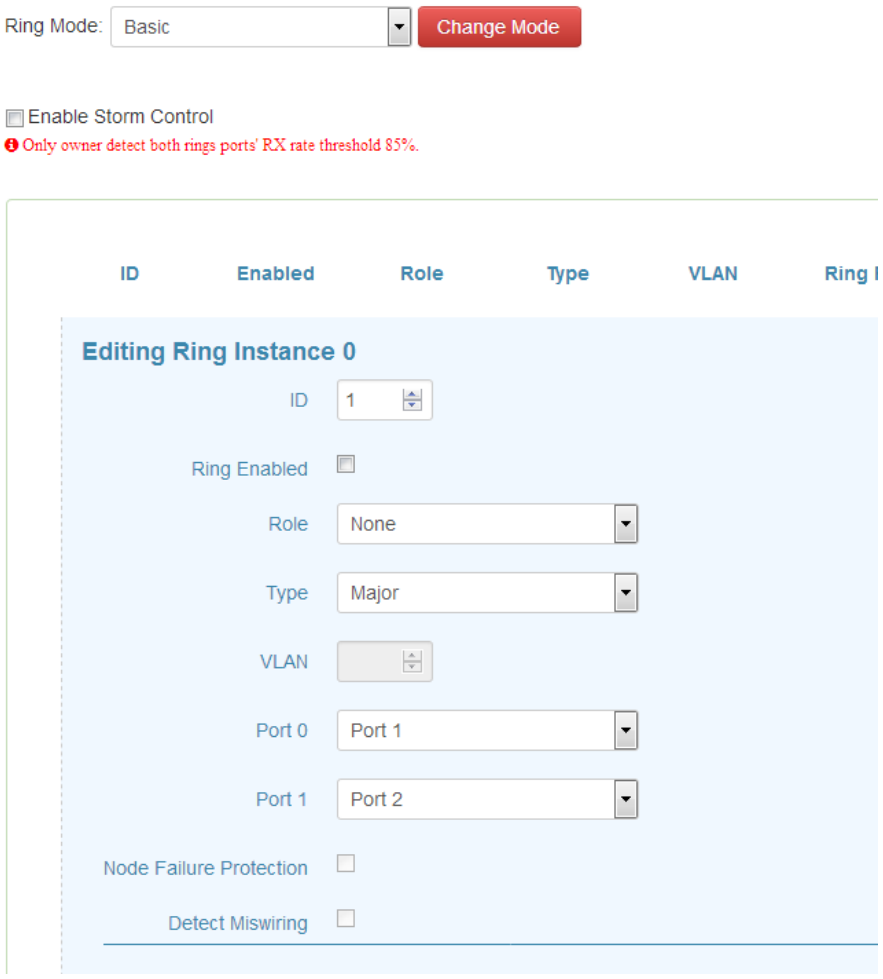
Auto Ring

Auto Ring applies with single ring topology only. The operator only need to assign ring ports with each switch, the other options will be defined automatically by switch.

Note: Please keep the setting of ID & Type as default because Auto Ring mode only supports single ring topology.

Basic Ring

It was designed for the compatibility with most of other vendor's ERPS under G.8032v1 standard (Single ring topology).

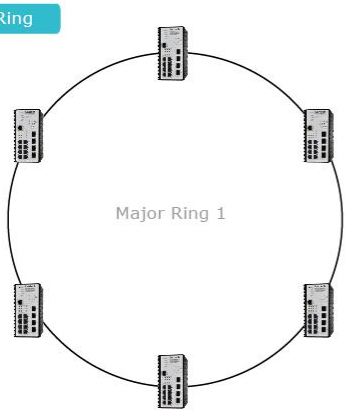


Enhanced Ring

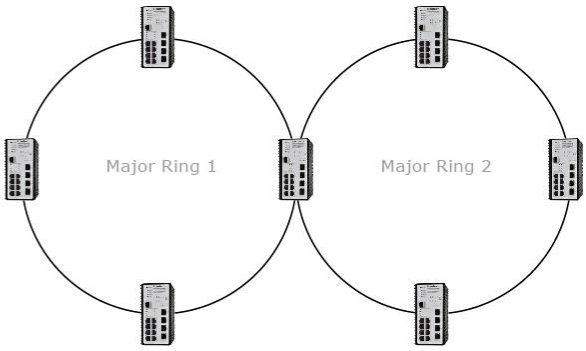
Lantech Enhanced ring mode supports multiple rings, please refer to the following demo topologies. All rings (include Major ring and Sub ring) must be in the same VLAN.

Note: This is proprietary Lantech ring.

