Lantech

Web UI User's Manual

I(P)GS-3208MGSFP

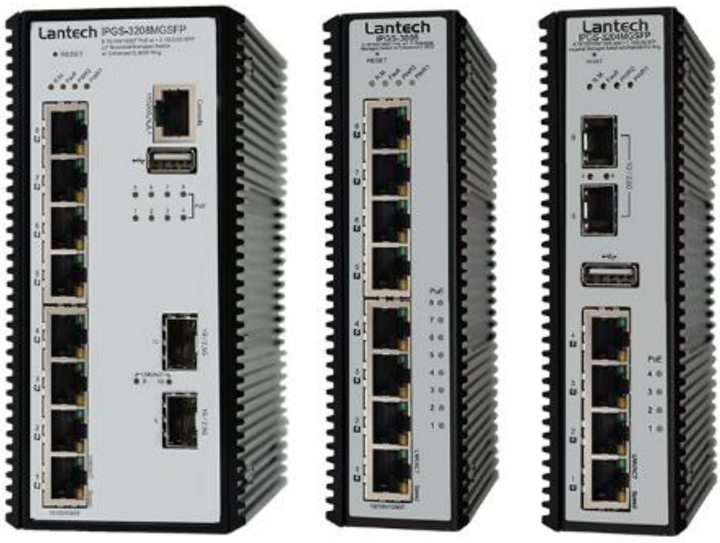
I(P)GS-3208C

I(P)GS-3204MGSFP

I(P)GS-3008

IP30-rated Series

IP30-rated L2$^+$ Industrial Managed Switch w/Enhanced G.8032 Ring



Latest update: Aug 2017

Version: 1.00

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 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

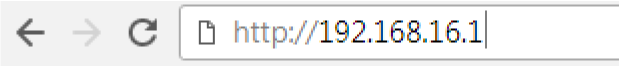
Before using the web management, install the industrial switch on the network and make sure that any one of the PCs on the network can connect with the industrial switch through the web browser.

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**

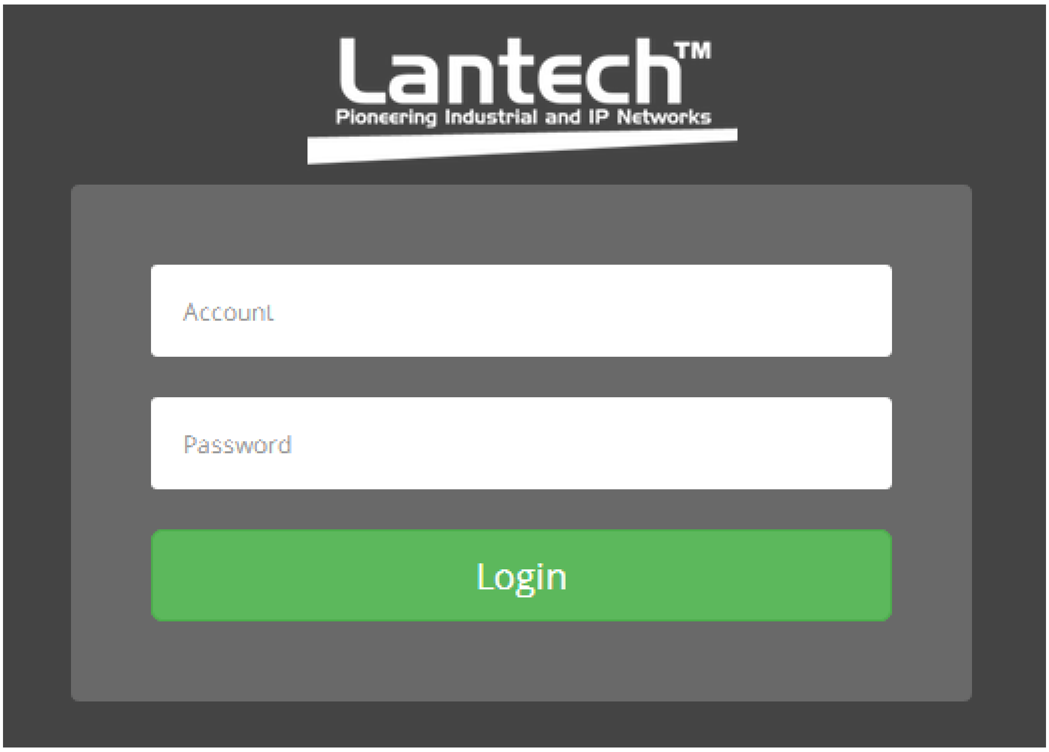
1.2 System Login

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



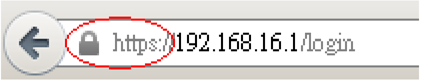
http://192.168.16.1

3. The login screen will appear right after



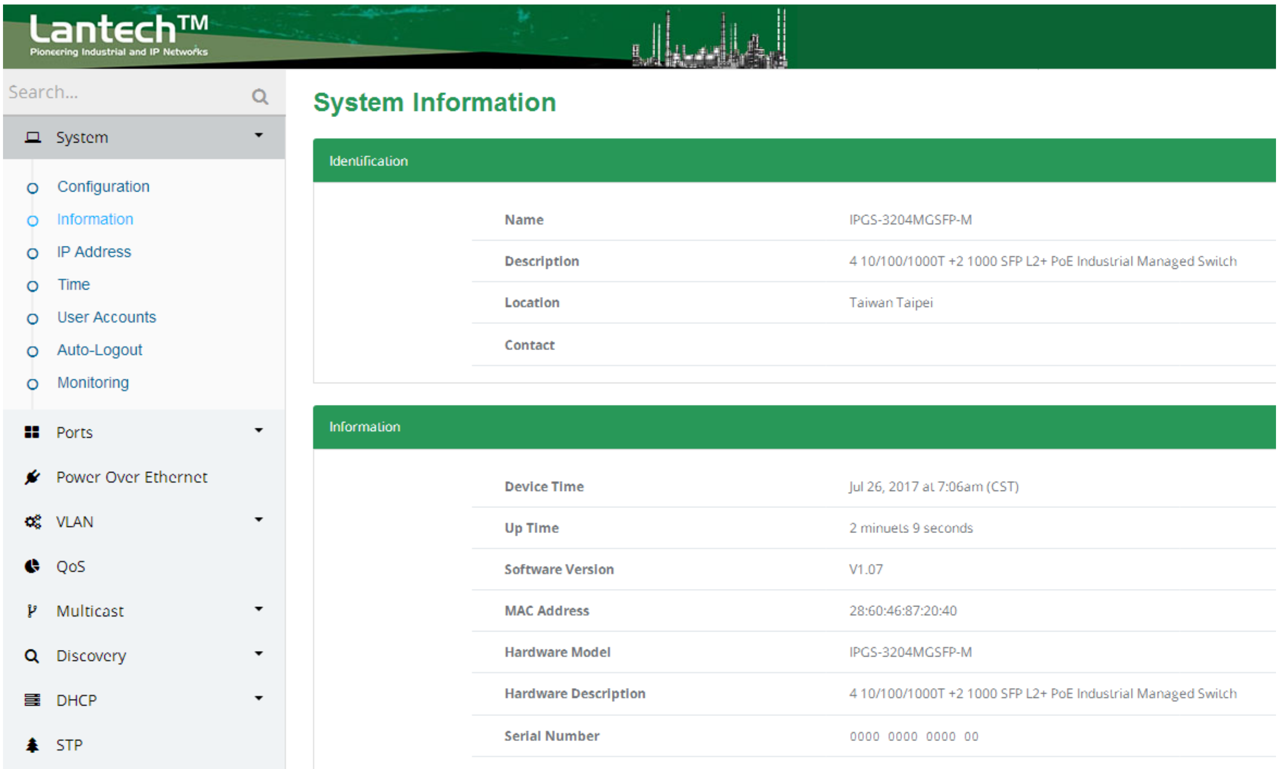
Login screen

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



System Information

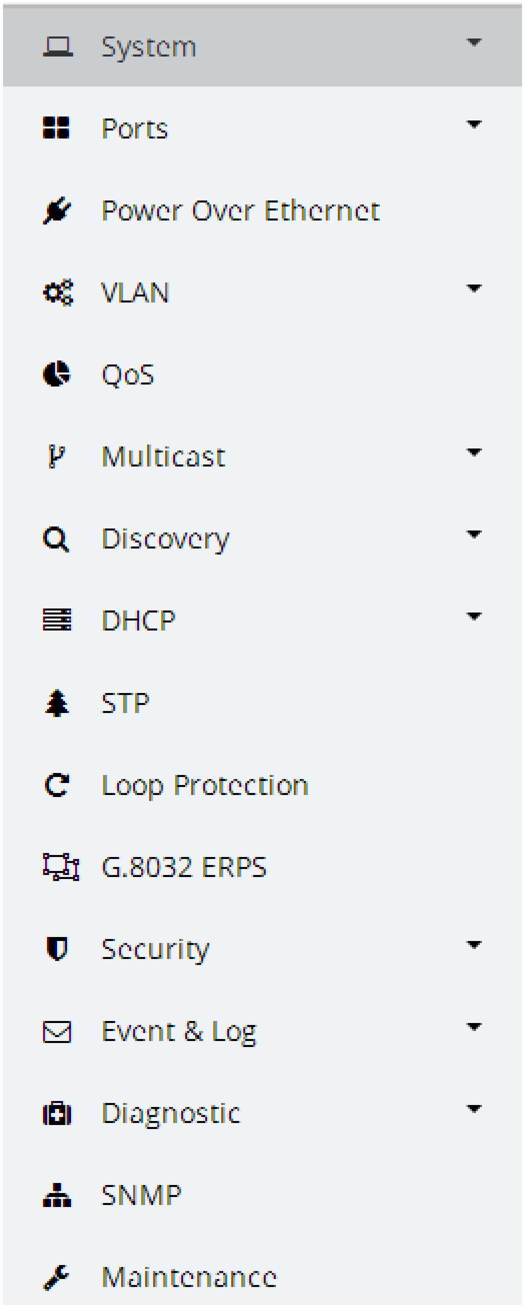
Identification

Name	IPGS-3204MGSFP-M
Description	4 10/100/1000T +2 1000 SFP L2+ PoE Industrial Managed Switch
Location	Taiwan Taipei
Contact	

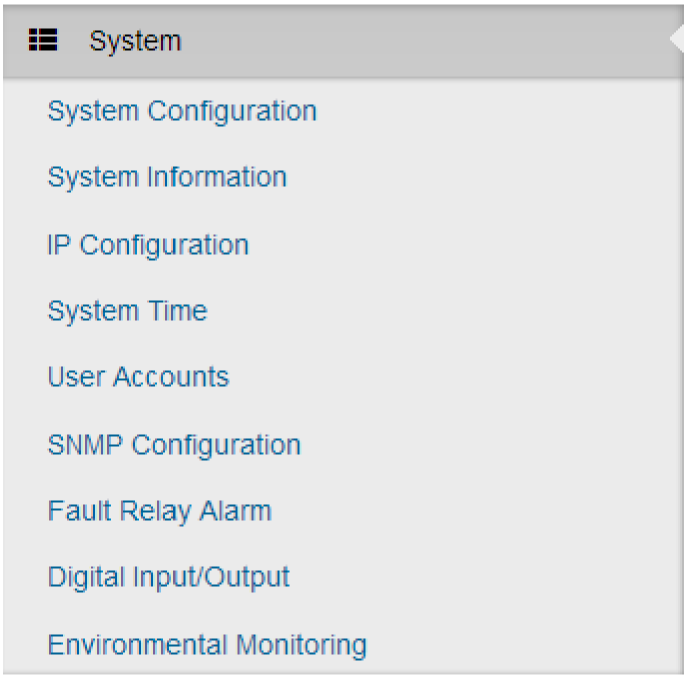
Information

Device Time	Jul 26, 2017 at 7:06am (CST)
Up Time	2 minuets 9 seconds
Software Version	V1.07
MAC Address	28:60:46:87:20:40
Hardware Model	IPGS-3204MGSFP-M
Hardware Description	4 10/100/1000T +2 1000 SFP L2+ PoE Industrial Managed Switch
Serial Number	0000 0000 0000 00

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.


System
Ports
Power Over Ethernet
VLAN
QoS
Multicast
Discovery
DHCP
STP
Loop Protection
G.8032 ERPS
Security
Event & Log
Diagnostic
SNMP
Maintenance

2. System



The “System” submenu consists of the followings:

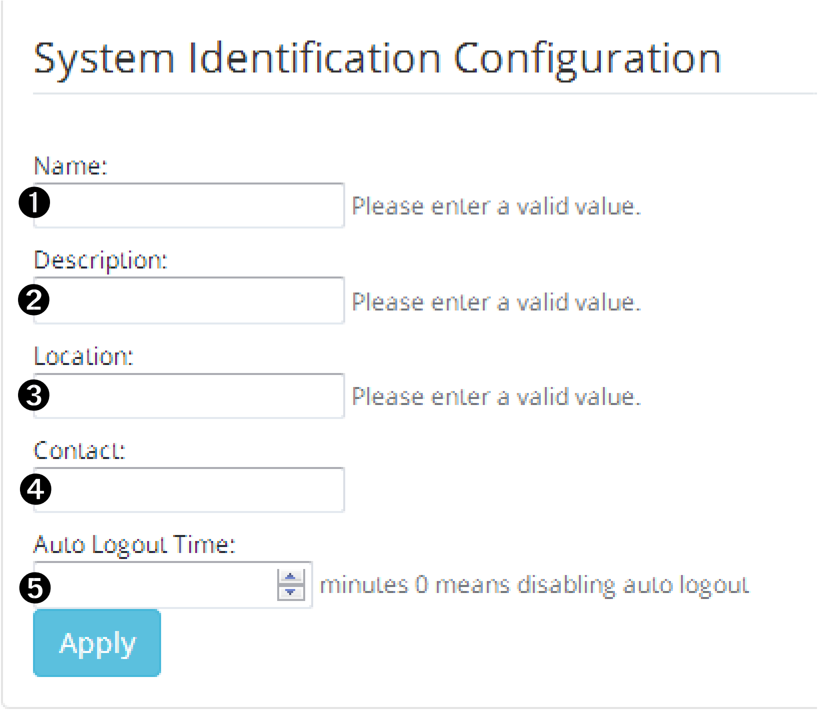
- System Configuration
- System Information
- IP Configuration
- System Time
- User Accounts
- SNMP Configuration
- Fault Relay Alarm
- Digital Input/Output
- Environment Monitoring

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



System Identification Configuration

Name:

❶ Please enter a valid value.

Description:

❷ Please enter a valid value.

Location:

❸ Please enter a valid value.

Contact:

❹

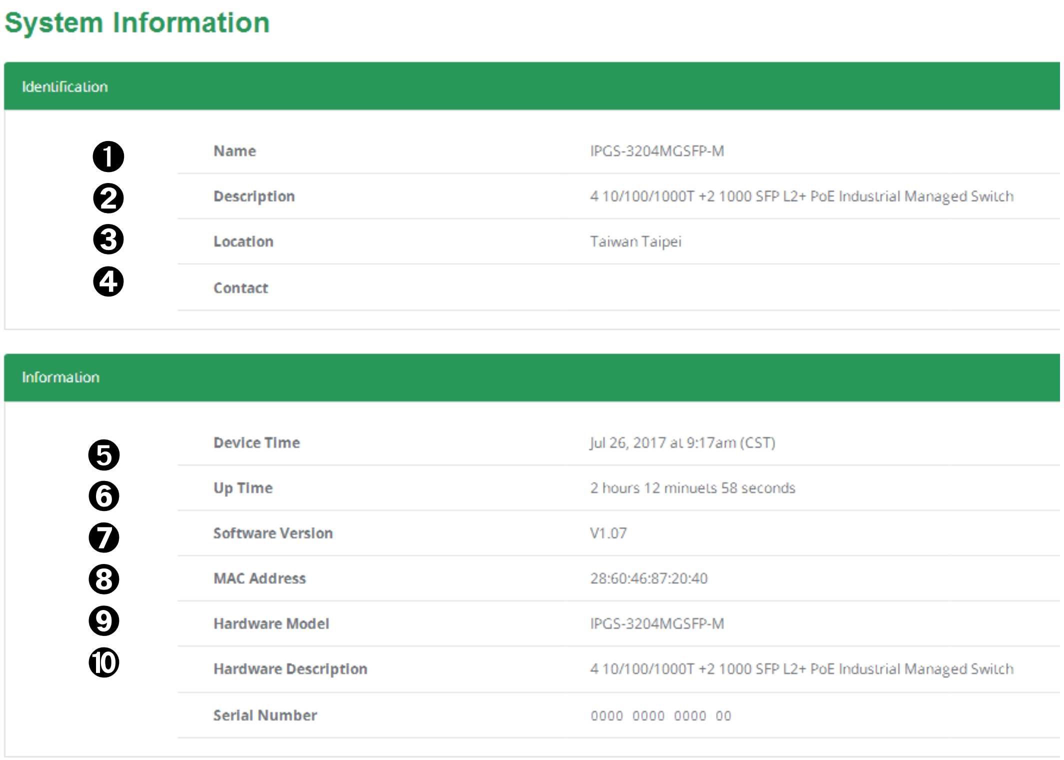
Auto Logout Time:

❺ minutes 0 means disabling auto logout

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.



System Information

Identification

❶	Name	IPGS-3204MGSFP-M
❷	Description	4 10/100/1000T +2 1000 SFP L2+ PoE Industrial Managed Switch
❸	Location	Taiwan Taipei
❹	Contact	

Information

❺	Device Time	Jul 26, 2017 at 9:17am (CST)
❻	Up Time	2 hours 12 minuets 58 seconds
❼	Software Version	V1.07
❽	MAC Address	28:60:46:87:20:40
❾	Hardware Model	IPGS-3204MGSFP-M
❿	Hardware Description	4 10/100/1000T +2 1000 SFP L2+ PoE Industrial Managed Switch
	Serial Number	0000 0000 0000 00

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

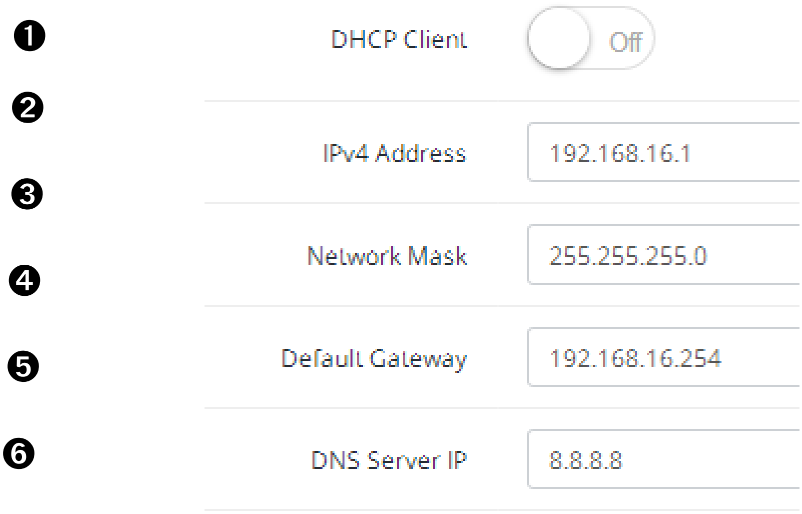
Information

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.