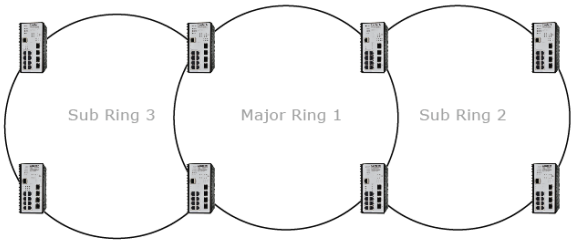
Single Ring



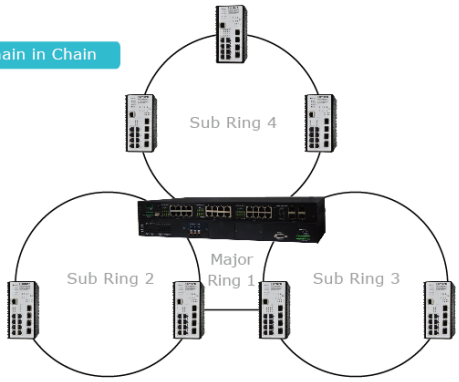
Dual Rings



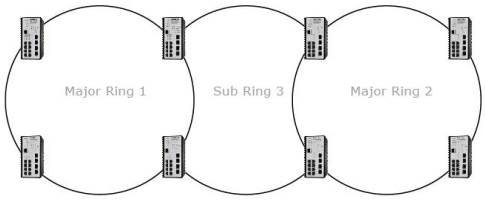
Multiple Chain



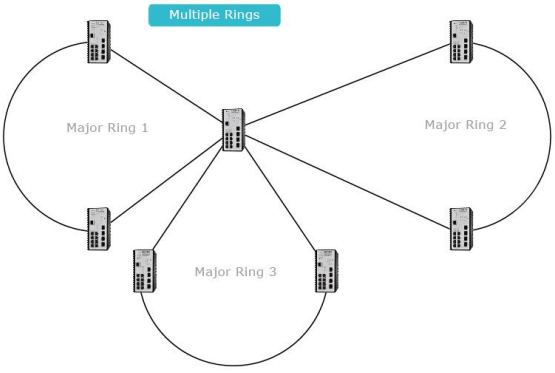
Chain in Chain



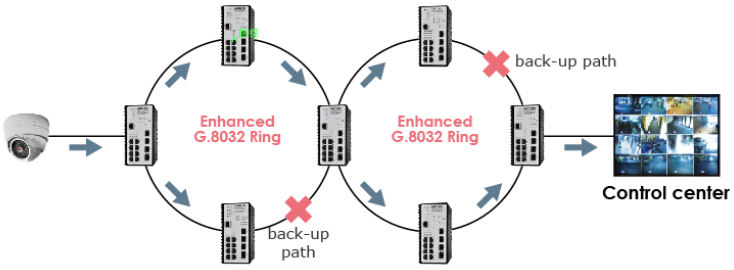
Redundant Coupling



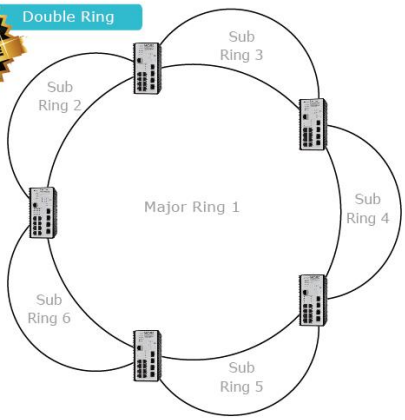
Multiple Rings



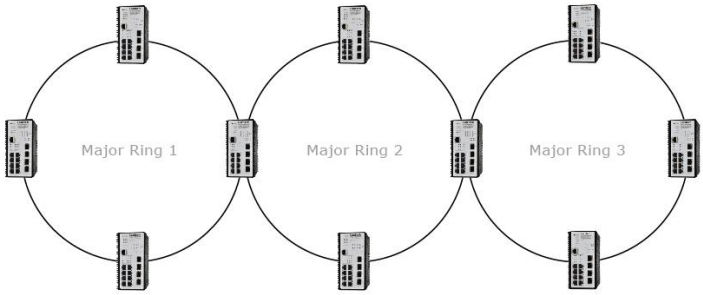
Enhanced Ring for Multicast Recovery



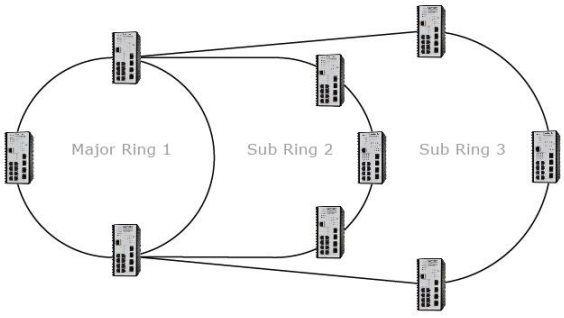
Double Ring



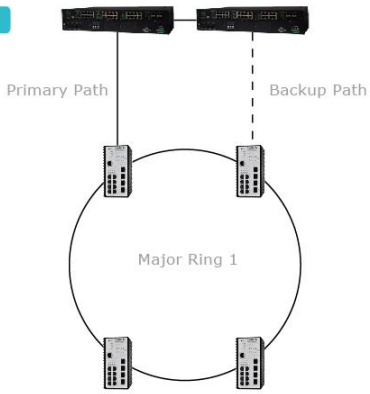
Cascade Chain



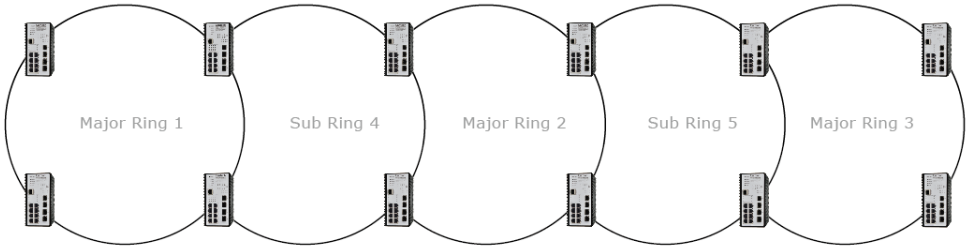
Multiple Chain Share Common Ends

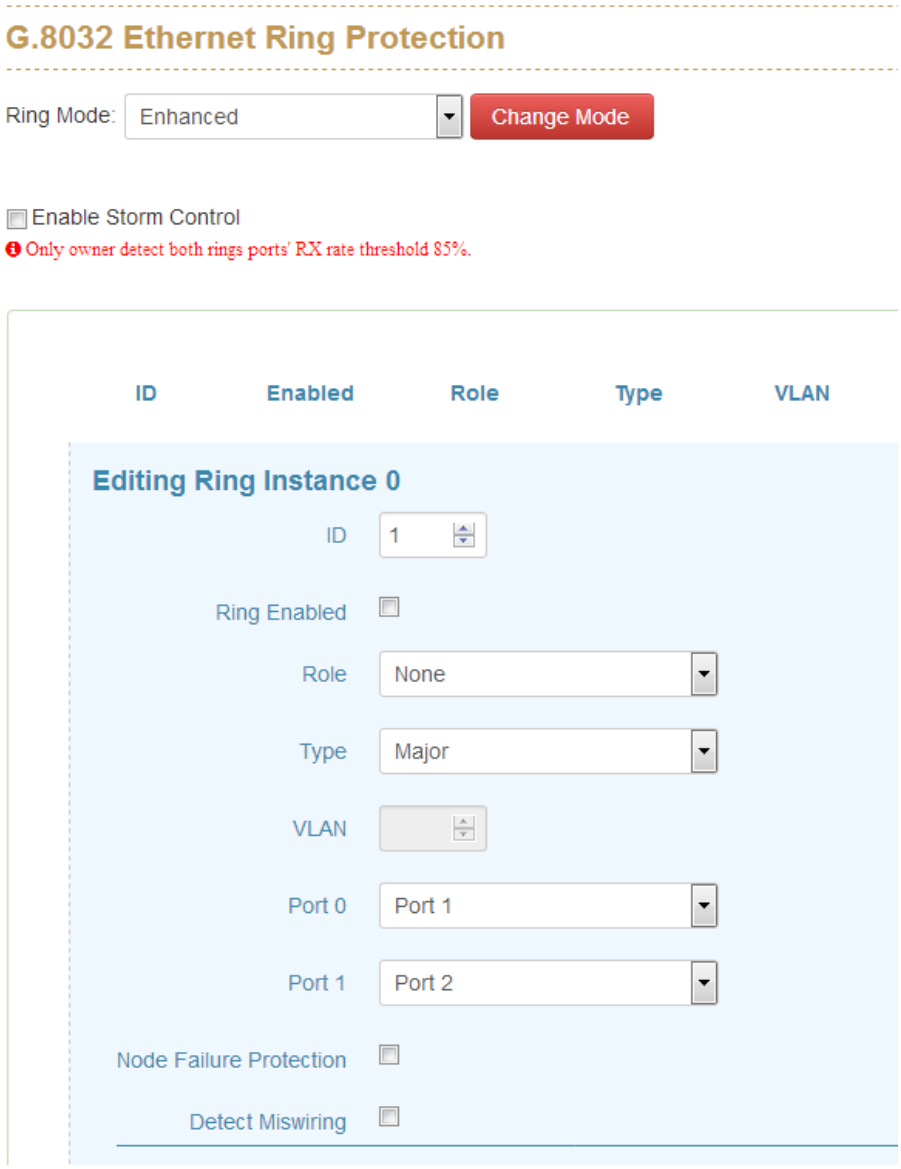


Dual Homing



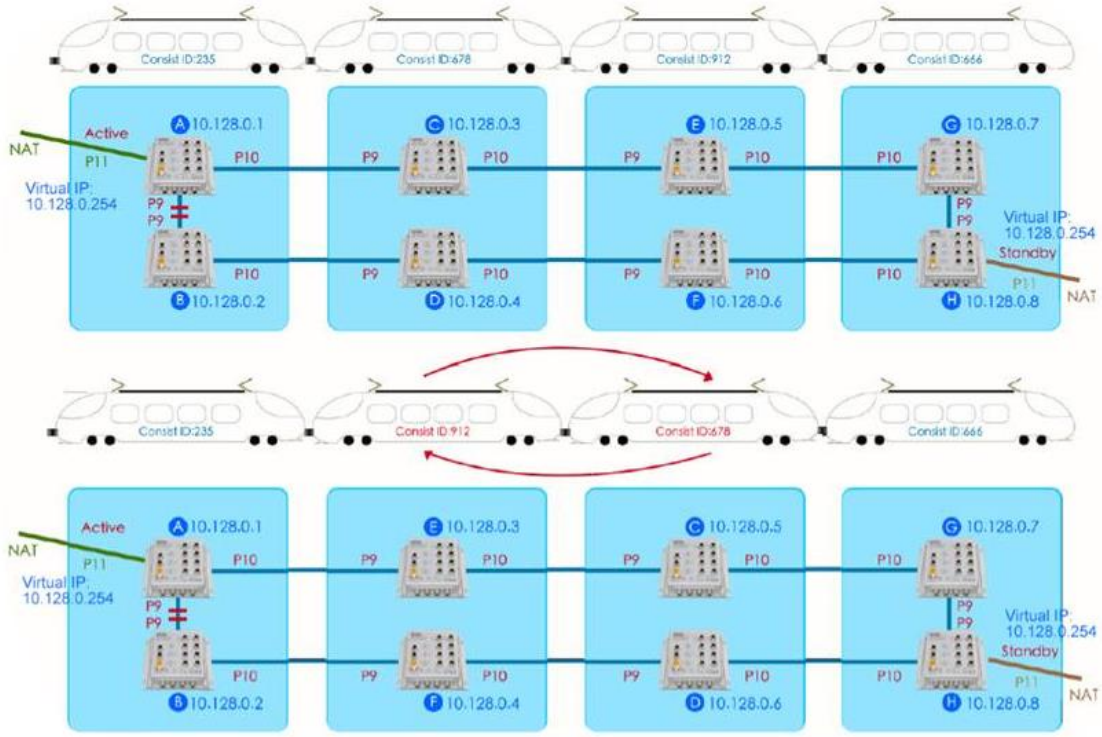
Redundant Coupling with Multiple Rings

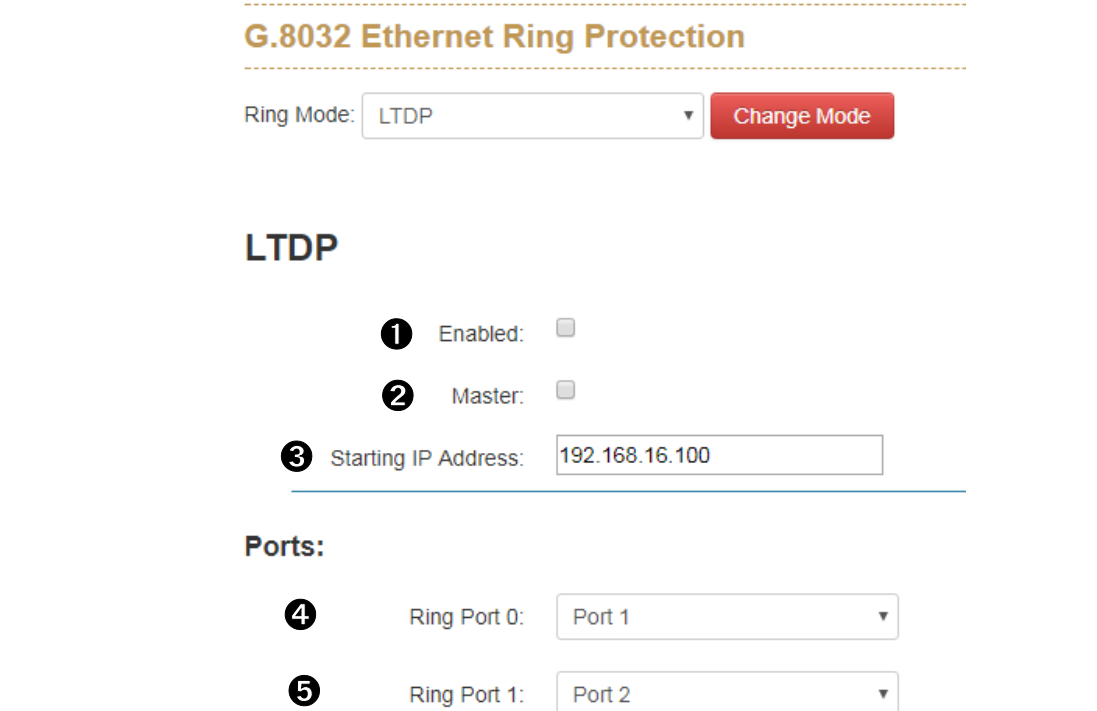



G.8032 Ethernet Ring Protection
Ring Mode:
Enhanced
Change Mode
Enable Storm Control
Only owner detect both rings ports' RX rate threshold 85%.
ID
Enabled
Role
Type
VLAN
Editing Ring Instance 0
ID
1
Ring Enabled
Role
None
Type
Major
VLAN
Port 0
Port 1
Port 1
Port 2
Node Failure Protection
Detect Miswiring

LTDP

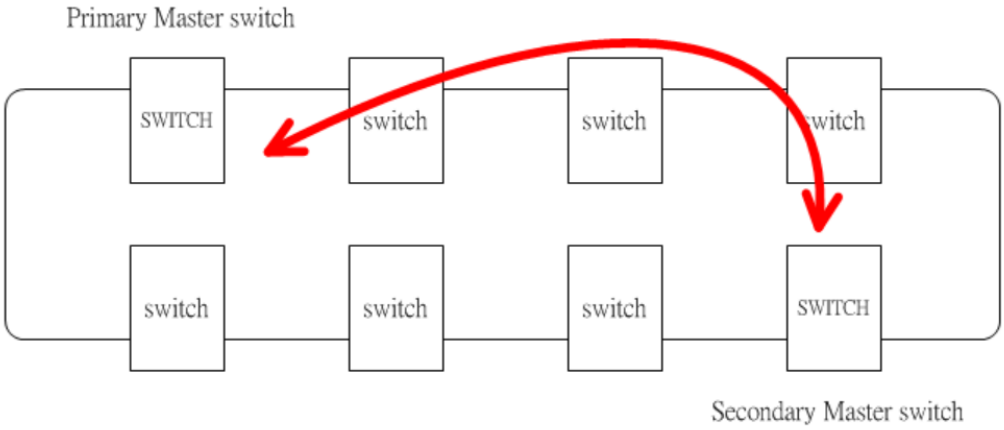
LTDP is designed for dynamic installation environment of train application, beside fail uplink connection protection and node failure protection, it also support IP assign automatically and configuration backup and restore automatically.



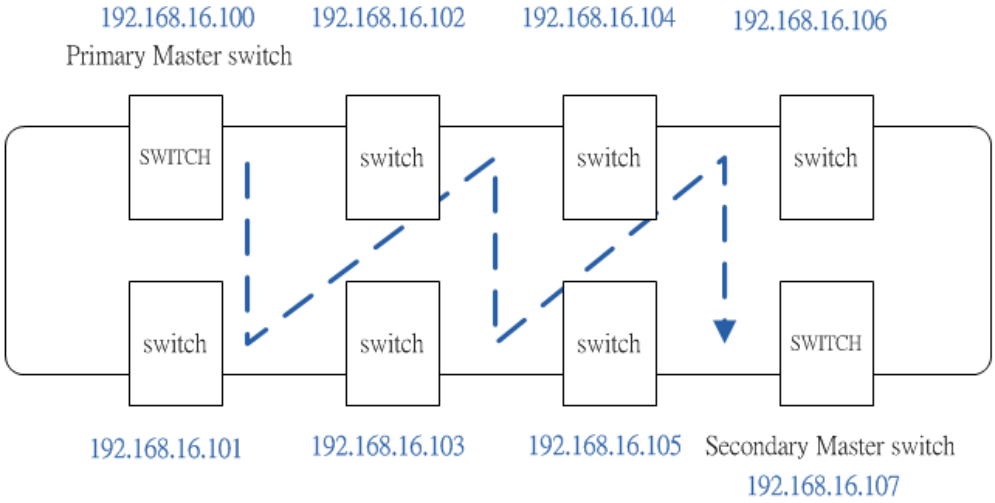


Name	Description
❶ **Enabled:**	Enable LTDP
❷ **Master:**	Set master switch of LTDP
❸ **Starting IP address:**	Set Starting IP address of IP range which you want to assign to all switches in field
❹ **Ring Port 0:**	First Ring Port of LTDP
❺ **Ring Port 1:**	Second Ring Port of LTDP.

Master: you need to assign 2 master switches in front carriage and end carriage, these 2 master switch will be responsible to assign IP address switch and backup configuration file of each switch. They will be backup with each other.