DHCP Client Off

IPv4 Address 192.168.16.1

Network Mask 255.255.255.0

Default Gateway 192.168.16.254

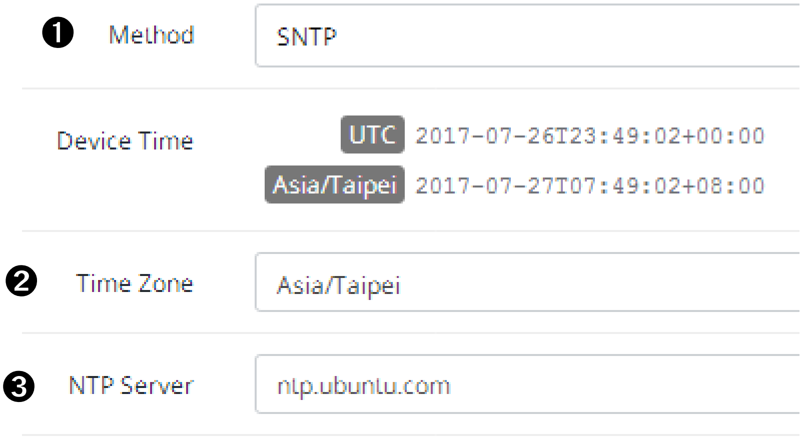
DNS Server IP 8.8.8.8

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

The Simple Network Time Protocol (SNTP) enables you to synchronize the system time in your network. The switch supports the SNTP client and the SNTP server function. The SNTP server runs the UTC (Universal Time Coordinated) measurement which will correspond to SNTP client that will adjust to local time zone. However, the local time difference will not be taken into account.



❶ Method: SNTP

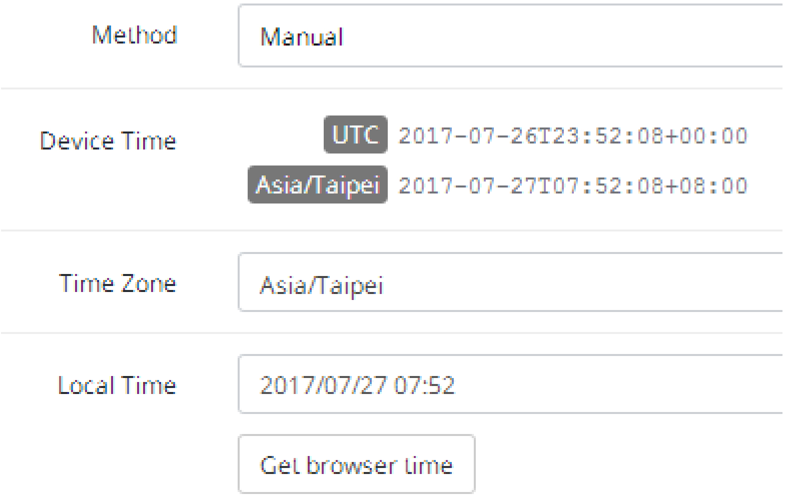
Device Time: UTC 2017-07-26T23:49:02+00:00
Asia/Taipei 2017-07-27T07:49:02+08:00

❷ Time Zone: Asia/Taipei

❸ NTP Server: ntp.ubuntu.com

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td><b>❷ Time Zone:</b></td><td>Universal Time Coordinated. Set the switch location time zone. The following table lists the different location time zone for your reference.
<table>
<tr><th>Possible Values</th><th>Default Setting</th></tr>
<tr><td>Please refer to the “Table: Location Time Zone” below</td><td>None</td></tr>
</table></td></tr>
<tr><td><b>❶ Method:</b></td><td>You can set the time of switch manually or set SNTP server to let the switch synch the time with SNTP server via internet.
<table>
<tr><th>Possible Values</th><th>Default Setting</th></tr>
<tr><td>Manual, SNTP</td><td>SNTP</td></tr>
</table></td></tr>
<tr><td><b>❸ SNTP server:</b></td><td>The IP address of SNTP server.</td></tr>
</table>

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.



Method: Manual

Device Time: UTC 2017-07-26T23:52:08+00:00
Asia/Taipei 2017-07-27T07:52:08+08:00

Time Zone: Asia/Taipei

Local Time: 2017/07/27 07:52

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

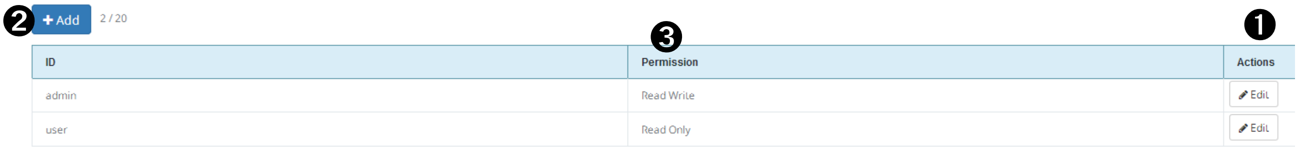
Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - 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.

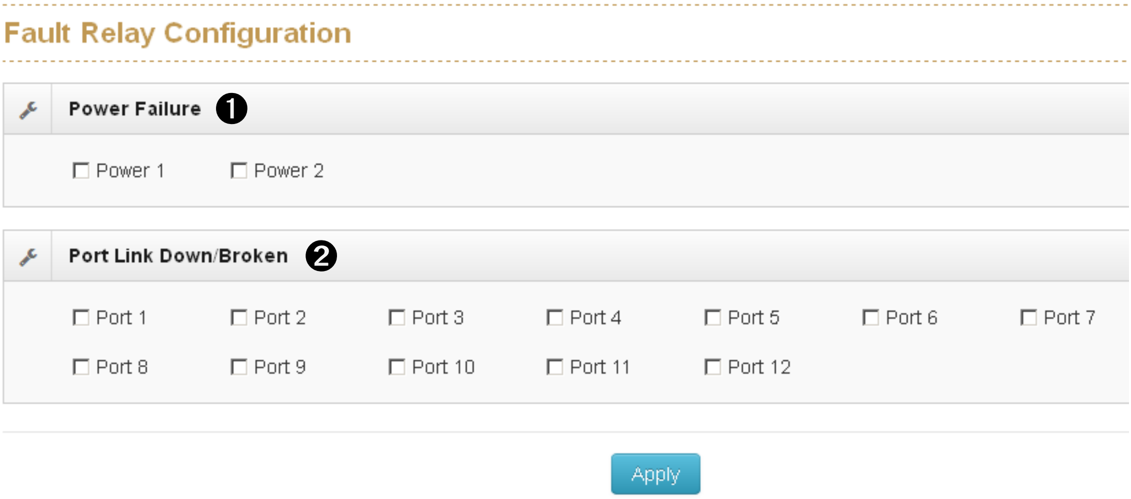


ID	Permission	Actions
admin	Read Write	Edit
user	Read Only	Edit

Name	Description
❶ **Actions:**	Reset the password of an account
❷ **Add:**	Press to add new account
❸ **Permission:**	Permission level of an account

2.6. 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.



Fault Relay Configuration

Power Failure ❶

□ Power 1 □ Power 2

Port Link Down/Broken ❷

□ Port 1 □ Port 2 □ Port 3 □ Port 4 □ Port 5 □ Port 6 □ Port 7
□ Port 8 □ Port 9 □ Port 10 □ Port 11 □ Port 12

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.

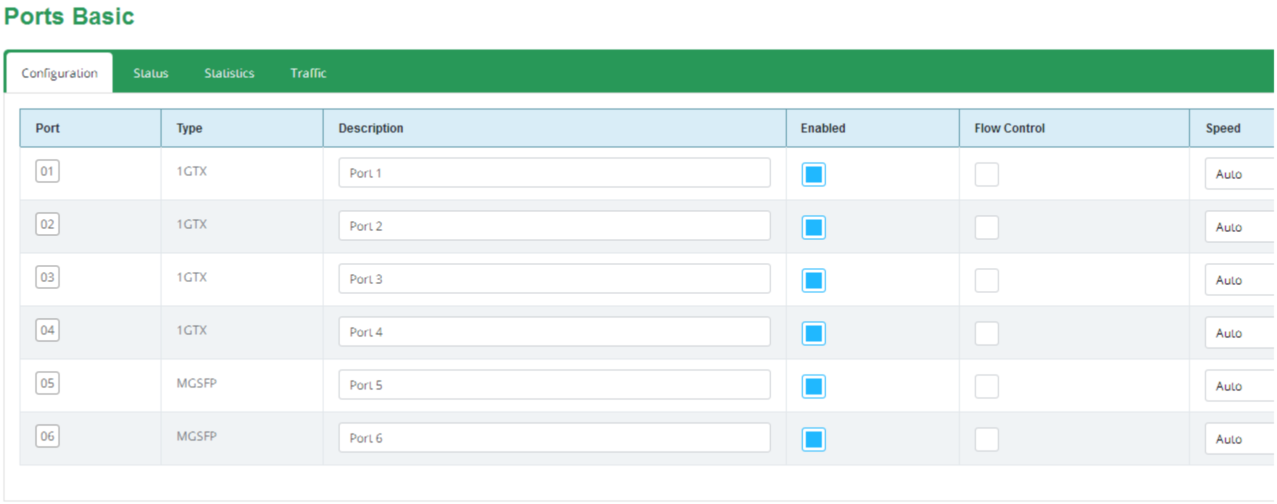
3. Ports Basic

This configuration table allows you to configure each port of the device and also display each port‘s current mode of operation (link state, bit rate (speed) and duplex mode).

3.1. Configuration

This page displays current port configurations. Ports can also be configured here.

The port settings relate to the currently selected stack unit, as reflected by the page header.

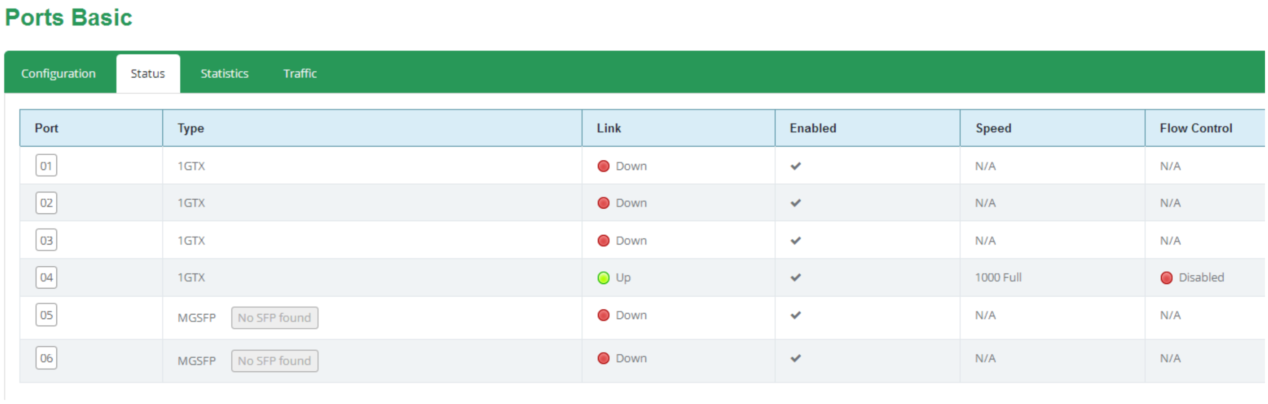


Port	Type	Description	Enabled	Flow Control	Speed
01	1GTX	Port 1	☑	□	Auto
02	1GTX	Port 2	☑	□	Auto
03	1GTX	Port 3	☑	□	Auto
04	1GTX	Port 4	☑	□	Auto
05	MGSFP	Port 5	☑	□	Auto
06	MGSFP	Port 6	☑	□	Auto

Name	Meaning
Port:	This is the logical port number for this row.
Type:	Media type of port
Description:	Enter up to 47 characters to be descriptive name for identifies this port.
Enabled:	The port can be set to disable or enable mode. If the port setting is disable then will not receive or transmit any packet.
Flow Control:	Set flow control function of the port.
Speed:	Selects any available link speed for the given switch port. Only speed supported by the specific port is shown.

	Possible Values	Default Setting
	Disabled – Disables the switch port operation. **Auto** – Let switch port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner. 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

3.2. Status

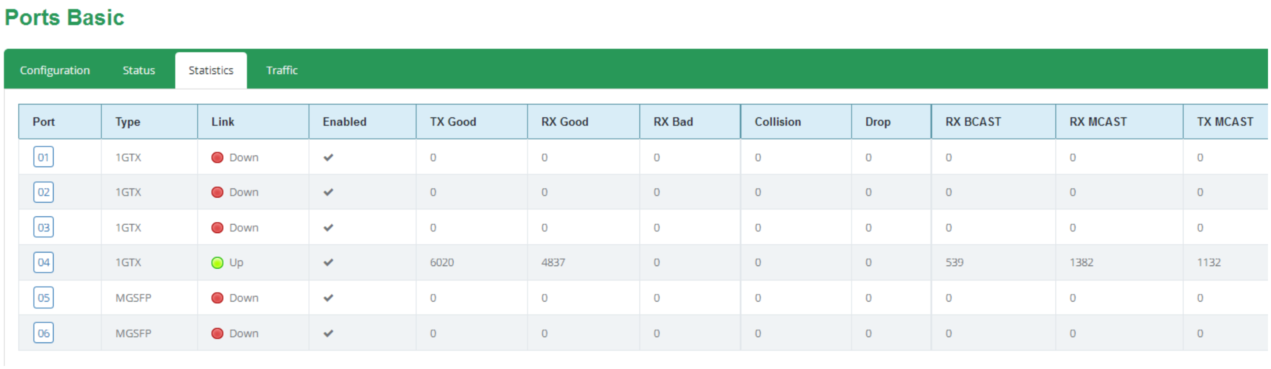


Ports Basic

Port	Type	Link	Enabled	Speed	Flow Control
01	1GTX	● Down	✓	N/A	N/A
02	1GTX	● Down	✓	N/A	N/A
03	1GTX	● Down	✓	N/A	N/A
04	1GTX	● Up	✓	1000 Full	● Disabled
05	MGSFP No SFP found	● Down	✓	N/A	N/A
06	MGSFP No SFP found	● Down	✓	N/A	N/A

Name	Meaning
Port No:	This is the logical port number for this row.
Type:	This is the logical port type.
Link:	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
Speed:	Provides the current link speed of the port.
Flow Control:	Status of Flow Control

3.3. Statistics



Ports Basic

Port	Type	Link	Enabled	TX Good	RX Good	RX Bad	Collision	Drop	RX BCAST	RX MCAST	TX MCAST
01	1GTX	● Down	✓	0	0	0	0	0	0	0	0
02	1GTX	● Down	✓	0	0	0	0	0	0	0	0
03	1GTX	● Down	✓	0	0	0	0	0	0	0	0
04	1GTX	● Up	✓	6020	4837	0	0	0	539	1382	1132
05	MGSFP	● Down	✓	0	0	0	0	0	0	0	0
06	MGSFP	● Down	✓	0	0	0	0	0	0	0	0

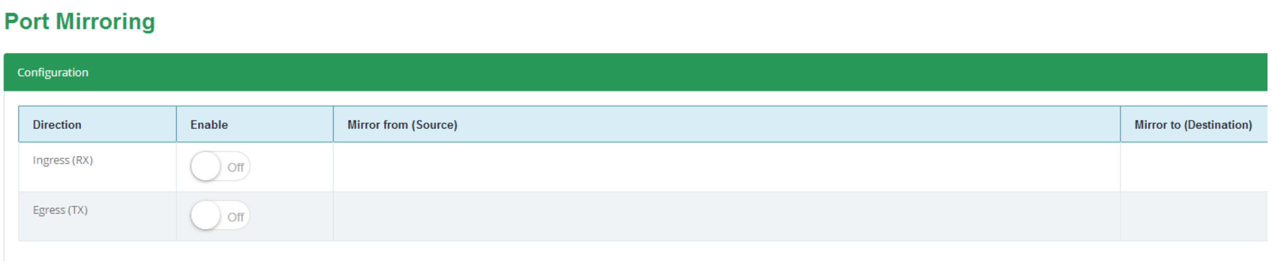
Name	Meaning
Port:	The logical port for the settings contained in the same row.
Type:	Displays the current speed of connection to the port.
Link:	The status of linking - Up or Down.
State:	It's set by Port Control. When the state is disabled, the port will

	not transmit or receive any packet.
Tx Good Packet:	The counts of transmitting good packets via this port.
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.
Rx Good Packet:	The counts of receiving good packets via this port.
Rx Bad Packet:	The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
Tx Abort Packet:	The aborted packet while transmitting.
Packet Collision:	The counts of collision packet.
Packet Dropped:	The counts of dropped packet.
Rx Bcast Packet:	The counts of broadcast packet.
Rx Mcast Packet:	The counts of multicast packet.

3.4. **Mirroring**

The Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port. That means traffic goes in or out monitored (source) ports will be duplicated into mirror (destination) port.

Destination Port: There is only one port can be selected to be destination (mirror) port for monitoring both RX and TX traffic which come from source port.
Source Port: The ports that user wants to monitor. All monitored port traffic will be copied to mirror (destination) port.