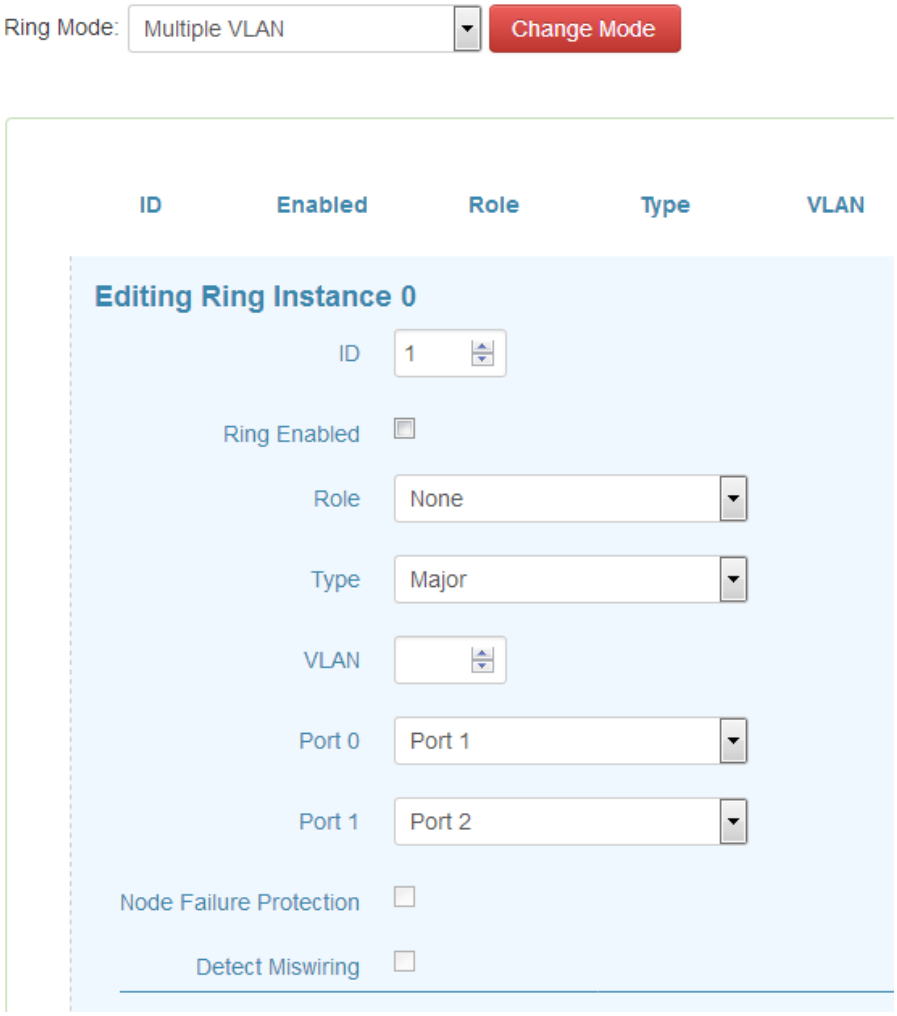


Starting IP address: Just need to set the first IP address of the IP range which you want to assign those switches, the primary master switch will assign IP address to all switches by the sequence of below diagram, remember all switches need to set the same IP address with this option.

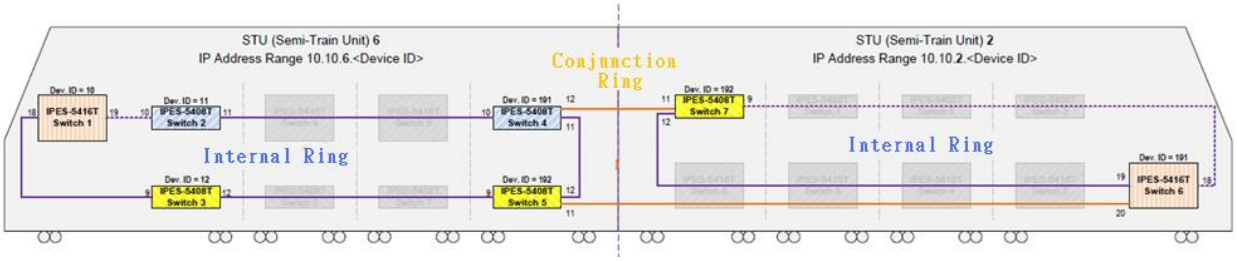

192.168.16.100
Primary Master switch
192.168.16.102
192.168.16.104
192.168.16.106
SWITCH
switch
switch
switch
switch
switch
switch
SWITCH
192.168.16.101
192.168.16.103
192.168.16.105
Secondary Master switch
192.168.16.107

Multiple VLAN

All rings (include Major ring and Sub ring) can be implemented with different VLAN. This Multiple VLAN mode can be compatible with most of other brand switches.

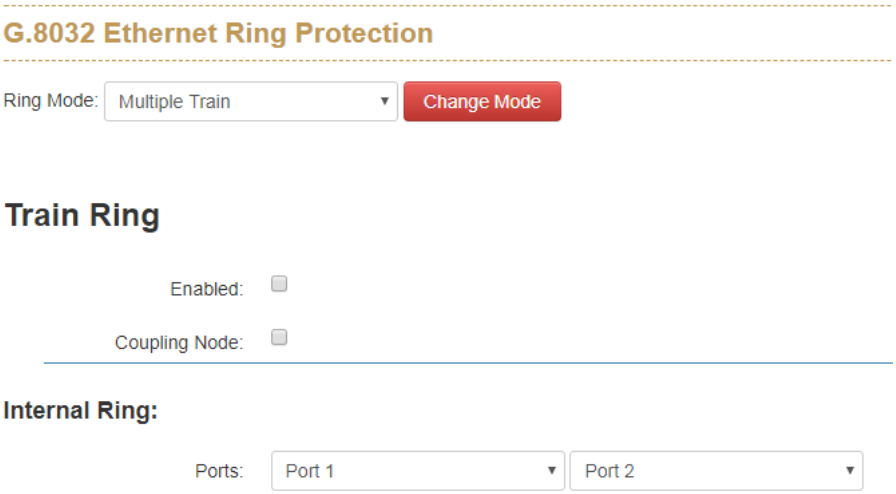


Multiple Train Ring

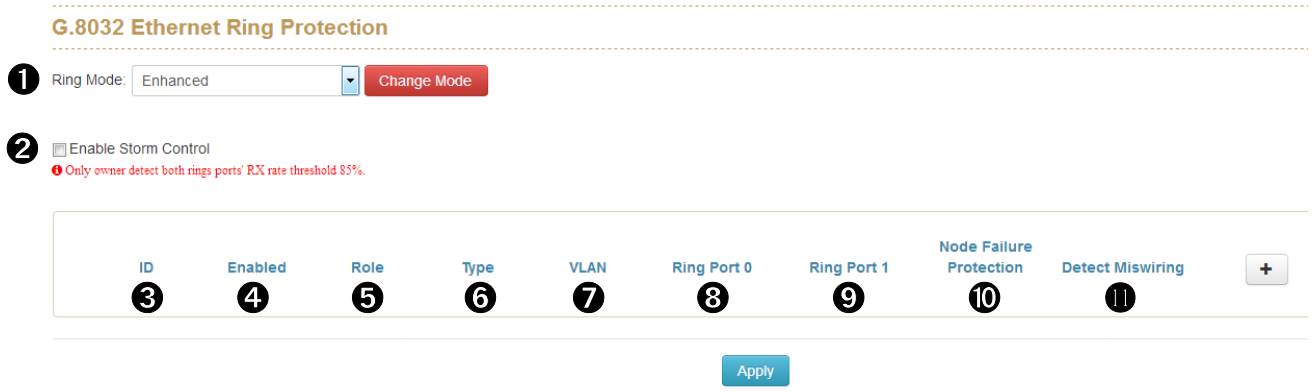


Multi-Train Ring is designed for the redundancy network of train application, as above picture. Multiple train ring supports dynamic coupling topology that is able to couple two rings automatically which requires in train coupling applications.

Note: Train ring must consist of minimum four (4) Lantech switches in the conjunction ring.



19.2 Interface



Name	Description
❶ **Ring Mode:**	There are 5 modes can be chosen, switch need to be rebooted after mode changed **Variants**: Auto, Basic, Enhanced, LTDP, Multiple VLAN, Multiple Train **Default Setting**: Enhanced
❷ **Enable Storm Control:**	This function only can be activated by owner switch. If owner switch detects loop issue, it will force to disable RPL port. It can only be enabled with owner switch.
❸ **ID:**	The ID of the created protection group
❹ **Enabled:**	Enable/Disable the G.8032 ERPS.
❺ **Role:**	It can be either RPL owner or RPL Neighbor.
❻ **Type:**	Type of Protecting ring. It can be either major ring or sub-ring.
❼ **VLAN:**	VLAN of per ring , only available with Multiple VLAN mode.
❽ **Ring Port 0:**	This will create a Port 0 of the switch in the ring. Please refer to 18.4 for rule of setting port 0.
❾ **Ring Port 1:**	This will create "Ring Port 1" of the switch in the Ring. Please refer to 18.4 for rule of setting port 1.
❿ **Node Failure Protection:**	This option can avoid loop under circumstance of power outrage to switches that will be rebooted after power restore. It can only be enabled with owner switch.

⓫ **Detect Misswiring:**	This option can prevent incorrect ring port wiring that is conflict with pre-set ring ports and incur loop issue.

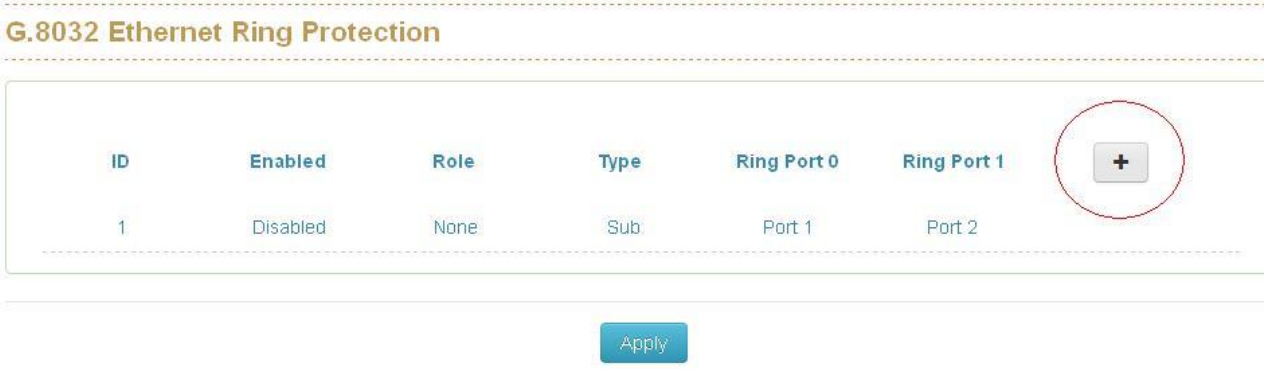
19.3 Setting Up and Configuring

18.3.1. G.8032

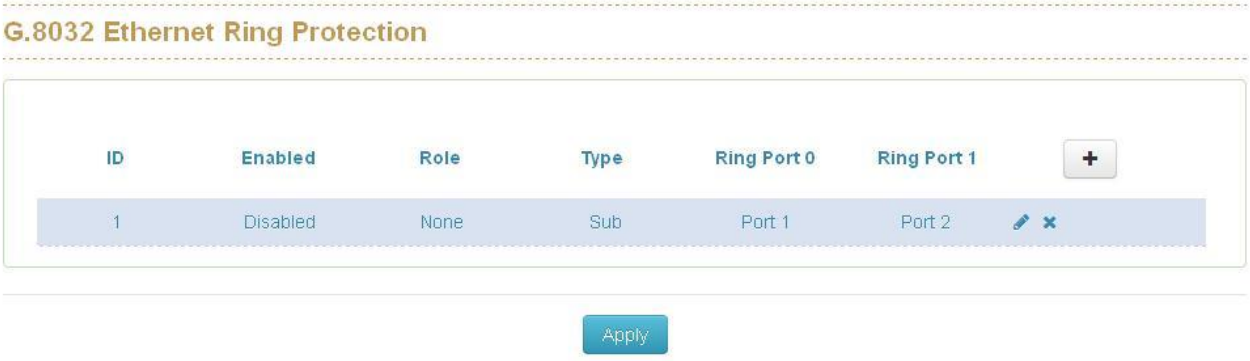
Before Setup: Make sure you have disabled the MSTP protocol.

Note: in this case, we will use the port 9 and port 10 of each switch to build a ring.

1. Press "+" icon to add one ring with G.8032 protocol.



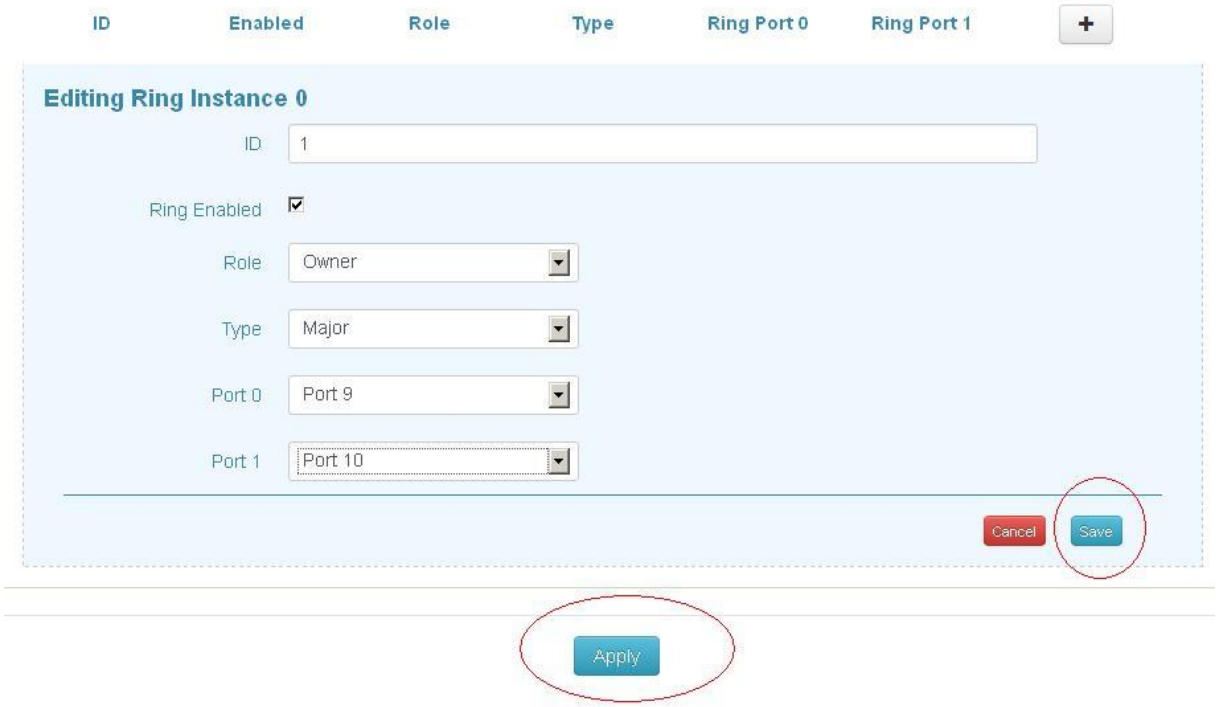
2. Enter edit mode



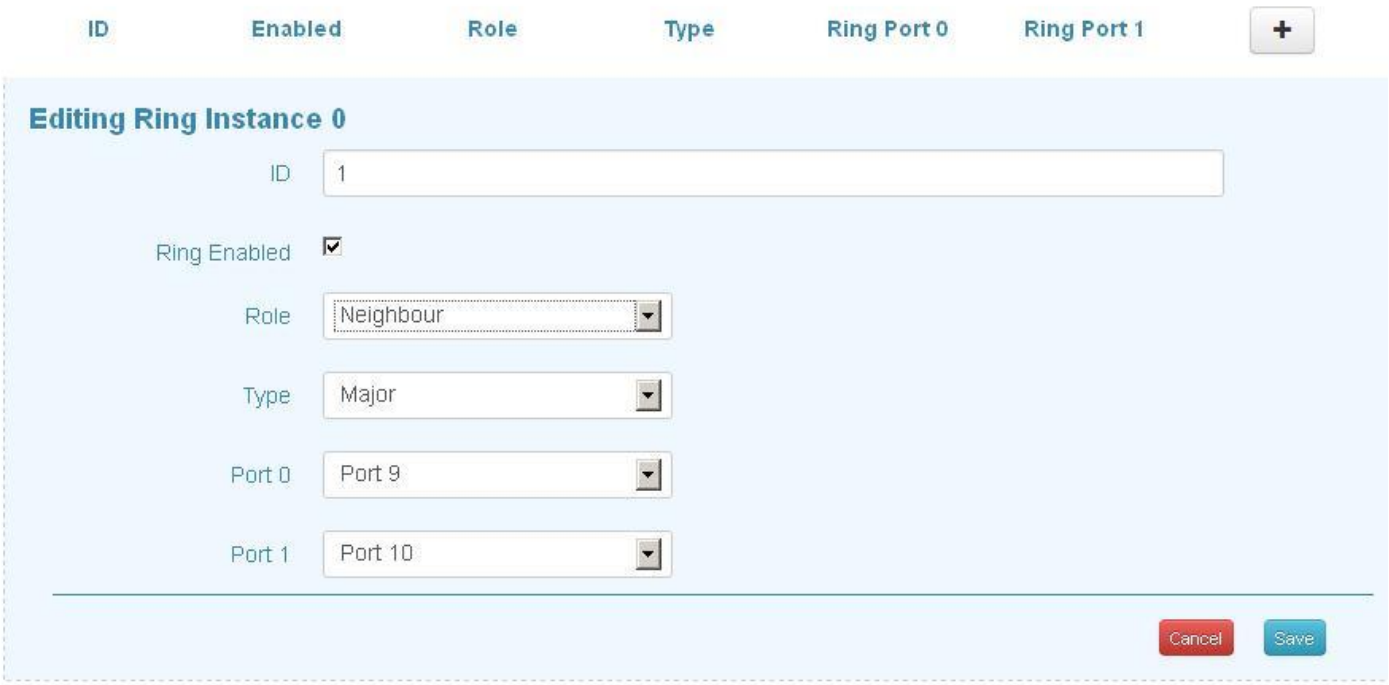
3. Take an example of three switches in the ring of G.8032, one plays the role of "owner", another for "neighbor" and the other for "none" , please remember three very import rules in the setting procedure:
   - ■ the port0 of "owner" switch must connect with the "neighbor" switch.
   - ■ After enable the ring of G8032, the port0 of owner switch will be blocked at first.