Port Mirroring

Configuration

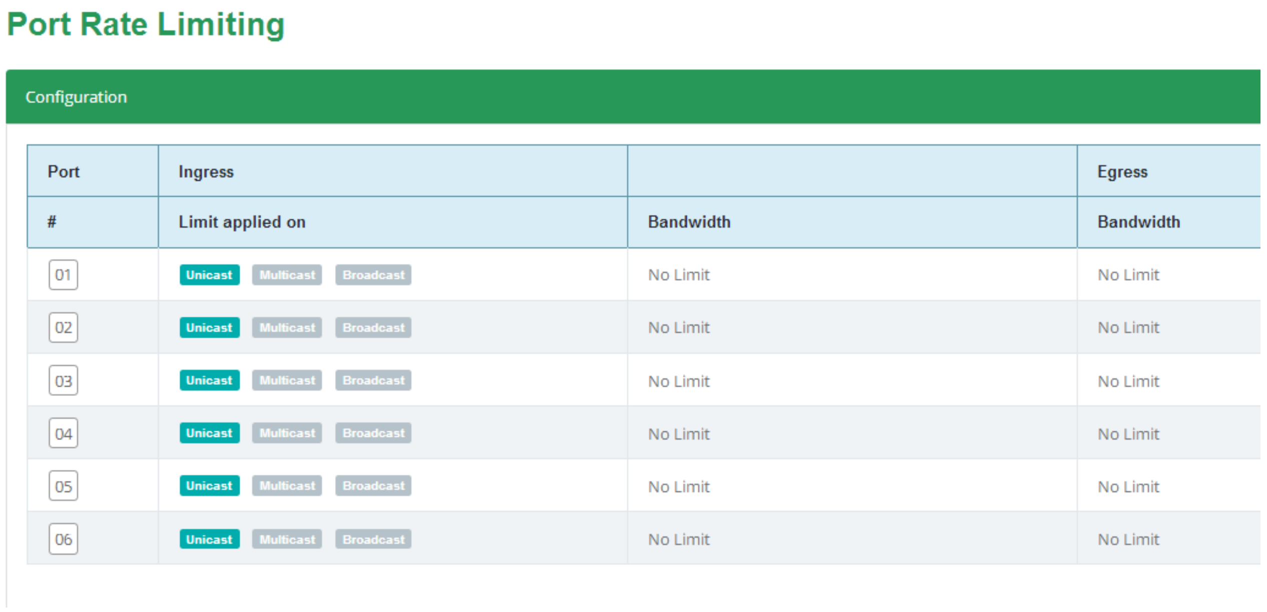
Direction	Enable	Mirror from (Source)	Mirror to (Destination)
Ingress (RX)	Off		
Egress (TX)	Off		

Name	Meaning
Enable:	Enable or disable port mirror function
Mirror from(Source):	The port which you want to monitor
Mirror to(Destination):	The port which you use to connect monitoring equipment

3.5. Rate Limiting

You can set up every port's bandwidth rate and frame limitation type.

Ingress Limit Frame type: select the frame type that wants to filter. The frame types have 4 options for selecting: All, broadcast/ multicast/ flooded unicast, broadcast/ multicast, and broadcast only. These 4 types are only for ingress packet. The egress rate only supports all type packets.



Port Rate Limiting

Configuration

Port	Ingress		Egress
#	Limit applied on	Bandwidth	Bandwidth
01	Unicast Multicast Broadcast	No Limit	No Limit
02	Unicast Multicast Broadcast	No Limit	No Limit
03	Unicast Multicast Broadcast	No Limit	No Limit
04	Unicast Multicast Broadcast	No Limit	No Limit
05	Unicast Multicast Broadcast	No Limit	No Limit
06	Unicast Multicast Broadcast	No Limit	No Limit

<table>
<tr><th>Name</th><th>Meaning</th></tr>
<tr><td><b>Limit applied on:</b></td><td>All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set it's 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>Possible Values</th><th>Default Setting</th></tr>
<tr><td>1. All
2. broadcast/ multicast/ flooded unicast
3. broadcast/ multicast
4. broadcast only</td><td>N/A</td></tr>
</table></td></tr>
<tr><td><b>Ingress:</b></td><td>Enter the port effective ingress rate (The default value is "0").</td></tr>
<tr><td><b>Egress:</b></td><td>Enter the port effective egress rate (The default value is "0").</td></tr>
</table>

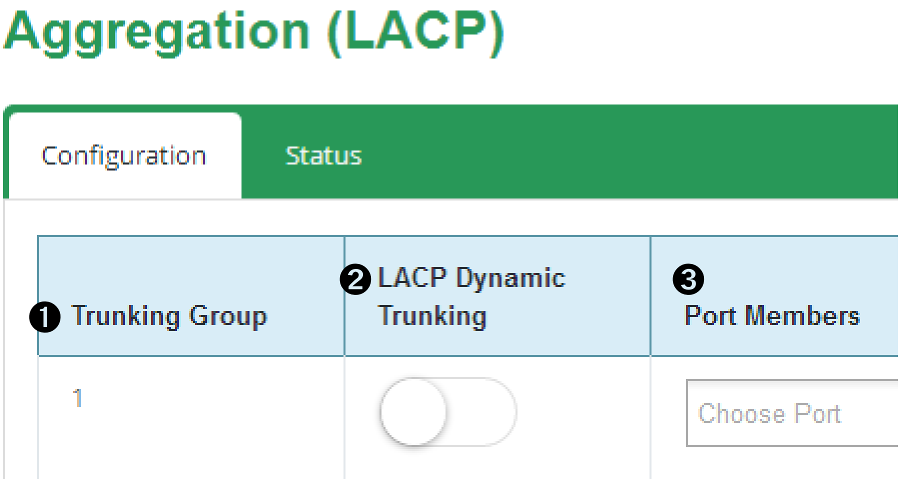
4. Aggregation

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

4.1. Aggregation Configuration

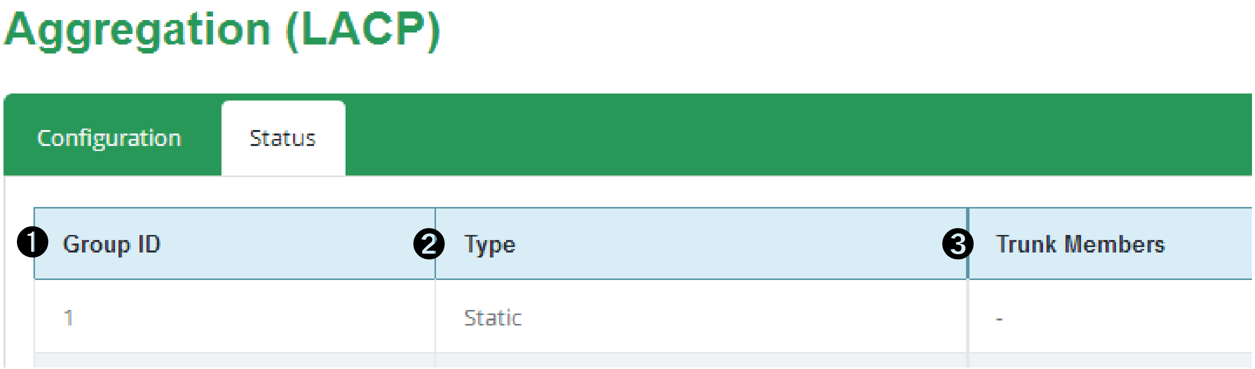


Group Configuration

Name	Description
❶ **Trunking Group:**	Number of trunk group
❷ **LACP**	Enable LACP Dynamic Trunk function by clicking the box

Dynamic Trunking:	
❸ **Port Members:**	Select which ports you want to aggregate with

4.2. Aggregation Status



❶ Group ID	❷ Type	❸ Trunk Members
1	Static	-

Name	Description
❶ **Group ID**	Number of trunk group
❷ **Type**	'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 **Trunk members**	Switch ports which bind the trunk group

5. 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.

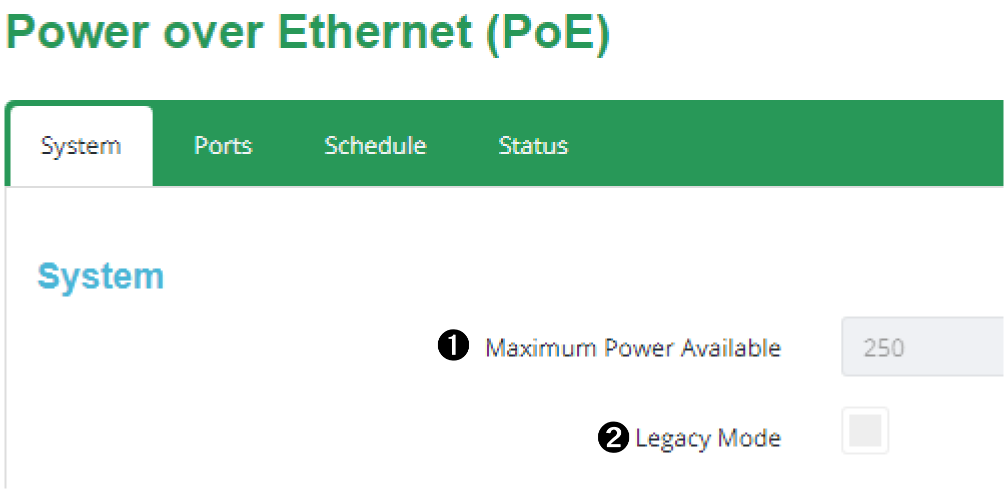
There are several common techniques for transmitting power over Ethernet cabling. Two of them have been standardized by IEEE 802.3 since 2003. These standards are known as *Alternative A* and *Alternative B*. For 10BASE-T and 100BASE-TX, only two of the four data/signal pairs in typical CAT-5 cable are 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.

5.1. System

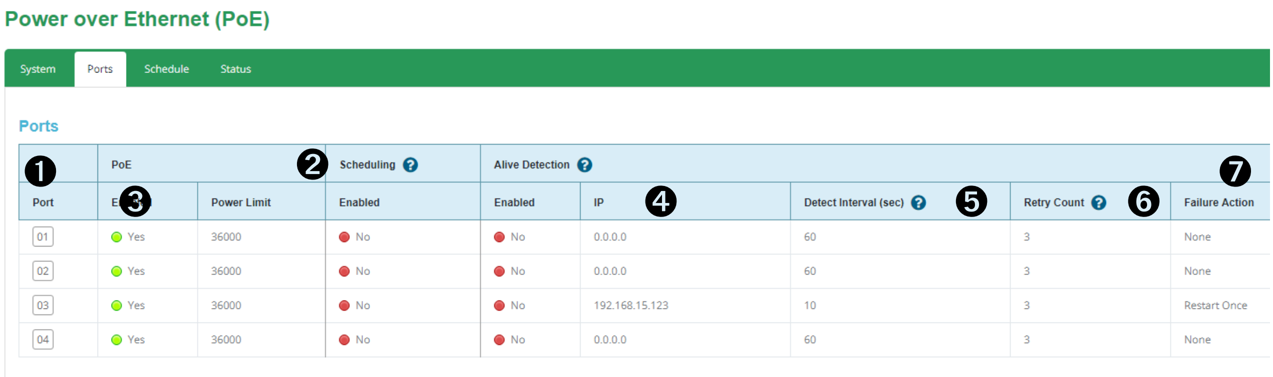


❶ Maximum Power Available: 250

❷ Legacy Mode □

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>❶ Maximum Power Available:</td><td>Define the limit of total power consumption.</td></tr>
<tr><td>❷ Legacy mode:</td><td>Force switch to supply power to legacy PD.</td></tr>
<tr><td>❸ Port :</td><td>Number of the PoE port.</td></tr>
<tr><td>❹ Scheduling:</td><td>The PoE port is under control with PoE scheduling function.</td></tr>
<tr><td>❺ Enable:</td><td>Enable or disable PoE function of the port.</td></tr>
<tr><td>❻ Priority:</td><td>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.
<table>
<tr><th>Priority Options</th><th>Default Setting</th></tr>
<tr><td>Low / High/ Critical</td><td>Low</td></tr>
</table></td></tr>
<tr><td>❼ Power Limit:</td><td>Define the maximum power of the PoE port.</td></tr>
</table>

5.2. Ports

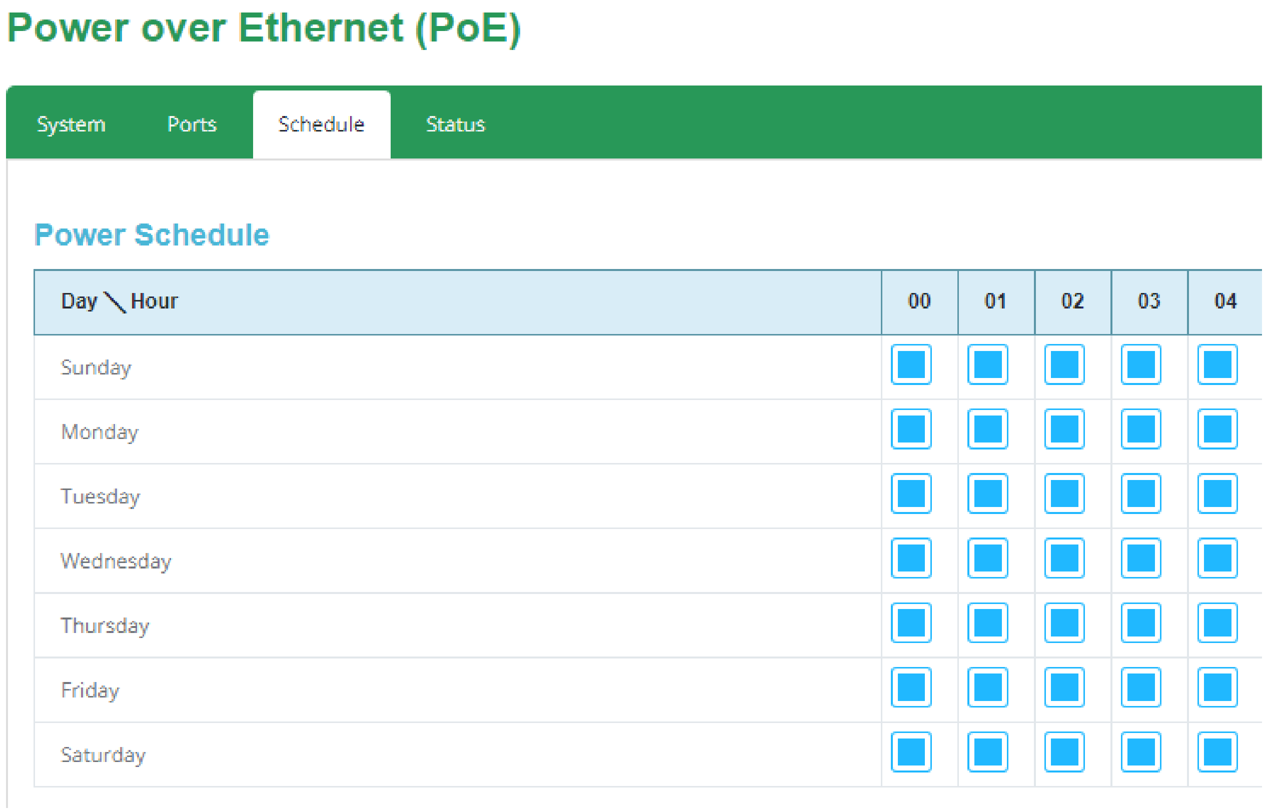


Ports

Port	PoE		Scheduling	Alive Detection				
	E❸d	Power Limit	Enabled	Enabled	IP	Detect Interval (sec)	Retry Count	Failure Action
01	● Yes	36000	● No	● No	0.0.0.0	60	3	None
02	● Yes	36000	● No	● No	0.0.0.0	60	3	None
03	● Yes	36000	● No	● No	192.168.15.123	10	3	Restart Once
04	● Yes	36000	● No	● No	0.0.0.0	60	3	None

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td><b>❶ Port:</b></td><td>Number of the PoE port</td></tr>
<tr><td><b>❷ Scheduling:</b></td><td>The PoE port is under control with PoE scheduling function.</td></tr>
<tr><td><b>❸ Enable:</b></td><td>Enable or disable PoE function of the port.</td></tr>
<tr><td><b>❹ IP:</b></td><td>IP address of PD.</td></tr>
<tr><td><b>❺ Detect Interval:</b></td><td>Detecting interval time.</td></tr>
<tr><td><b>❻ Retry Count:</b></td><td>How many times you want to retry to make sure the PD is fail.</td></tr>
<tr><td><b>❼ Failure Action:</b></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 only with the PoE Port.</td><td>Nothing</td></tr>
</table>
</td></tr>
</table>

5.3. Scheduling



Power over Ethernet (PoE)

Power Schedule

Day ╲ Hour	00	01	02	03	04
Sunday	☑	☑	☑	☑	☑
Monday	☑	☑	☑	☑	☑
Tuesday	☑	☑	☑	☑	☑
Wednesday	☑	☑	☑	☑	☑
Thursday	☑	☑	☑	☑	☑
Friday	☑	☑	☑	☑	☑
Saturday	☑	☑	☑	☑	☑

Set the PoE power-on schedule of a week.

6. 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

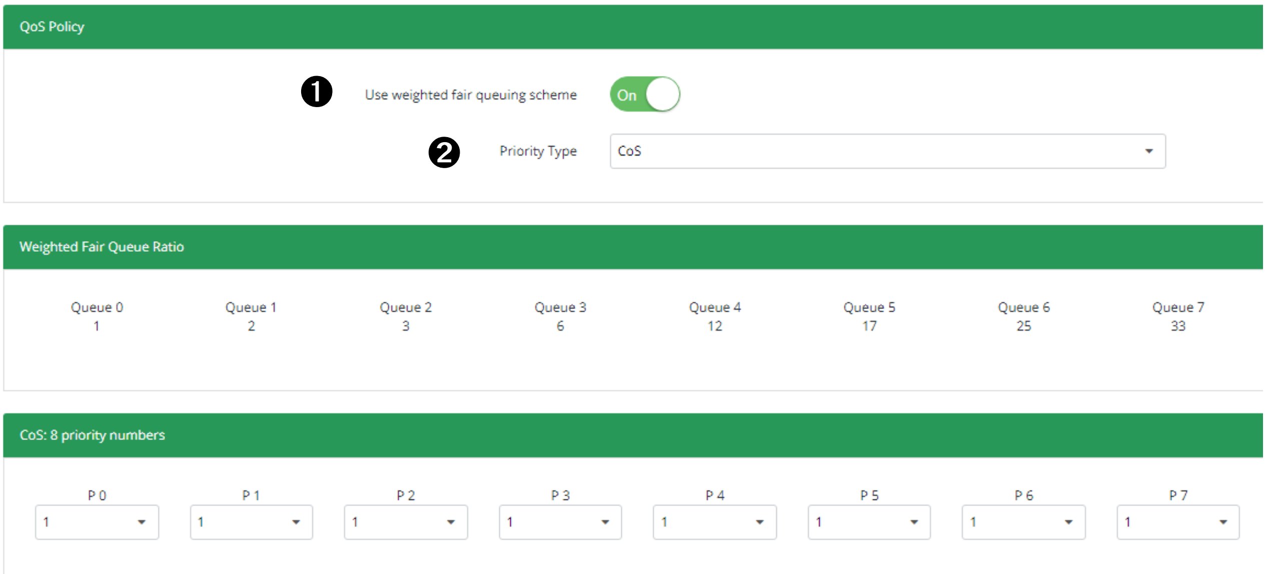
QoS Policy

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.

QoS Policy



QoS Policy

❶ Use weighted fair queuing scheme: On

❷ Priority Type: CoS

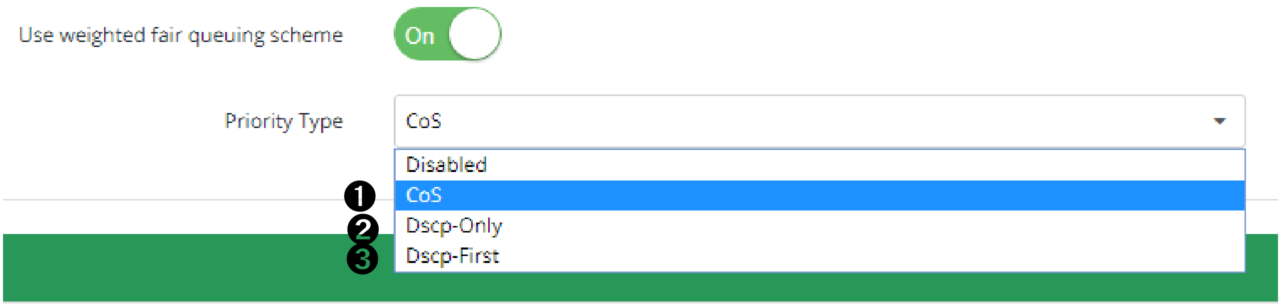
Weighted Fair Queue Ratio

Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
1	2	3	6	12	17	25	33

CoS: 8 priority numbers

P 0	P 1	P 2	P 3	P 4	P 5	P 6	P 7
1	1	1	1	1	1	1	1

Name	Description
❶ **Using the weight fair queue scheme:**	The switch will follow 33:25:17:12:6:3:2:1 rate to process priority queue from High to lowest queue.
❷ **Priority Type:**	■ **CoS:** the port priority will only follow the CoS priority that you have assigned. ■ **DSCP only:** the port priority will only follow the ToS priority that you have assigned. ■ **DSCP first:** the port priority will follow the ToS priority first, and the other priority rule.



Use weighted fair queuing scheme On

Priority Type CoS

Name	Description
❶ **Cos:**	Set the CoS priority level 0~7.
❷ **DSCP-Only:**	System provides 0~63 ToS priority level.
❸ **DSCP-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.

7. 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.

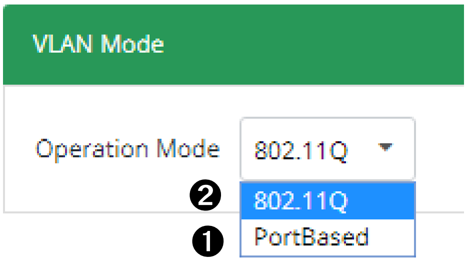
VLANs allow network administrators to group hosts together even if the hosts are not on the same network switch. This can greatly simplify network design and deployment, because VLAN membership can be configured through software. Without VLANs, grouping hosts according to their resource needs necessitates 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

7.1. Operation Mode

Set Port based VLAN or 802.1Q VLAN

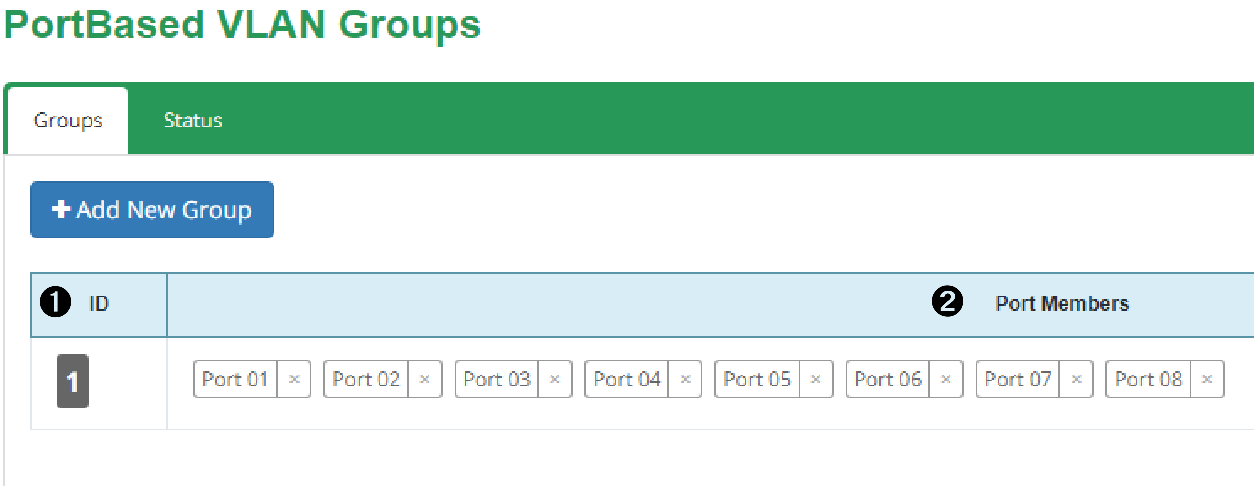


VLAN Mode

Operation Mode: 802.11Q

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

7.2. Port-based VLAN Groups

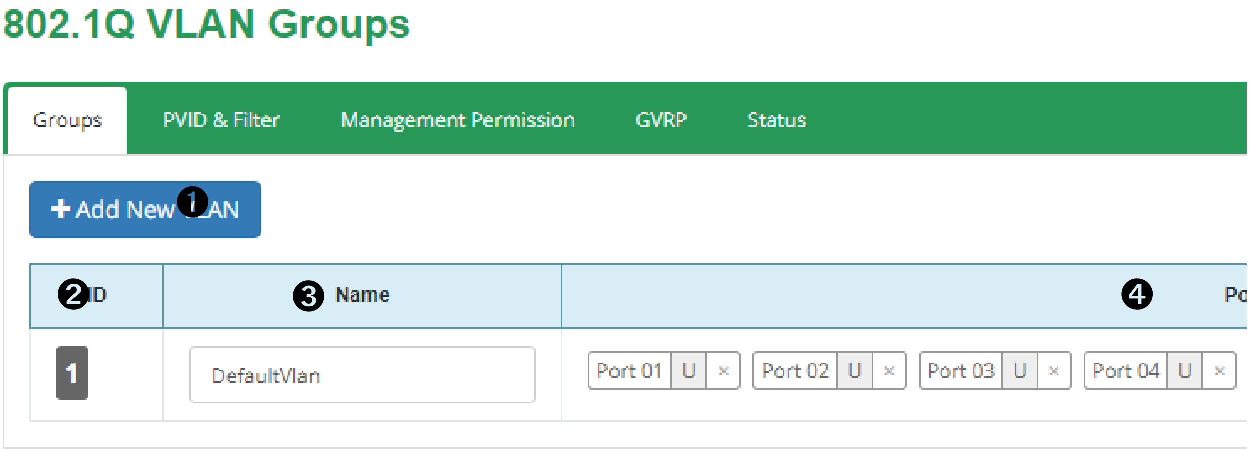


PortBased VLAN Groups

❶ ID	❷ Port Members
1	Port 01 × Port 02 × Port 03 × Port 04 × Port 05 × Port 06 × Port 07 × Port 08 ×

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

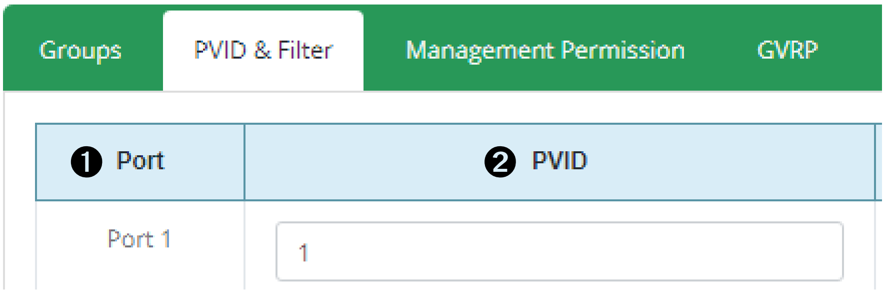
7.3. 802.1Q VLAN Groups



Name	Description
❶ **+Add new VLAN:**	Press to add new VLAN.
❷ **ID:**	Index number of VLAN group
❸ **Name:**	Name of VLAN group.
❹ **Port:**	Select member port of VLAN group, Mark “U” means Untagged port(access port) , 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. Mark “T” means tagged port(trunk port), 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.

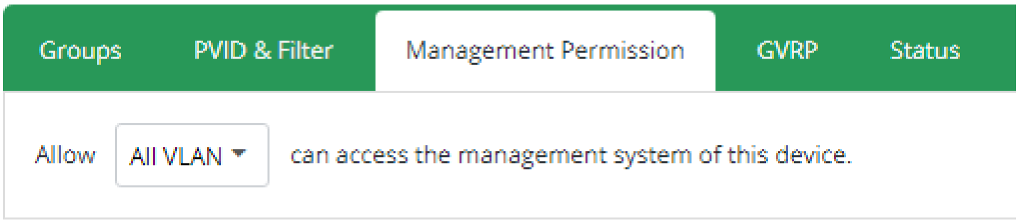
7.4. PVID & Filter



❶ Port	❷ PVID
Port 1	1

Name	Description
❶ **Port:**	Port number of switch.
❷ **PVID:**	ID of VLAN group

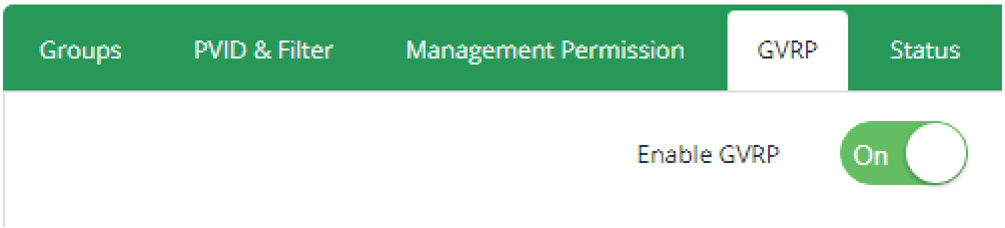
7.5. Management Permission



Allow All VLAN can access the management system of this device.

Set which VLAN can be allowed to access switch management interface.

7.6. GVRP

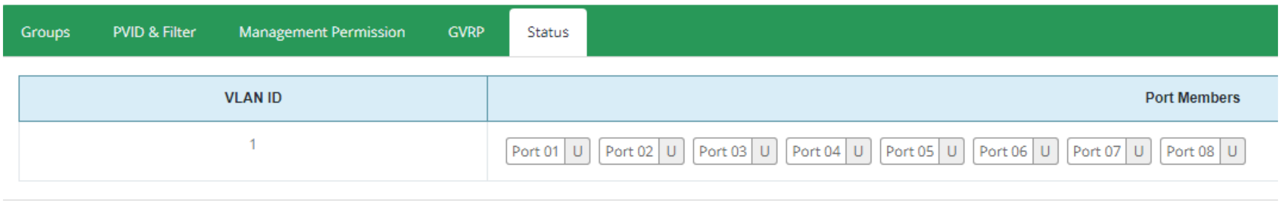


Enable GVRP: On

GVRP is a GARP application that provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports.

7.7. Status

Display the status of each VLAN group.



VLAN ID	Port Members
1	Port 01 U Port 02 U Port 03 U Port 04 U Port 05 U Port 06 U Port 07 U Port 08 U

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

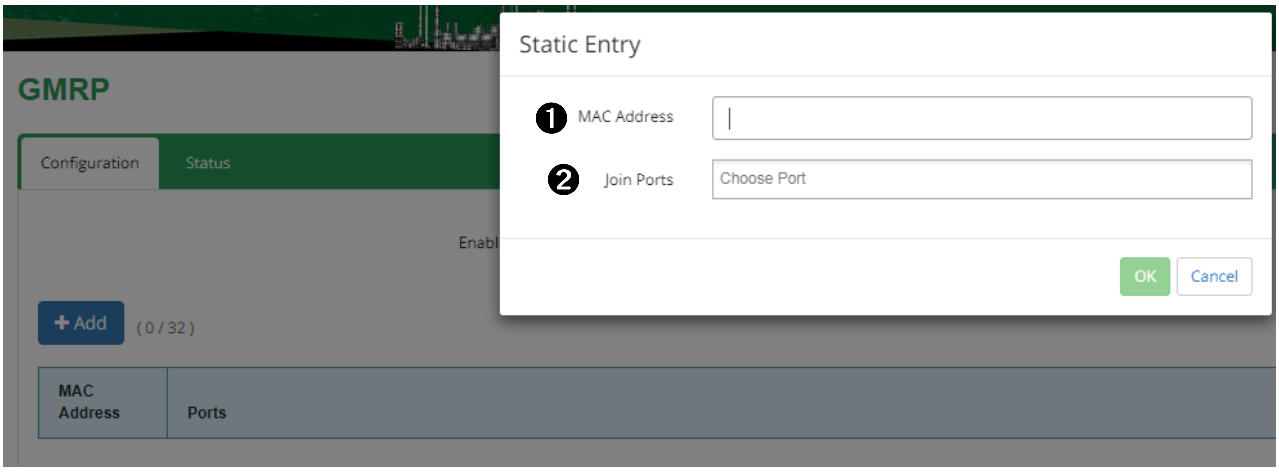
8. Multicast

In computer networking, multicast is group communication where information is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution. Multicast should not be confused with physical layer point-to-multipoint communication.

Group communication may either be application layer multicast or network assisted multicast, where the latter makes it possible for the source to efficiently send to the group in a single transmission. Copies are automatically created in other network elements, such as routers, switches and cellular network base stations, but only to network segments that currently contain members of the group.

8.1. GMRP

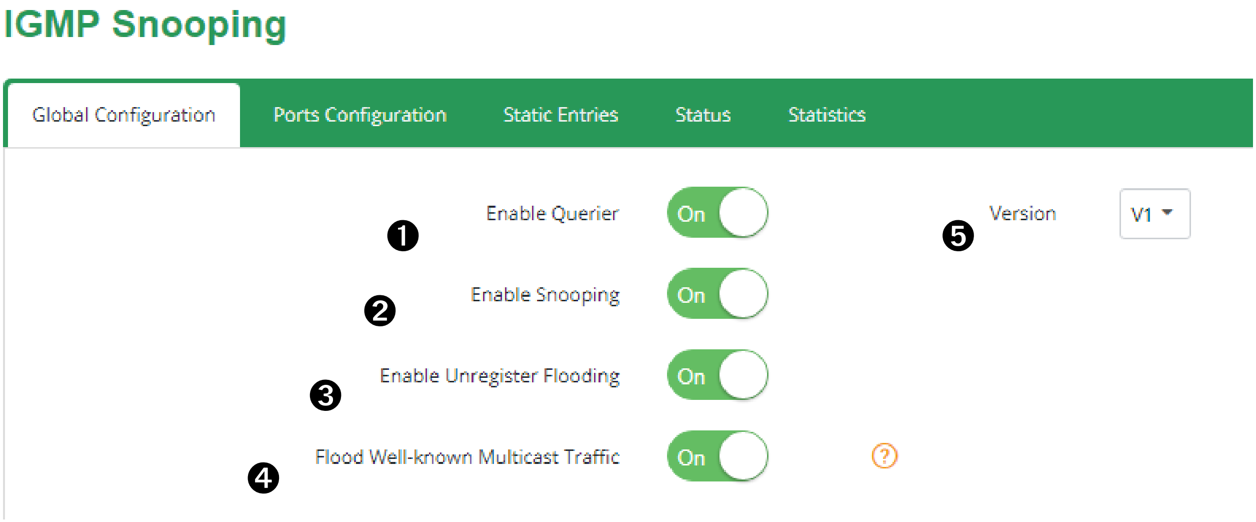
GMRP provides a mechanism that allows bridges and end stations to dynamically register group membership information with the MAC bridges attached to the same LAN segment and for that information to be disseminated across all bridges in the Bridged LAN that supports extended filtering services. The operation of GMRP relies upon the services provided by the GARP



Name	Description
❶ **MAC Address:**	MAC address of ending device

❷ **Join port:**	Which port will be assigned with ending device

8.2. IGMP Snooping



Enable Querier: On

Enable Snooping: On

Enable Unregister Flooding: On

Flood Well-known Multicast Traffic: On

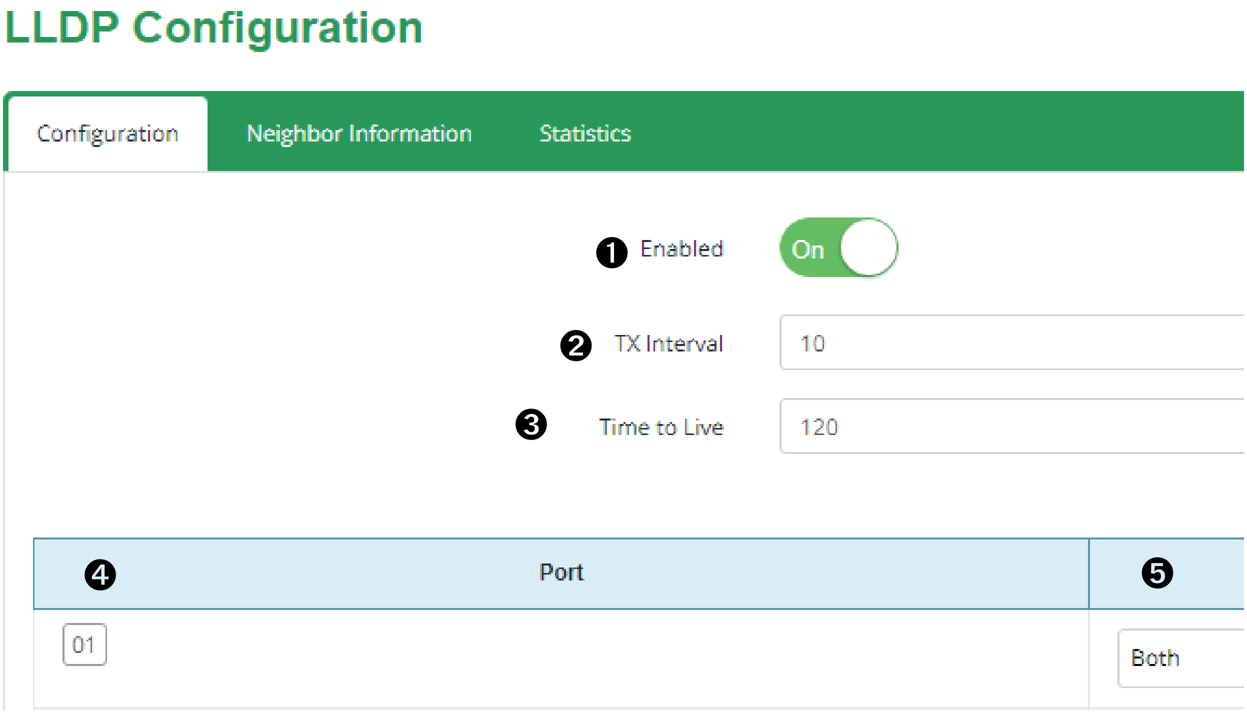
Version: V1

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

Name	Description
❶ **Enable Querior:**	Enable or disable IGMP querior.
❷ **Enable Snooping:**	Enable or disable IGMP Snooping
❸ **Enable Unregister Flooding:**	Allow switch to flood all unregister Multicast stream
❹ **Flood Well-known Multicast Traffic:**	Allow switch to flood all well-known Multicast stream
❺ **Version Name:**	Version of IGMP protocol.