To play safe, we suggest the user to finished all setting G8032 then connect the physical connection if the user is not familiar with the G8032 function.

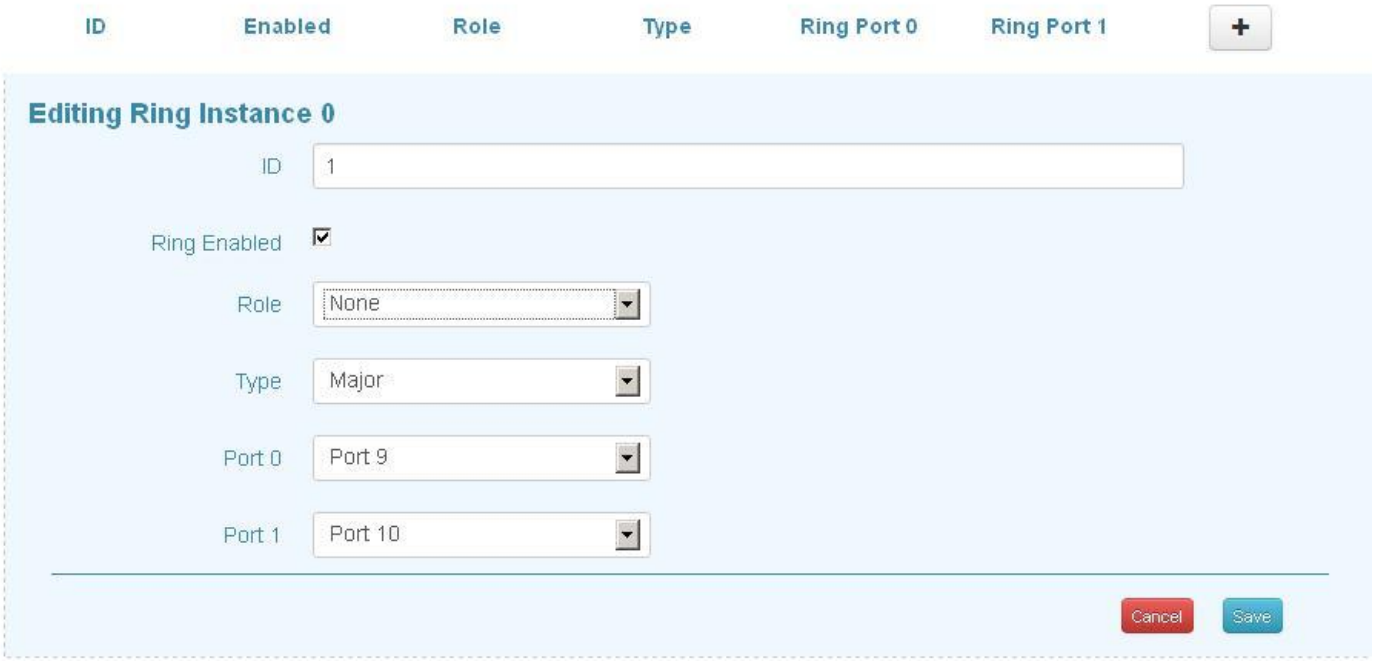
4. The setting of owner switch, remember to press "SAVE" and "APPLY" to confirm the setting. (For we only have single ring of three switches, so we set the type as Major)



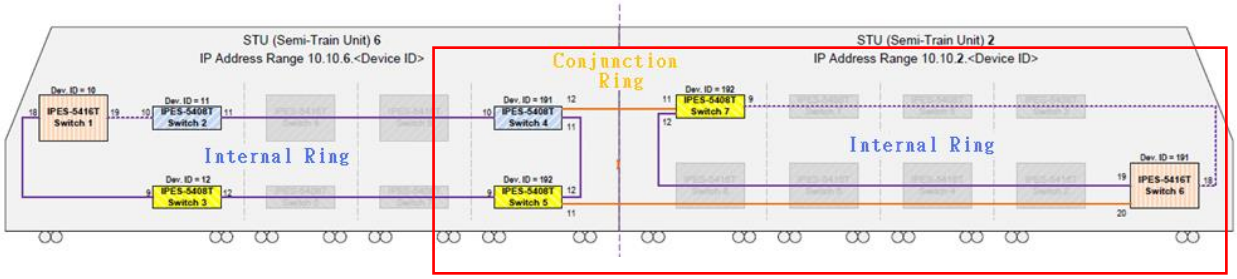
5. The setting of neighbor switch



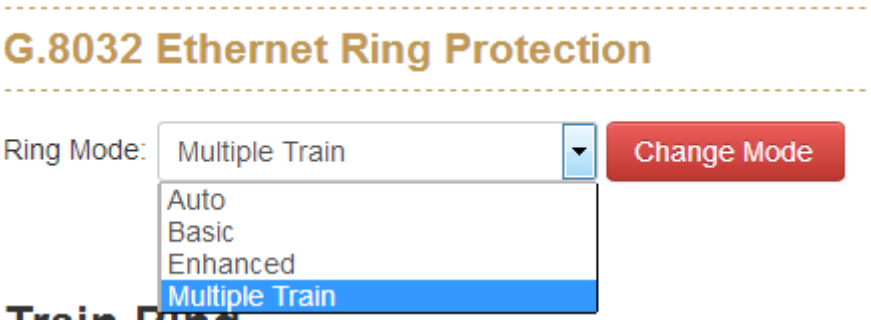
6. The setting of none switch



18.3.2. Multiple Train Ring

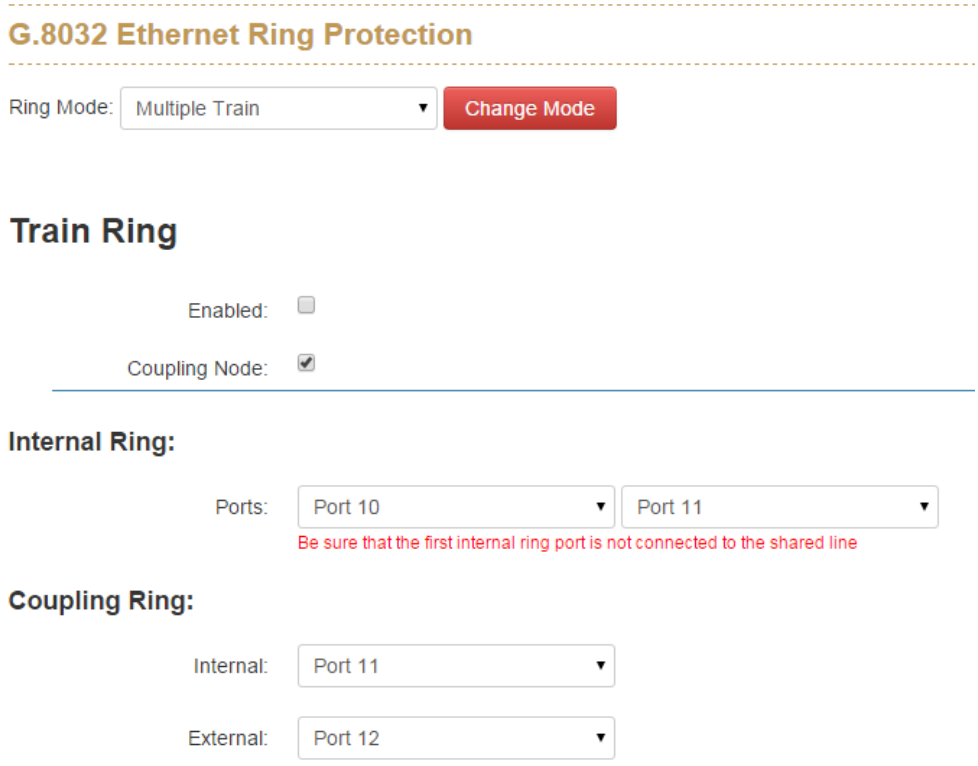


Step1: Enable ITU G.8032 to "Multiple Train" mode.

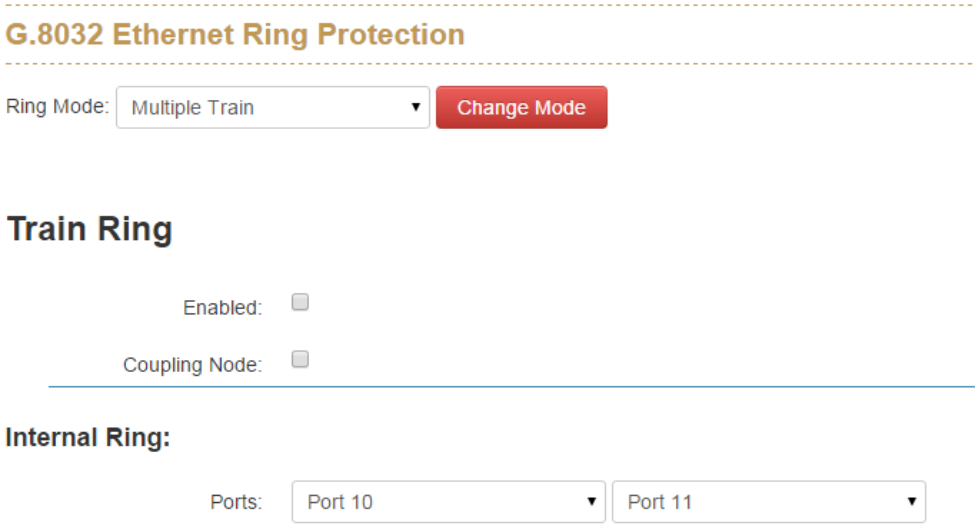


Step2: Select ring ports

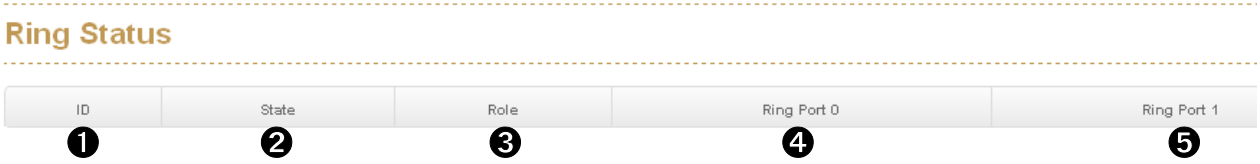
Example 1: Enable "Coupling Node" (Those 4 switches on right side are responsible to couple consist networks together)



Example 2: Disable "Coupling Node" (The other switches of each STU)



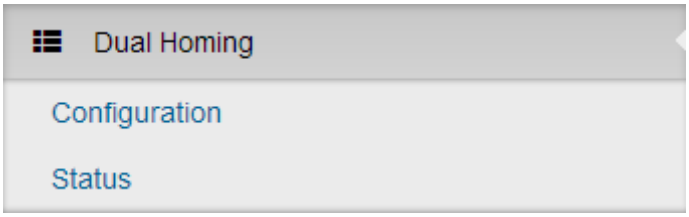
19.4 Ring Status



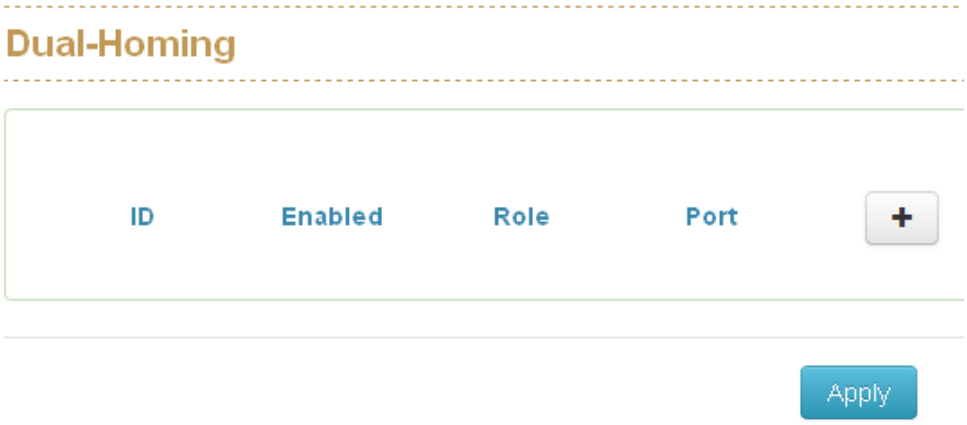
Name	Description
❶ **ID:**	The ID of the created Protection group
❷ **State:**	ERPS state according to State Transition Tables in G.8032.
❸ **Role:**	It can be either RPL owner or RPL Neighbor.
❹ **Ring Port 0:**	true : ring port 0 is blocking false : ring port 0 is not blocking
❺ **Ring Port 1:**	true : ring port 0 is blocking false : ring port 0 is not blocking

Note: If you have configured VLANS, Remember to set VLAN trunk port as ring port.

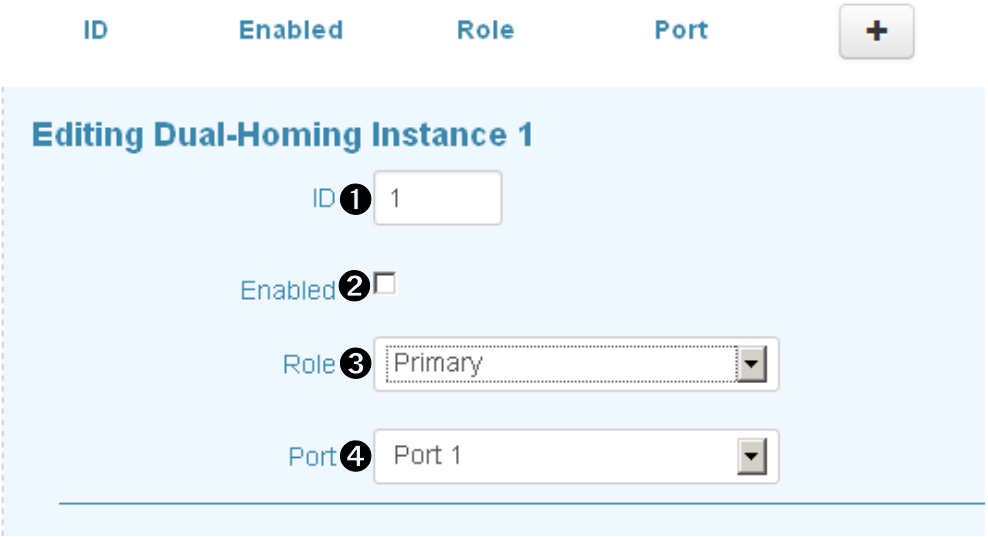
20. Dual Homing



This function was designed to connect ITU-Ring with the other redundancy protocol like STP、RSTP、MSTP.



Press "+" to add setting with Dual-Homing function.



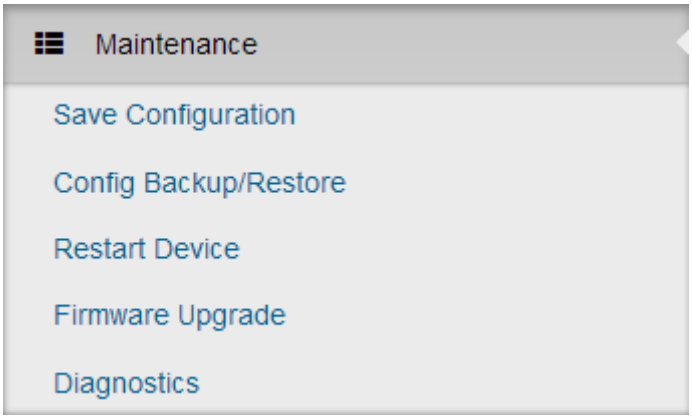
Name	Description
❶ **ID**:	The ID of Dual Homing connection

❷ **Enable**:	Enable the Dual Homing function of this port
❸ **Role**:	There should be 2 connections between RSTP with ITU-Ring, one set Primary, the other set Secondary.
❹ **Port**:	The port connects to the switch which runs RSTP protocol.

Variants	**Default Setting**
Primary/Secondary	Primary

Note: There are max. two connections between ITU-Ring with other redundancy protocol and each switch only support single Dual-Homing connection.