9. Discovery

9.1. LLDP Configuration



LLDP Configuration

Configuration | Neighbor Information | Statistics

❶ Enabled: On

❷ TX Interval: 10

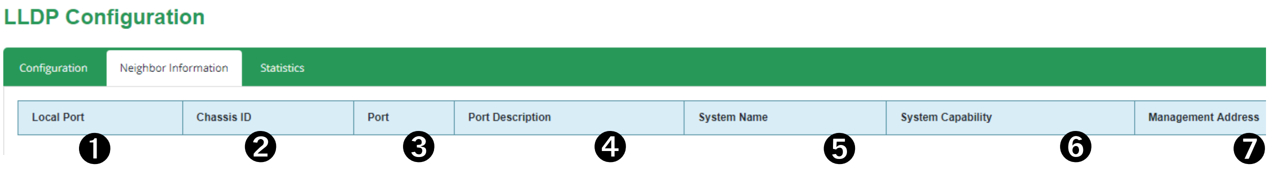
❸ Time to Live: 120

❹ Port	❺
01	Both

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 **Time to live:**	How long will the switch keep all LLDP information.
❹ **Port :**	The switch port number for LLDP mode.
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.

9.2. LLDP Neighbor Information



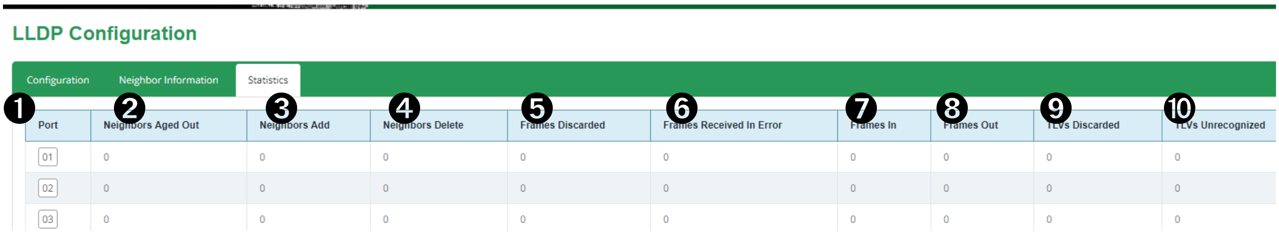
This page provides a status-quo for all LLDP neighbors. The table shows the LLDP neighbor information that contains the followings:

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 Capabilities:**	It describes the neighbor unit's capabilities which include the 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.

9.3. Statistics

This page provides an overview of all LLDP traffic.



Port	Neighbors Aged Out	Neighbors Add	Neighbors Delete	Frames Discarded	Frames Received In Error	Frames In	Frames Out	TLVs Discarded	TLVs Unrecognized
01	0	0	0	0	0	0	0	0	0
02	0	0	0	0	0	0	0	0	0
03	0	0	0	0	0	0	0	0	0

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.

10. 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.

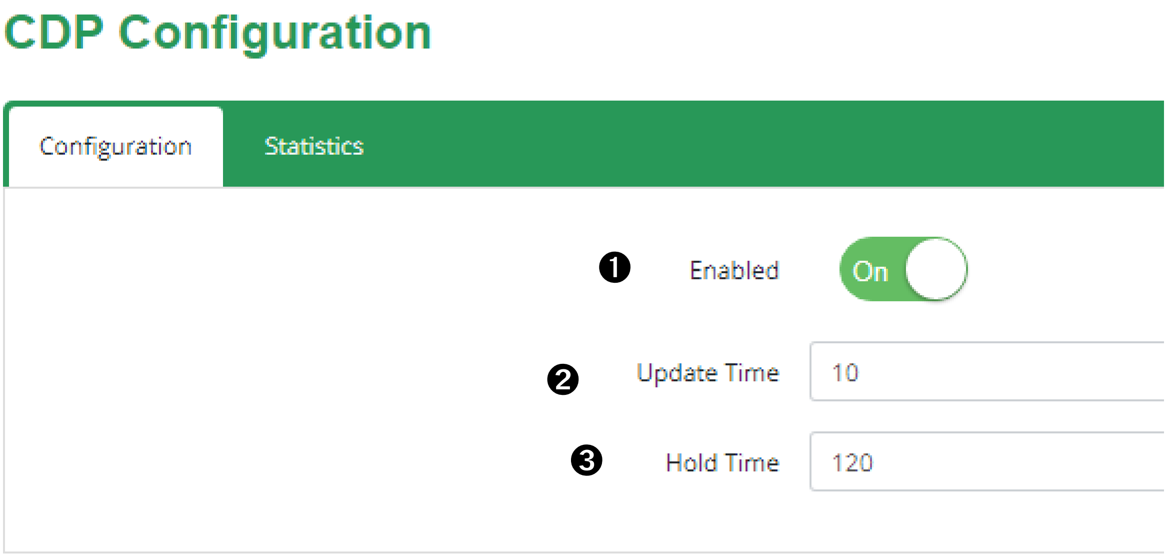
Cisco devices send CDP announcements to the multicast destination address 01-00-0c-cc-cc-cc, out each connected network interface. These multicast frames may be received by Cisco switches and other networking devices that support CDP into their connected network interface. This multicast destination 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

10.1. CDP Configuration Device Settings


CDP Configuration

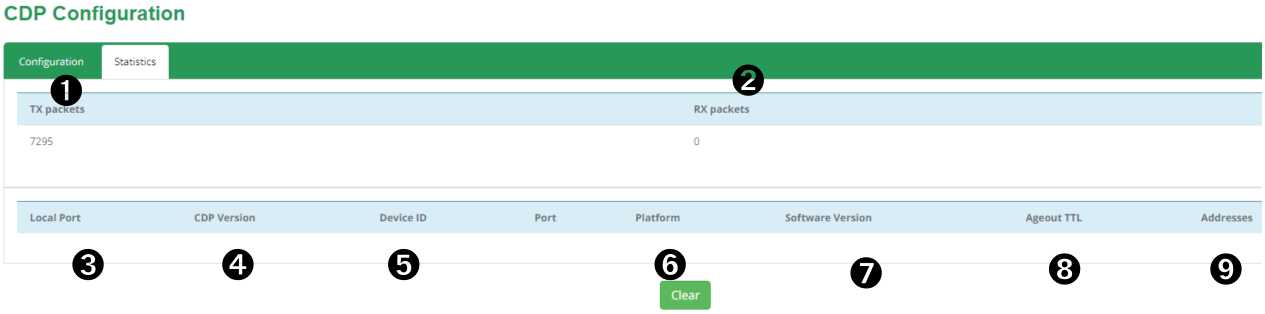
❶ Enabled: On

❷ Update Time: 10

❸ Hold Time: 120

Name	Description
❶ **Enabled:**	Enabled the switch to send out CDP information, and will analyze CDP information received from neighbors.
❷ **Update Time:**	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 **Hold time :**	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.

10.2. CDP Status


CDP Configuration

TX packets	RX packets
7295	0

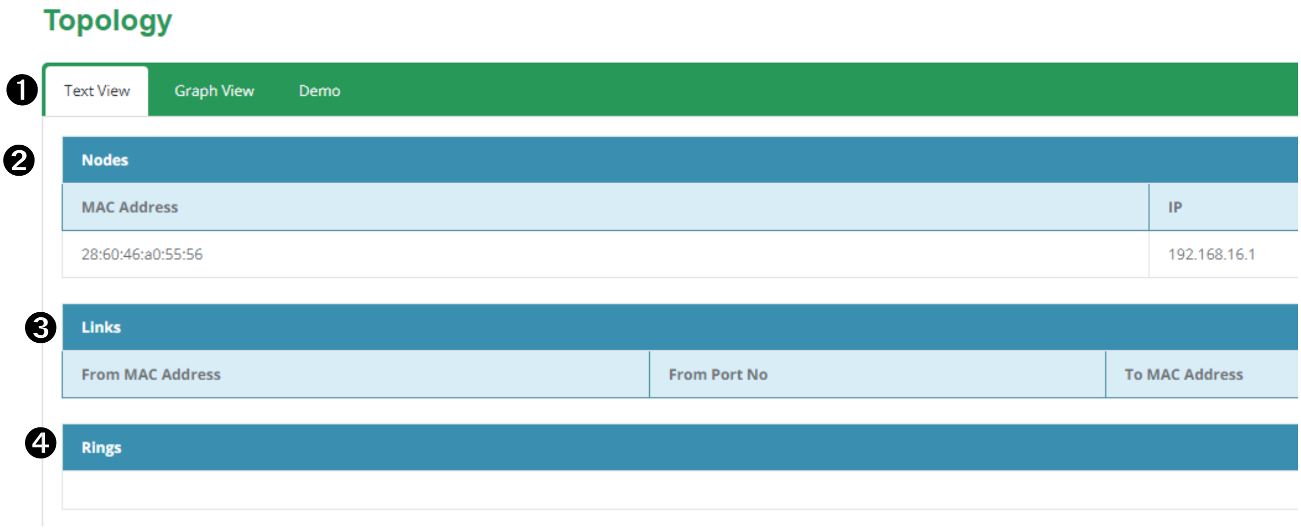
Local Port	CDP Version	Device ID	Port	Platform	Software Version	Ageout TTL	Addresses

10.2.1. Statistics

Name	Description
❶ **Tx Packets:**	The number of CDP frames transmitted on the switch.
❷ **Rx Packets :**	The number of CDP frames received on the switch.

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.

10.3. Topology



Topology

Text View | Graph View | Demo

Nodes

MAC Address	IP
28:60:46:a0:55:56	192.168.16.1

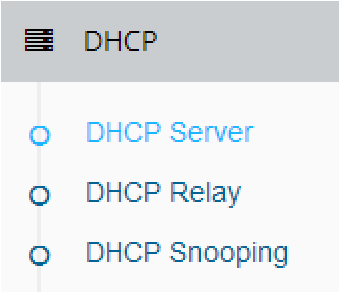
Links

From MAC Address	From Port No	To MAC Address

Rings

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.

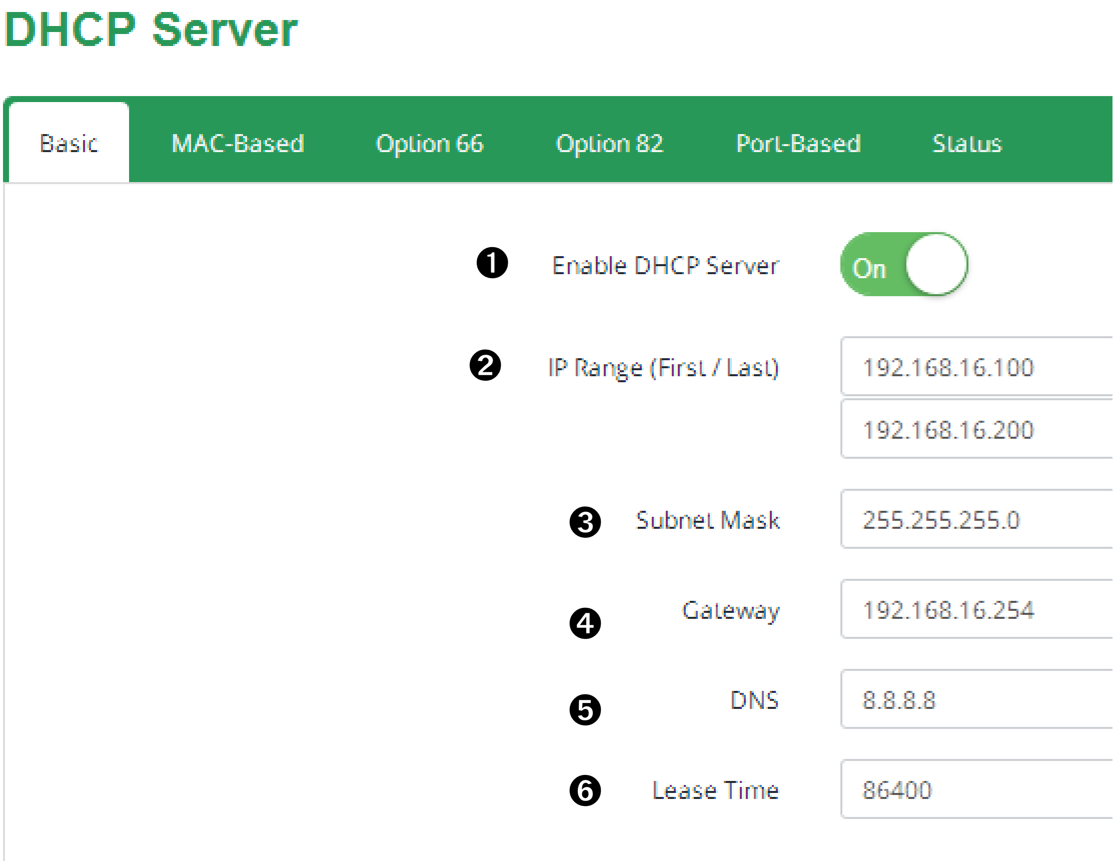
11. DHCP



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

11.1. Basic DHCP Server



❶ Enable DHCP Server: On

❷ IP Range (First / Last): 192.168.16.100 / 192.168.16.200

❸ Subnet Mask: 255.255.255.0

❹ Gateway: 192.168.16.254

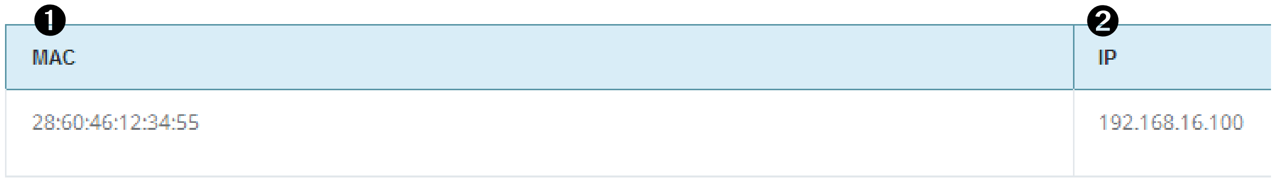
❺ DNS: 8.8.8.8

❻ Lease Time: 86400

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.

11.2. Mac-based DHCP

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

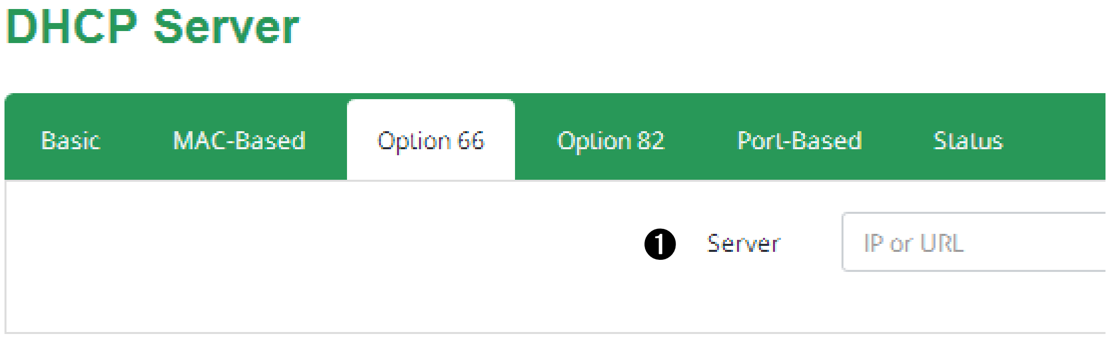


❶ MAC	❷ IP
28:60:46:12:34:55	192.168.16.100

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

11.3. DHCP Option 66

Assign dedicated IP of TFTP server under DHCP option66 standard.



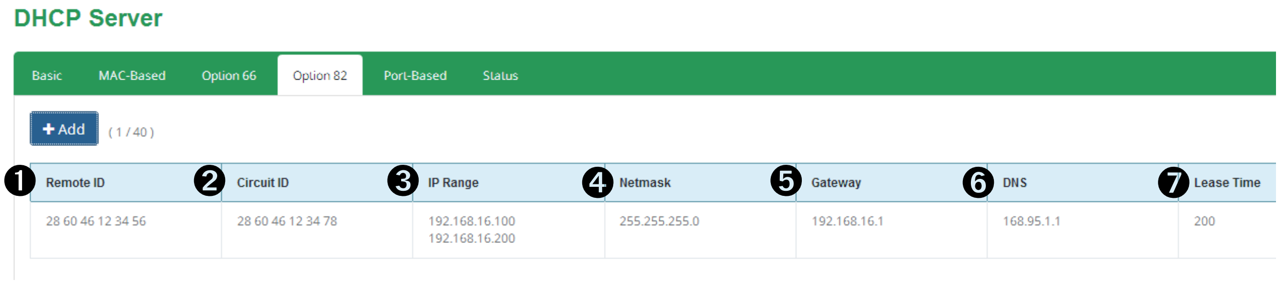
DHCP Server

❶ Server: IP or URL

Name	Description
❶ Server:	IP address of TFTP server

11.4. 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.