21. Maintenance

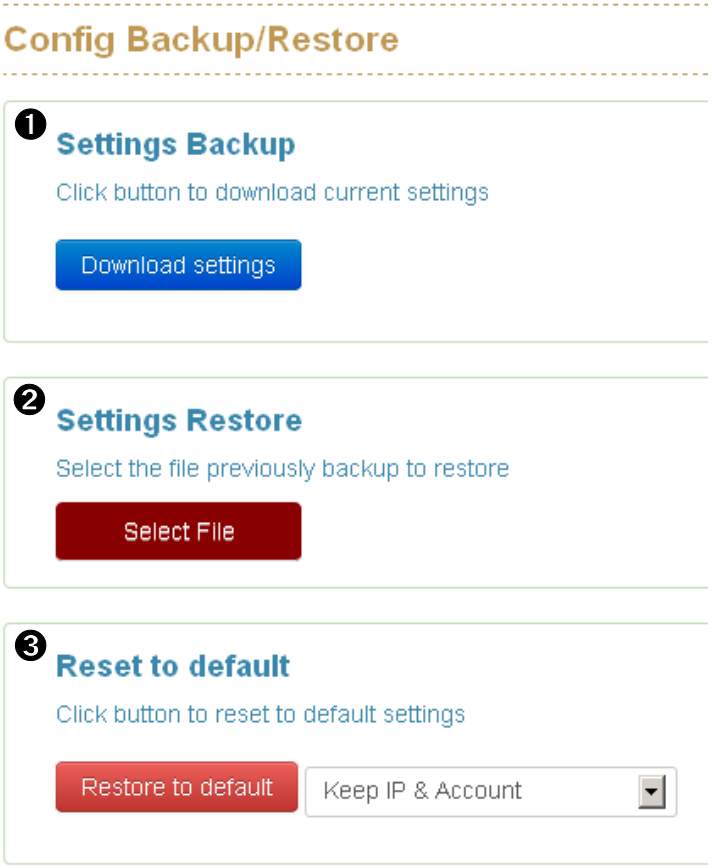


- System Config Save: Save the settings.
- Config Backup/Restore: Download and upload the configuration file.
- Maintenance Reboot: Reboot the switch manually.
- Firmware Upgrade: Update the firmware.

20.1 Save Configuration

Click to save the settings.

20.2 Configuration Backup/Restore



Settings Backup

Settings Backup is for saving the entire configuration of a switch into YML format which can be edited by office utility.

Settings Restore

Settings Restore is for restoring the configuration from YML backup.

Name	Description
❶ **Settings Backup:**	Download/ export the configuration from switch for back up.
❷ **Settings Restore:**	Upload/ import a previous configuration to startup.
❸ **Reset to default:**	Reset the switch with four resetting options.

Resetting Options	Default Setting
Keep IP & Account,	Keep IP & Account

	Keep User Accounts, Keep Network Configs, Restore Everything	

20.3 Restart Device (Maintaince Reboot)

Click to reboot the switch manually.

20.4 Firmware Upgrade

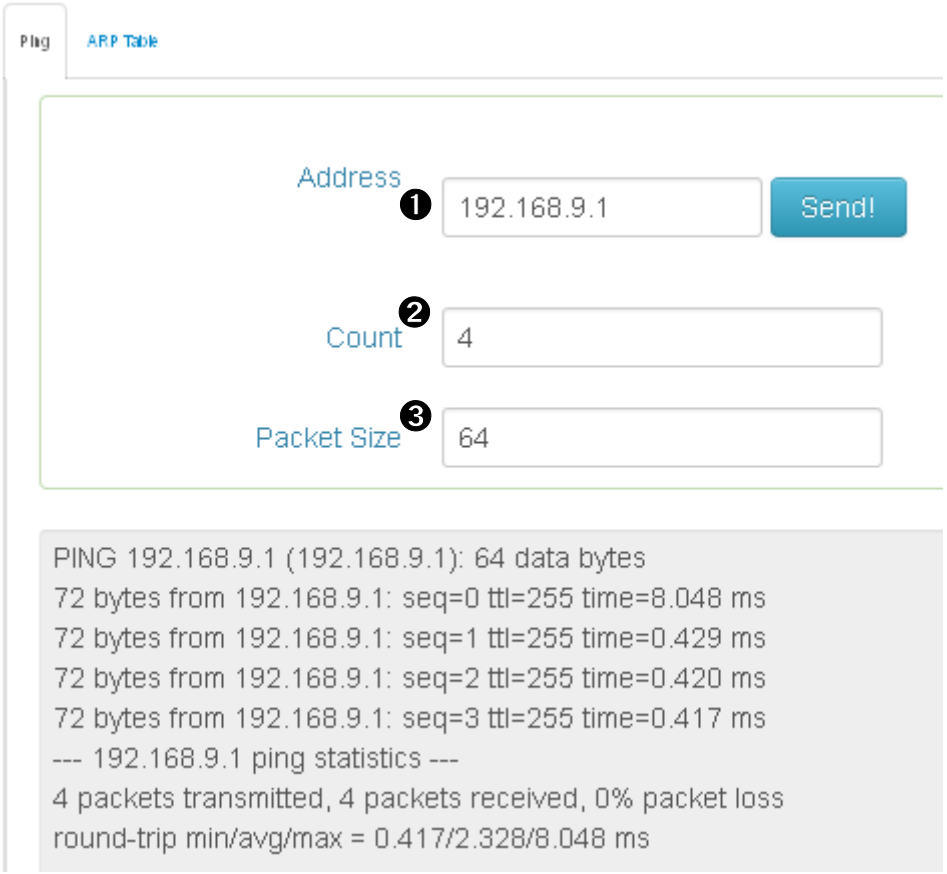
Update the switch by pressing "Select File" to browse computer and select the proper firmware. It will be taking 60 to 90 seconds to finish the work.

20.5 Diagnostics

Diagnosis panel contains the tables below and each of them helps technician to set up proper scenario for troubleshooting.

- Ping
- ARP Table

Ping



Name	Description
❶ **Address:**	Enter the IP address to ping.
❷ **Count:**	Enter how many times to ping the address.
❸ **Packet Size:**	Enter the size of ping packet.

ARP Table

Address Resolution Protocol (ARP) helps to map an IP address to a MAC address that is recognized in the local network and ARP Table shows the list of pinged MAC address and its corresponding IP address.

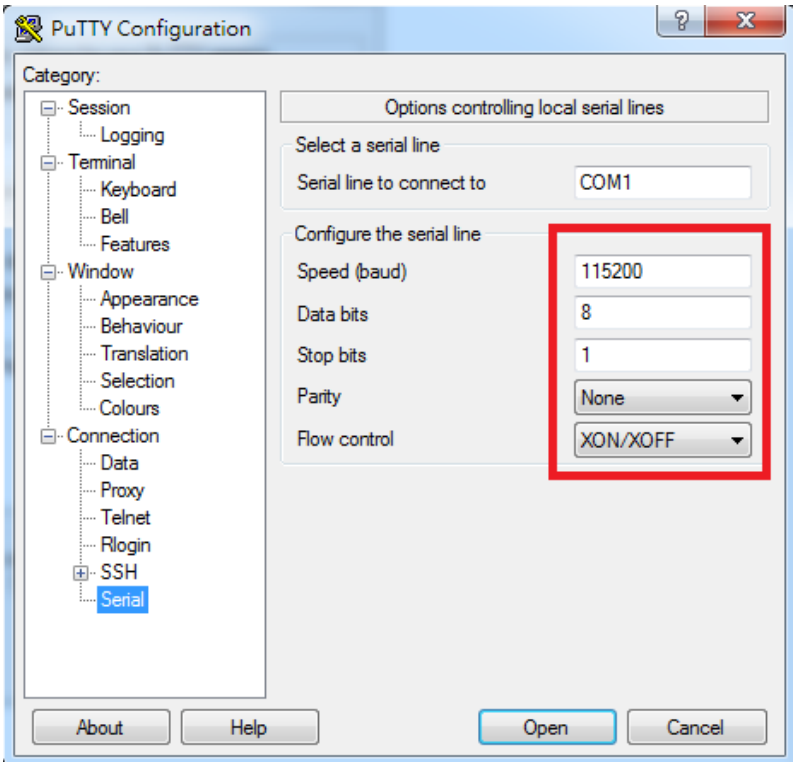
Appendix — Command Line mode

Besides web access, Lantech switch also support console and Telnet access. However, both of console and Telnet access support only command line user interface, so, herewith the link to download the list of commands:
http://www.lantechcom.tw/global/eng/download/datasheet/M-CLI.pdf

Access via console port

When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

Baud Rate: 115200 bps
Data Bits: 8
Parity: none
Stop Bit: 1
Flow control: None



The settings of communication parameters

Click '**OK**' to complete the work and the blank screen will show up, when it does then press Enter key to have the login prompt appears. And now please key in "**cli**" to enter the command line mode and then key in '**admin**' (default value) for both Login and Password and press Enter to get to the interface of console management. Please refer to below picture for the login screen.

Access via Telnet

Use Telnet utility to access switch IP and make sure the Dest. port is set to 23. All the commands under Telnet mode are the same to the Console mode.