DHCP Server

❶ Remote ID	❷ Circuit ID	❸ IP Range	❹ Netmask	❺ Gateway	❻ DNS	❼ Lease Time
28 60 46 12 34 56	28 60 46 12 34 78	192.168.16.100 192.168.16.200	255.255.255.0	192.168.16.1	168.95.1.1	200

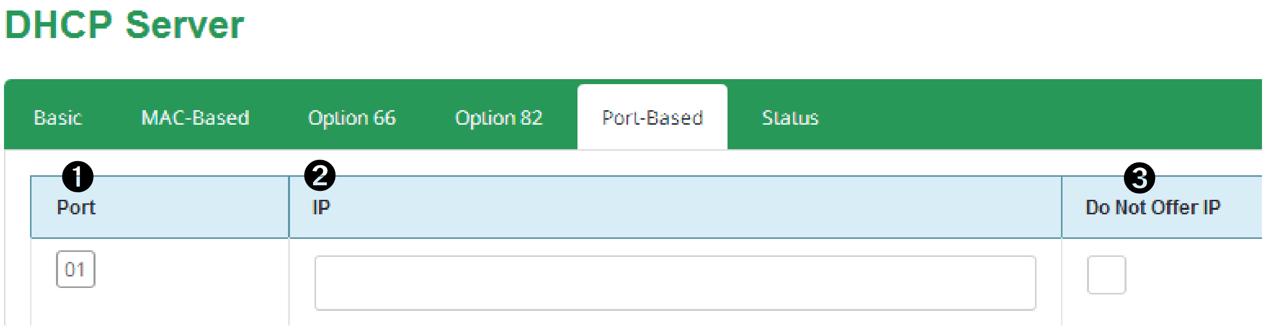
Name	Description

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.

11.5. Port-based DHCP

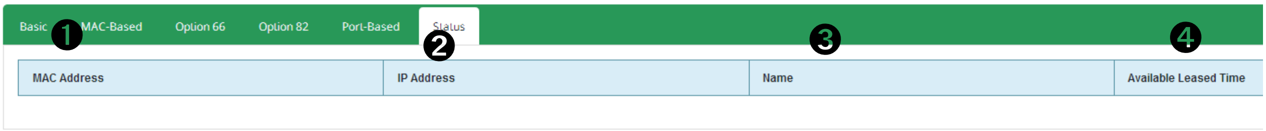
Assign dedicated IP address by port that is connected to the device.



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

11.6. DHCP Status

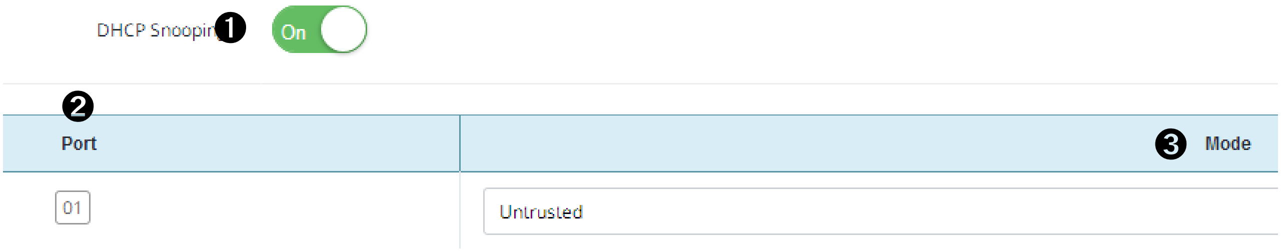
It will show you what IP address has been assigned to client.



Name	Description
❶ **Mac Address:**	MAC address of ending device
❷ **IP Address:**	IP address of ending device
❸ **Name:**	Host name of ending device
❹ **Available Leased Time:**	How long this IP address will be renewed with DHCP server.

11.7. DHCP Snooping

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



DHCP Snoopin❶ On

❷ Port	❸ Mode
01	Untrusted

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. **Possible Values**: Trusted, Untrusted **Default Setting**: Untrusted

12. STP

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.

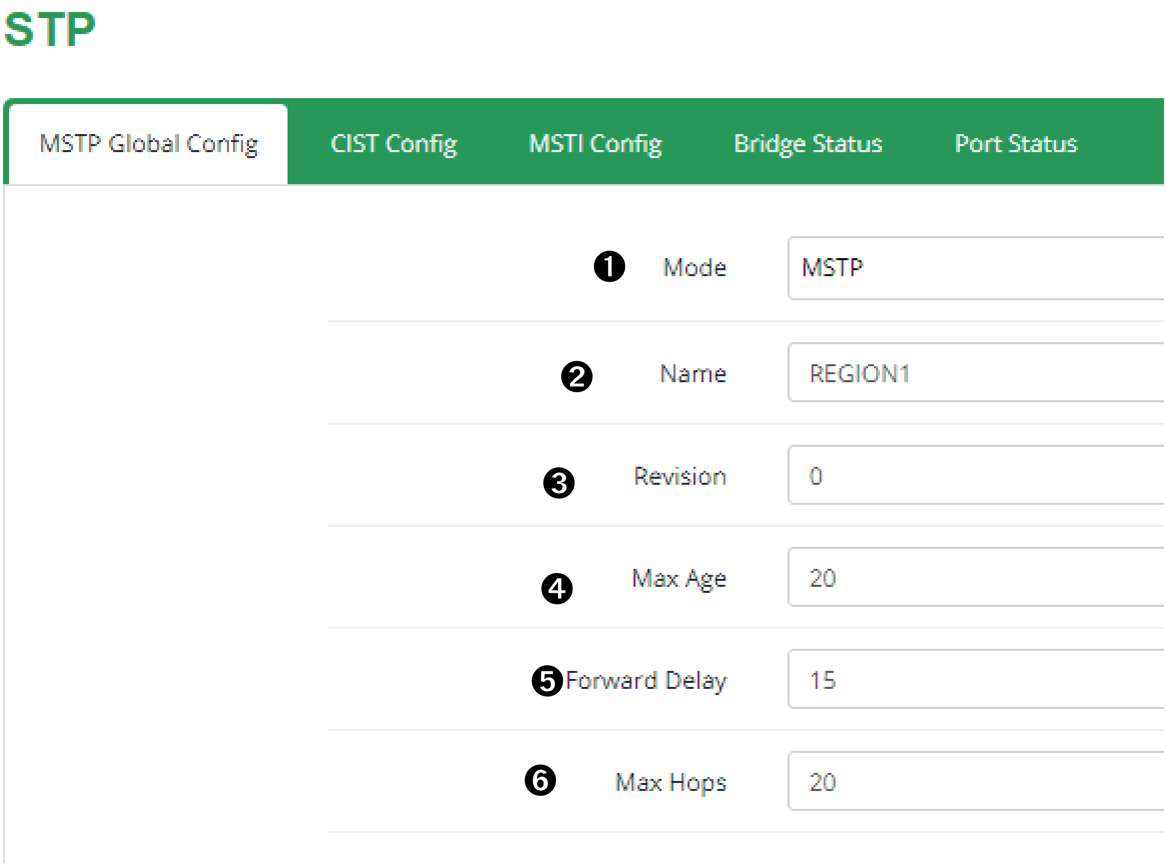
Within STP, the detection and reconfiguration of network topology (connection lost, add a new switch etc) will takes some time – like 30-50 seconds. However, many time-sensitive applications cannot tolerate such delay of network down time, Rapid Spanning Tree Protocol (RSTP) was conceived to overcome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

12.1. MSTP Global Configuration



Mode: MSTP
Name: REGION1
Revision: 0
Max Age: 20
Forward Delay: 15
Max Hops: 20

Name	Description
❶ **Mode:**	Select RSTP or MSTP redundancy protocol for network. **Variants**: RSTP, MSTP **Default Setting**: 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.

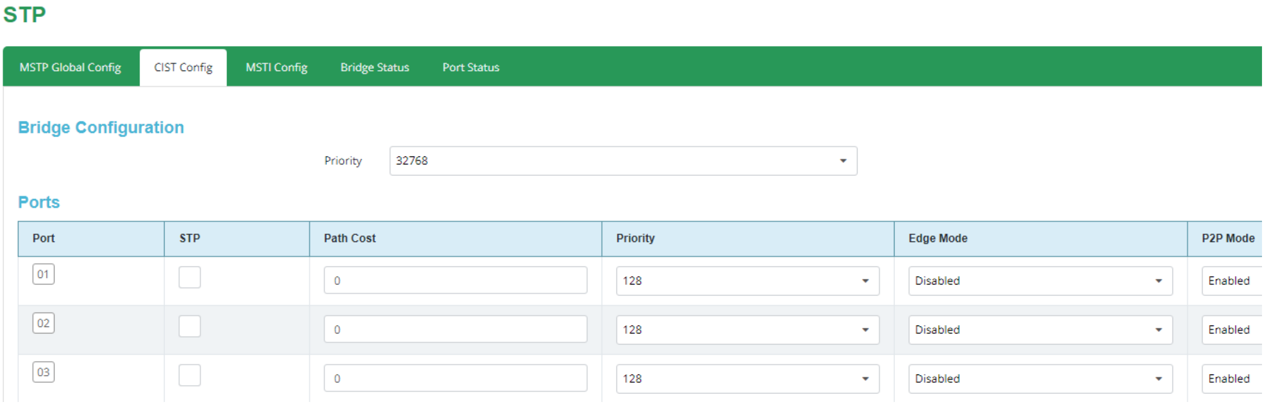
12.2. CIST Settings

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.



STP

Bridge Configuration

Priority: 32768

Ports

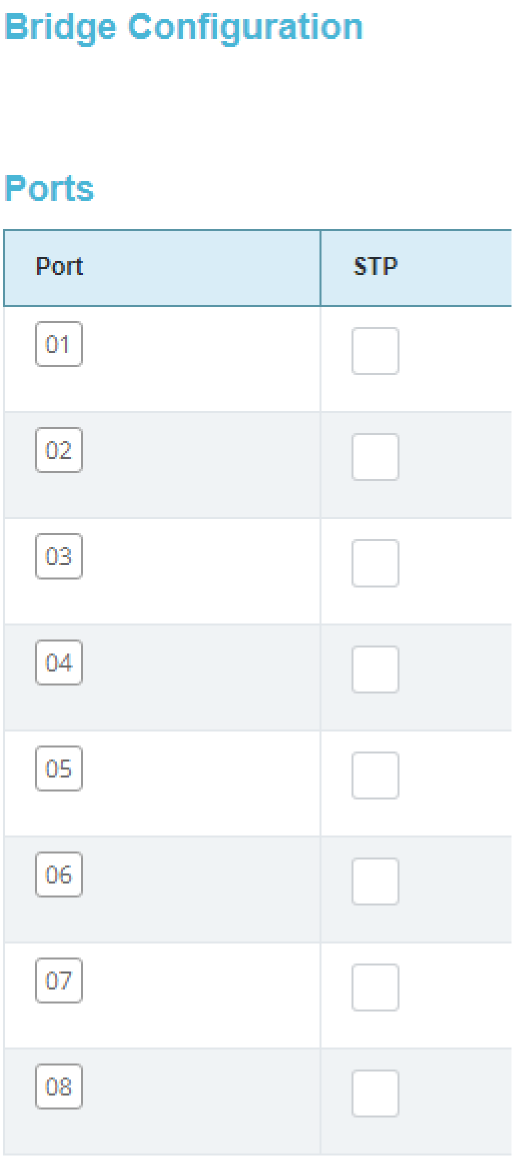
Port	STP	Path Cost	Priority	Edge Mode	P2P Mode
01	□	0	128	Disabled	Enabled
02	□	0	128	Disabled	Enabled
03	□	0	128	Disabled	Enabled

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.

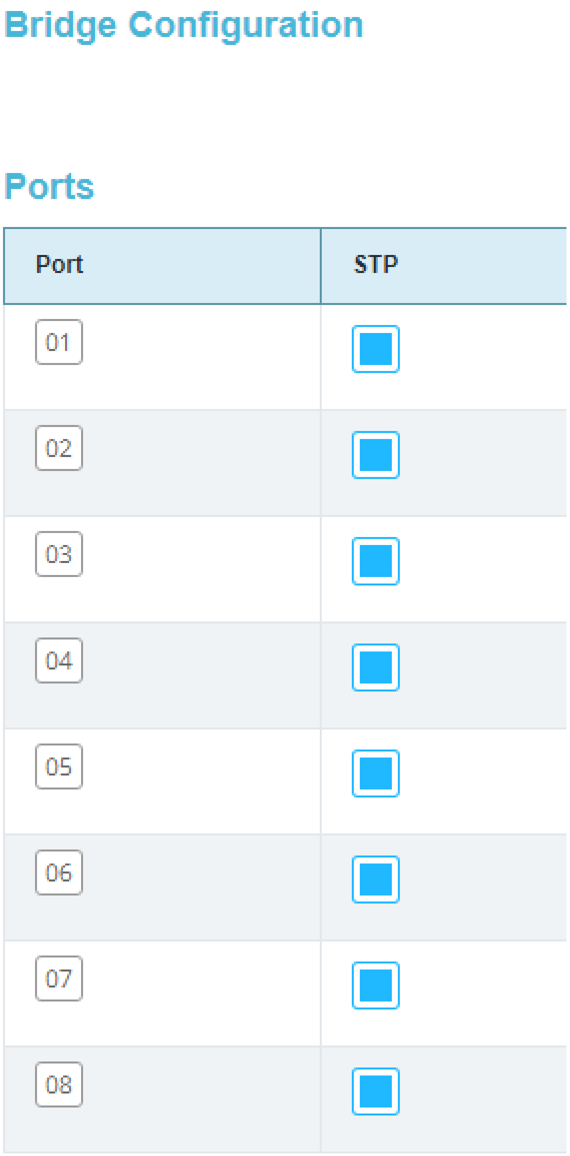


Bridge Configuration

Ports

Port	STP
01	□
02	□
03	□
04	□
05	□
06	□
07	□
08	□

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



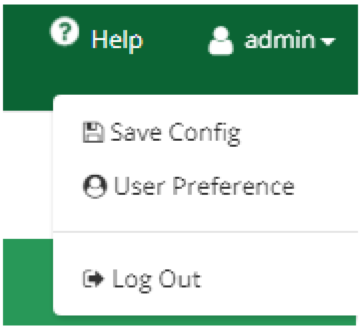
Bridge Configuration

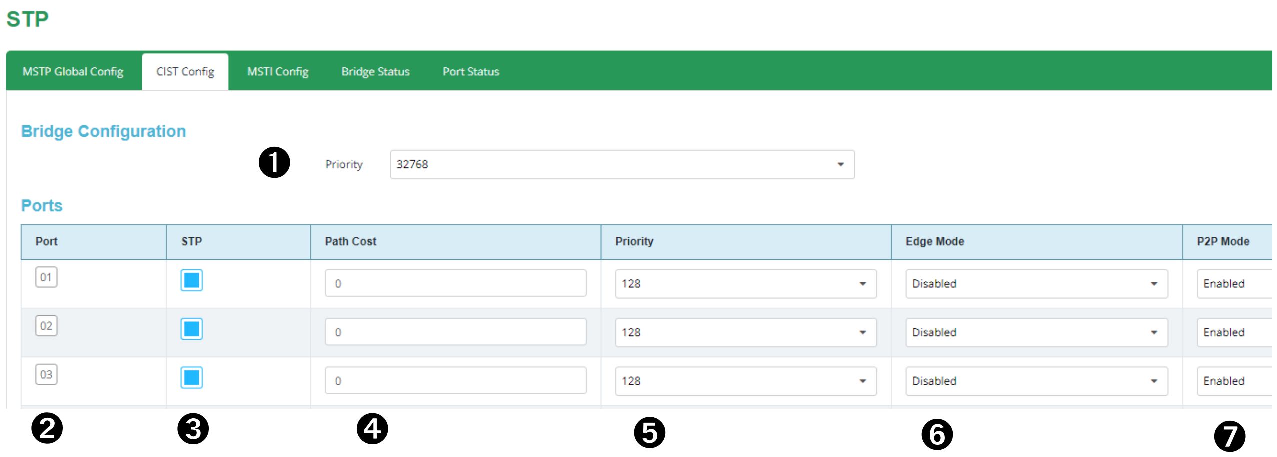
Ports

Port	STP
01	☑
02	☑
03	☑
04	☑
05	☑
06	☑
07	☑
08	☑

D. Remember to press "Apply"

E. Save setting





STP

Bridge Configuration

Priority 32768

Ports

Port	STP	Path Cost	Priority	Edge Mode	P2P Mode
01	☑	0	128	Disabled	Enabled
02	☑	0	128	Disabled	Enabled
03	☑	0	128	Disabled	Enabled

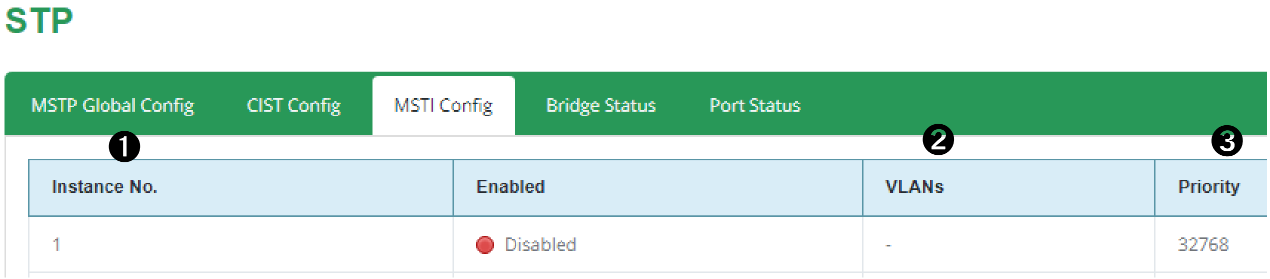
12.2.1. Bridge configuration

Name	Description
❶ **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.
❷ **Port:**	The switch port number of STP.

12.2.2. Ports

Name	Description
❸ **STP:**	Controls whether STP is enabled with this switch port.
❹ **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
❺ **Priority:**	Controls the port priority. This can be used to control priority of ports having identical path cost. (See above).
❻ **edge_mode:**	The port which connects with ending device.
❼ **p2p_mode:**	The port which connects with another switch

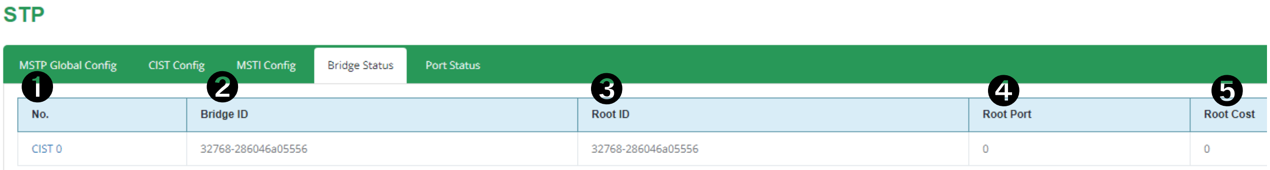
12.3. MSTI Settings



Instance No.	Enabled	VLANs	Priority
1	● Disabled	-	32768

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.

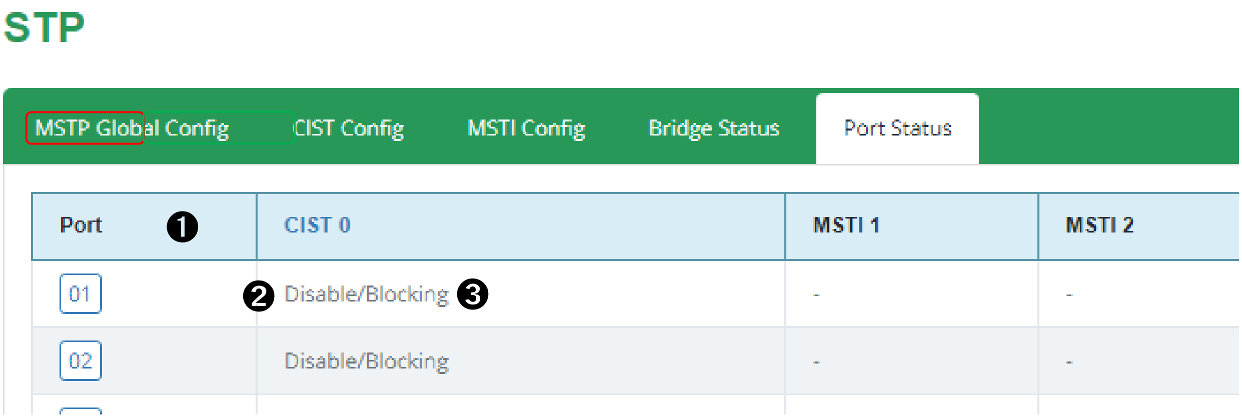
12.4. Bridges Status



No.	Bridge ID	Root ID	Root Port	Root Cost
CIST 0	32768-286046a05556	32768-286046a05556	0	0

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.

12.5. Port Status



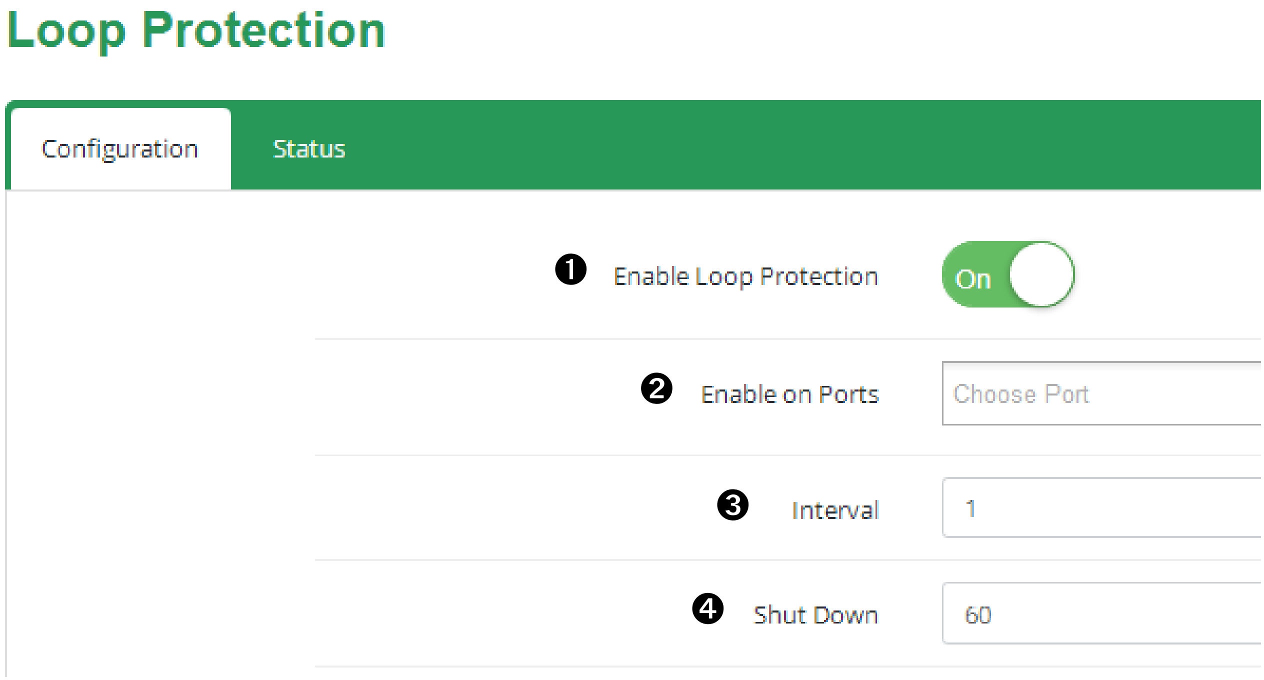
Port	CIST 0	MSTI 1	MSTI 2
01	Disable/Blocking	-	-
02	Disable/Blocking	-	-

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

13. Loop Protection

13.1. Configuration

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



Loop Protection

❶ Enable Loop Protection: On

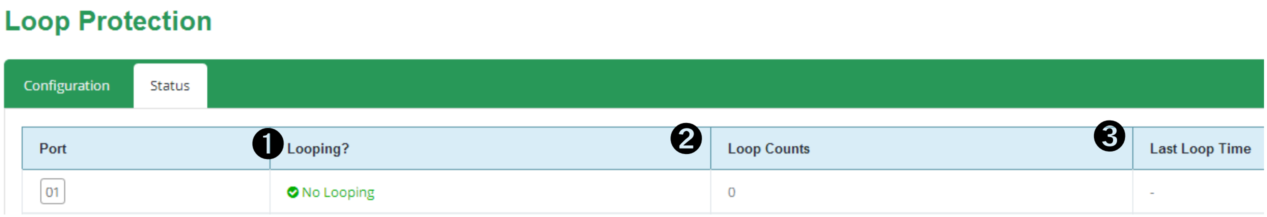
❷ Enable on Ports: Choose Port

❸ Interval: 1

❹ Shut Down: 60

Name	Description
❶ **Enable Loop Protection:**	Enable or disable loop protection.
❷ **Enable on ports**:	Define which port you want to enable loop protection.
❸ **Interval** :	Define how often the switch will check the loop status of each port.
❹ **Shutdown**	Define how long the port will be blocked when it is looping.

13.2. Status



Loop Protection

Port	Looping?	Loop Counts	Last Loop Time
01	✓ No Looping	0	-

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

14. 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.

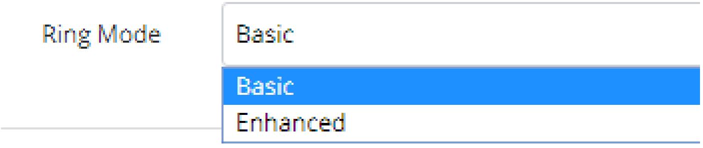
Lantech Auto, Enhanced and Multiple-Train ring are adapted to protect IGMP and data packets with faster recovery scheme, so if the network is in heavy duty of IGMP application, we suggest using those ring modes to achieve better redundancy.

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.

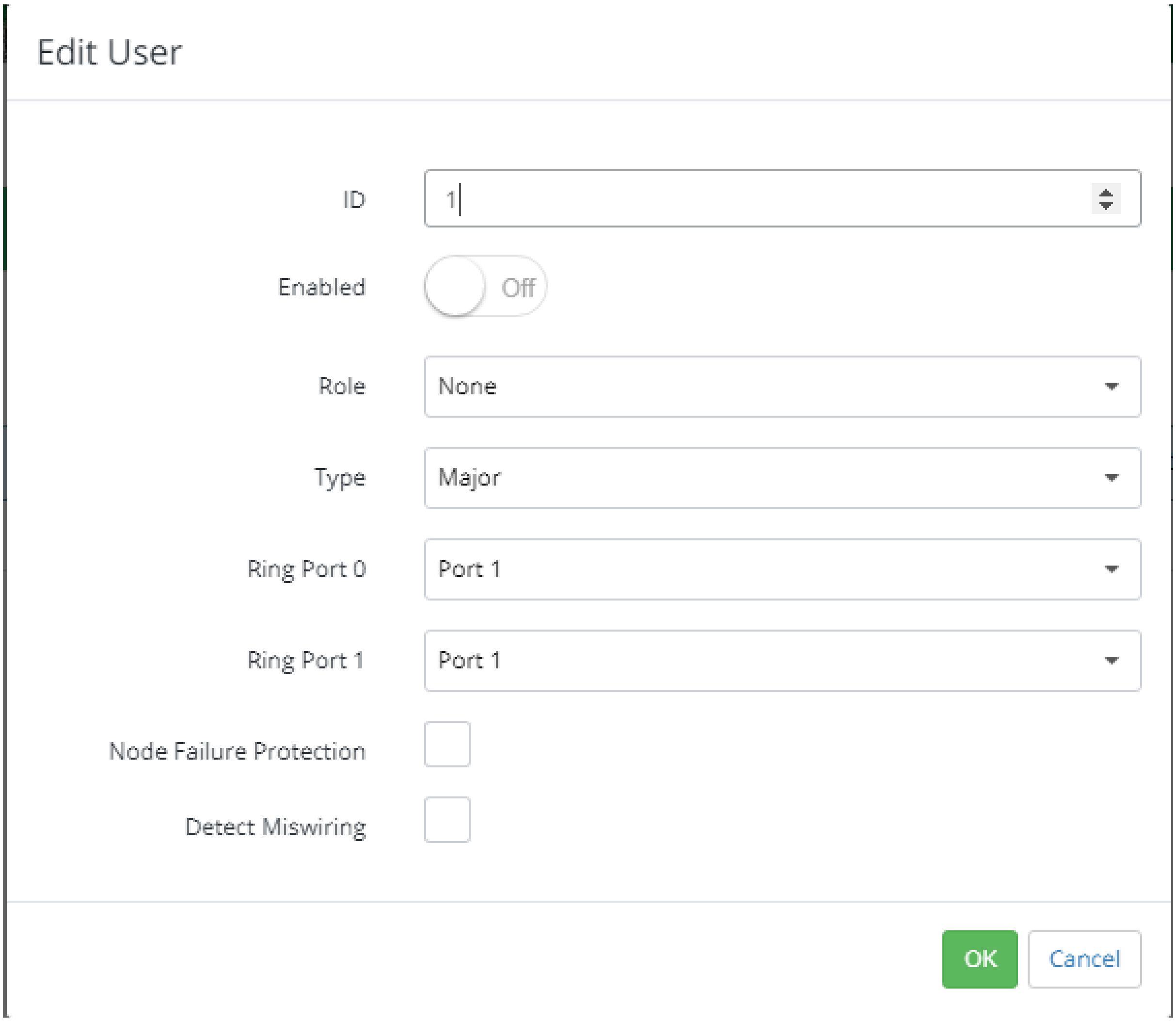
14.1. Introduction of Ring modes



Ring Mode: Basic

Basic Ring

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



Edit User

ID: 1

Enabled: Off

Role: None

Type: Major

Ring Port 0: Port 1

Ring Port 1: Port 1

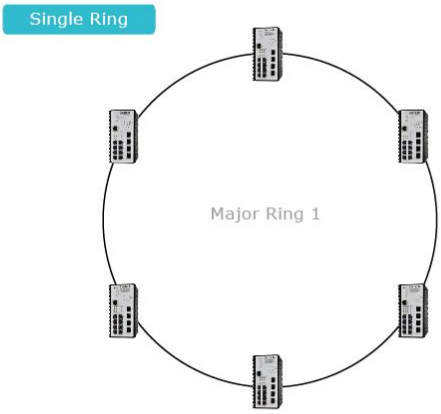
Node Failure Protection □

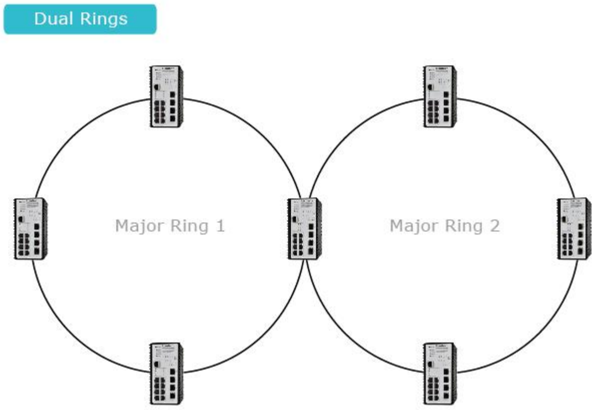
Detect Miswiring □

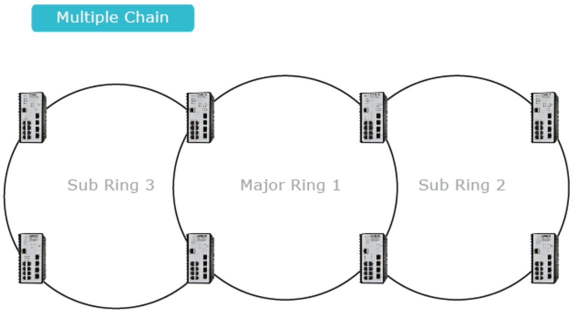
Enhanced Ring

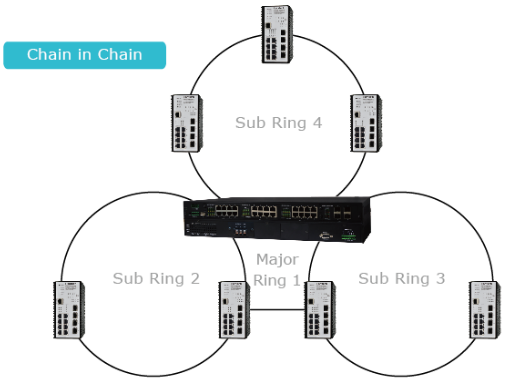
Lantech Enhanced ring mode supports multiple rings, please refer to the following demo topologies. All rings (include Major ring and Sub ring) must be in the same VLAN.

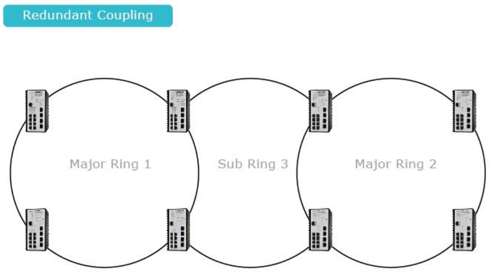
Note: This is proprietary Lantech ring.

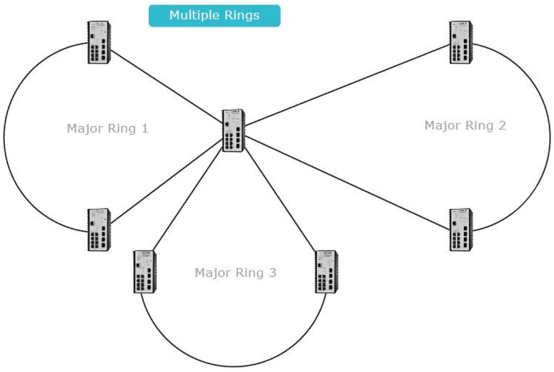


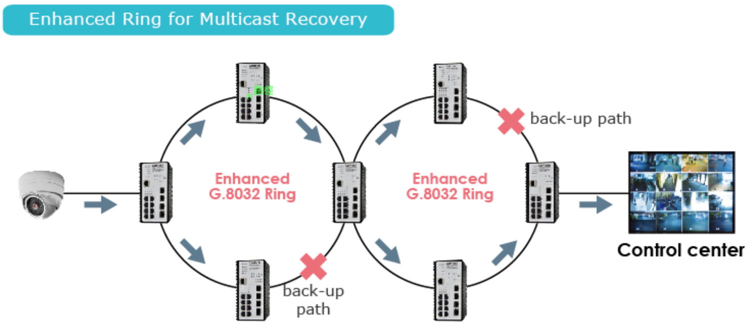


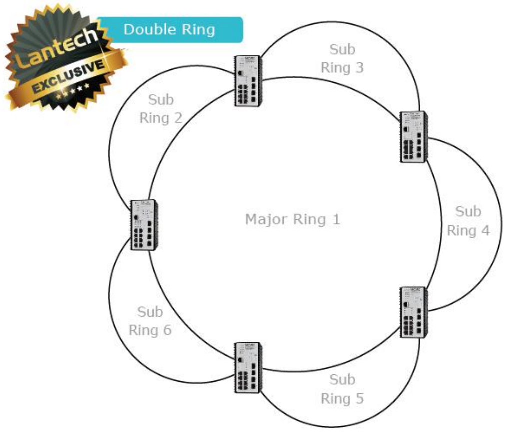


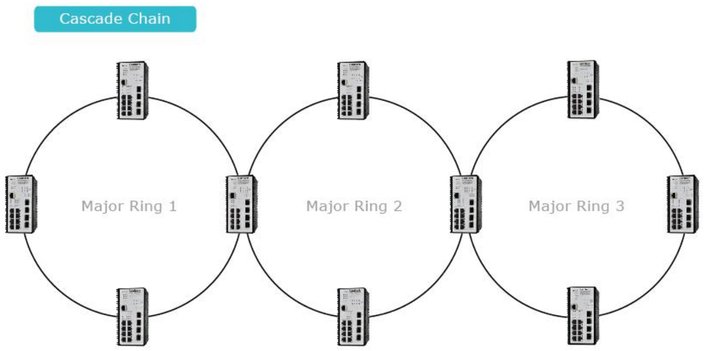


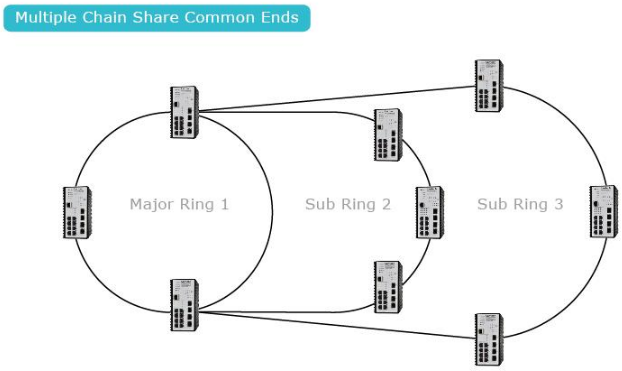


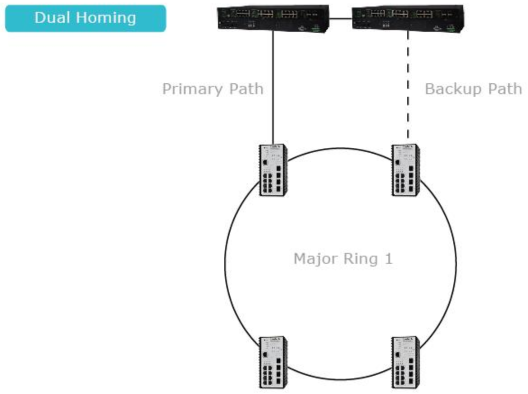


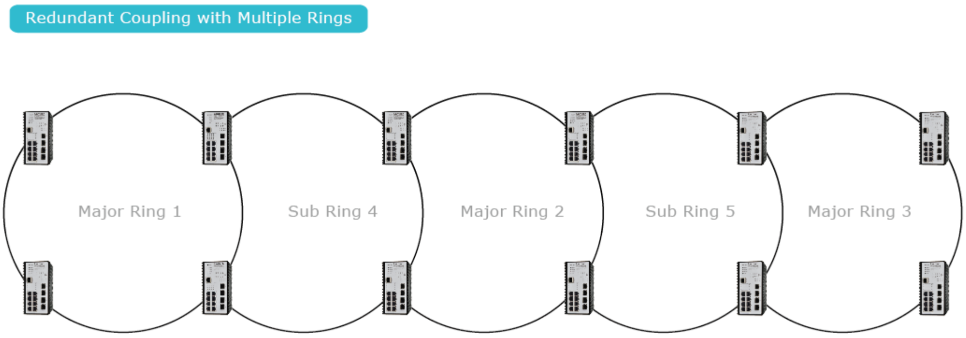

Enhanced Ring for Multicast Recovery
Enhanced G.8032 Ring
Enhanced G.8032 Ring
back-up path
back-up path
Control center


Lantech EXCLUSIVE
Double Ring
Sub Ring 3
Sub Ring 2
Major Ring 1
Sub Ring 4
Sub Ring 6
Sub Ring 5


Cascade Chain
Major Ring 1
Major Ring 2
Major Ring 3


Multiple Chain Share Common Ends
Major Ring 1
Sub Ring 2
Sub Ring 3


Dual Homing
Primary Path
Backup Path
Major Ring 1


Redundant Coupling with Multiple Rings
Major Ring 1
Sub Ring 4
Major Ring 2
Sub Ring 5
Major Ring 3

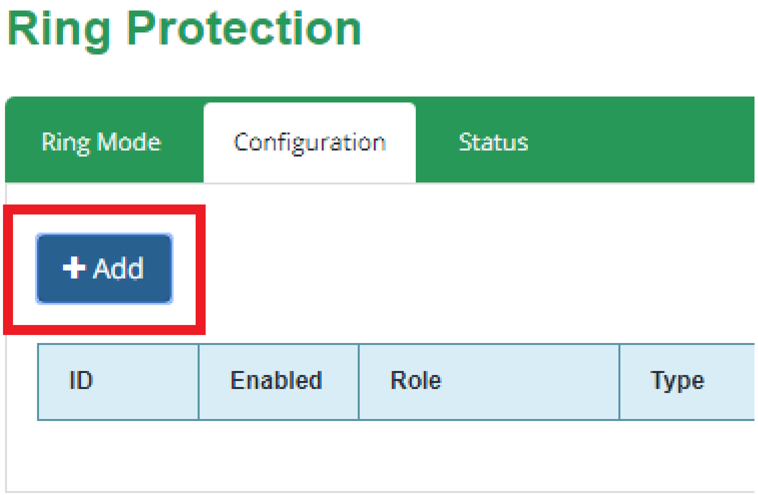
14.2. Setting Up and Configuring

14.2.1. G.8032

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

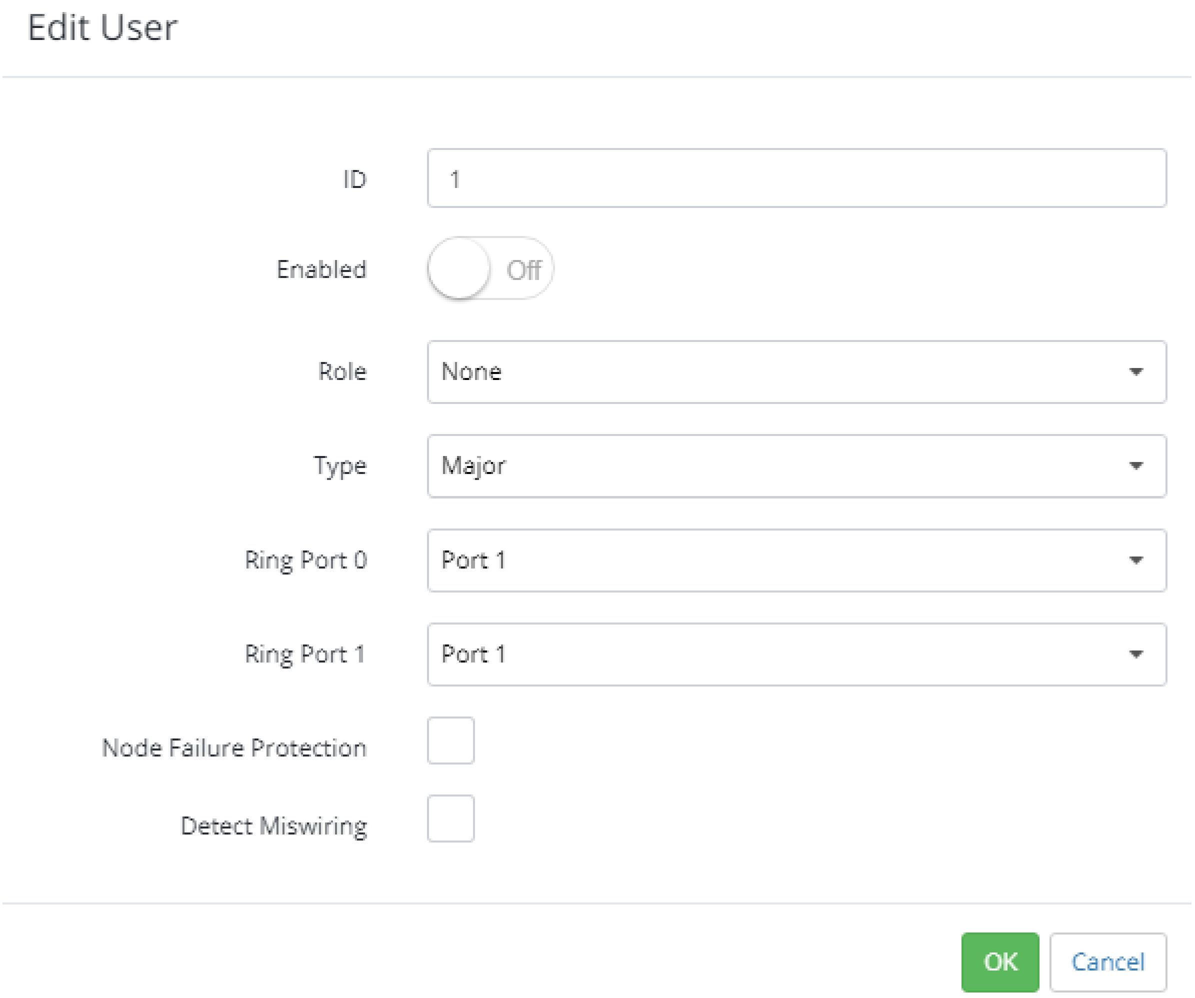
Note: in this case, we will use the port 9 and port 10 of each switch to build a ring.

1. Press “+Add” icon to add one ring with G.8032 protocol.



ID	Enabled	Role	Type

2. Enter edit mode



Edit User

ID: 1

Enabled: Off

Role: None

Type: Major

Ring Port 0: Port 1

Ring Port 1: Port 1

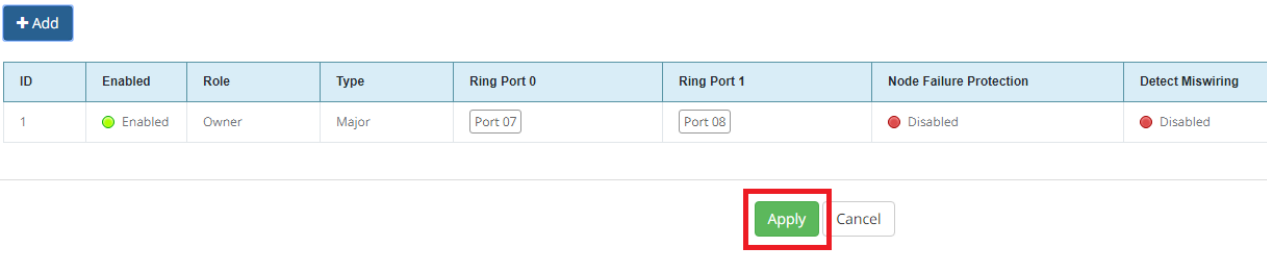
Node Failure Protection: □

Detect Miswiring: □

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.

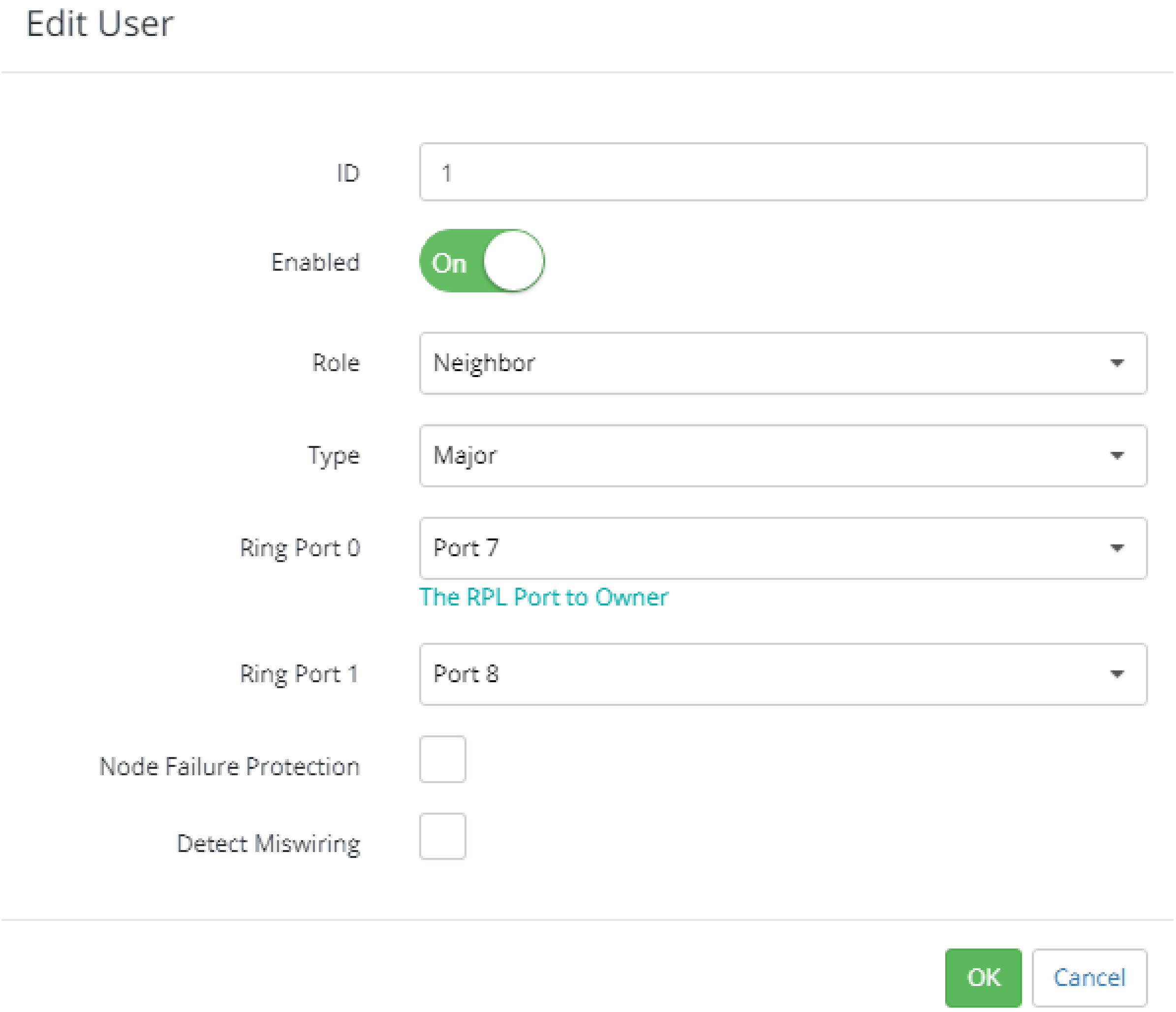
To play safe, we suggest the user to finished all setting G8032 then connect the physical connection if the user is not familiar with the G8032 function.

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



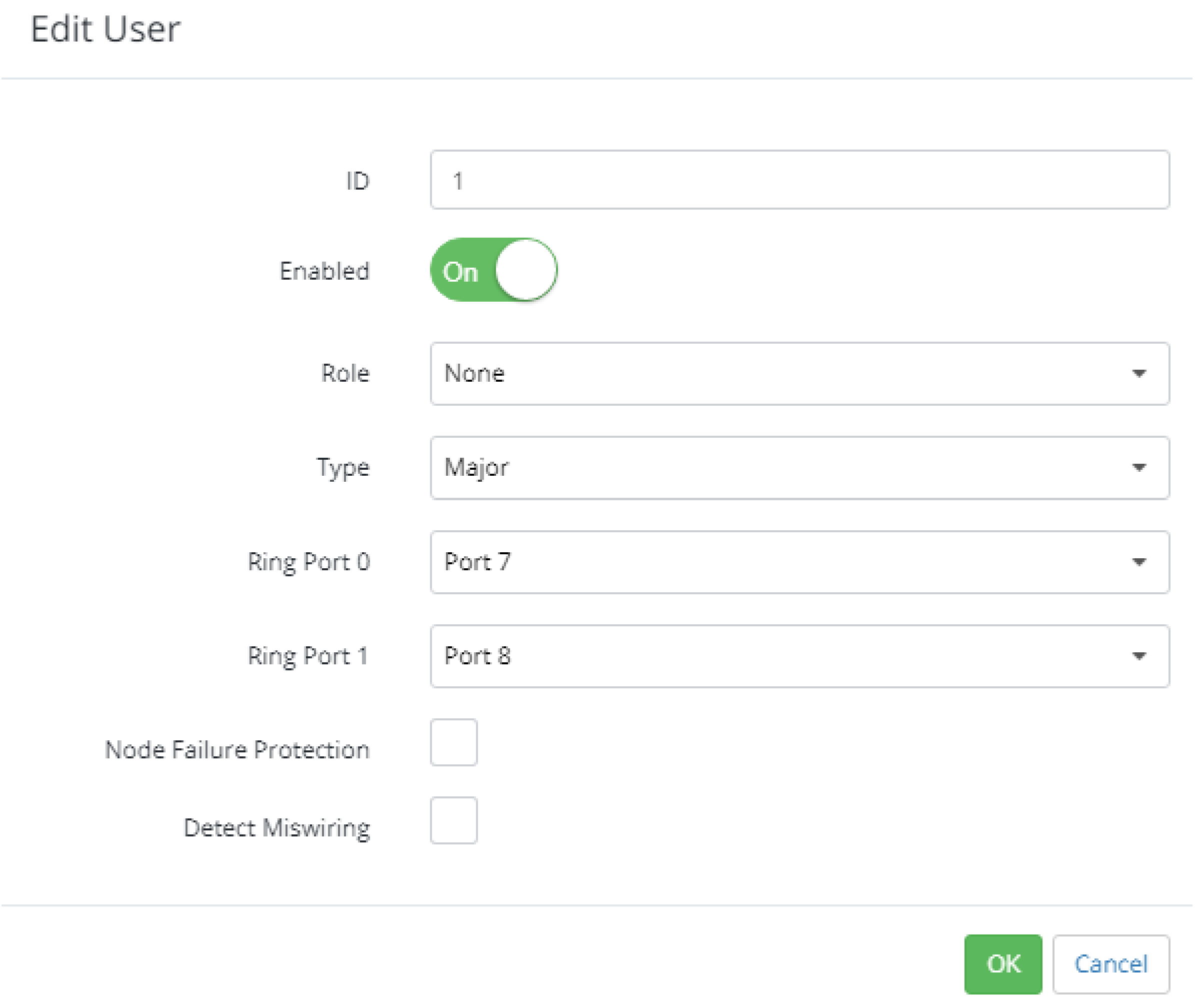
ID	Enabled	Role	Type	Ring Port 0	Ring Port 1	Node Failure Protection	Detect Miswiring
1	● Enabled	Owner	Major	Port 07	Port 08	● Disabled	● Disabled

5. The setting of neighbor switch


Edit User

ID	1
Enabled	On
Role	Neighbor
Type	Major
Ring Port 0	Port 7 The RPL Port to Owner
Ring Port 1	Port 8
Node Failure Protection	□
Detect Miswiring	□

6. The setting of none switch



Edit User

ID 1

Enabled On

Role None

Type Major

Ring Port 0 Port 7

Ring Port 1 Port 8

Node Failure Protection □

Detect Miswiring □

15. Security

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

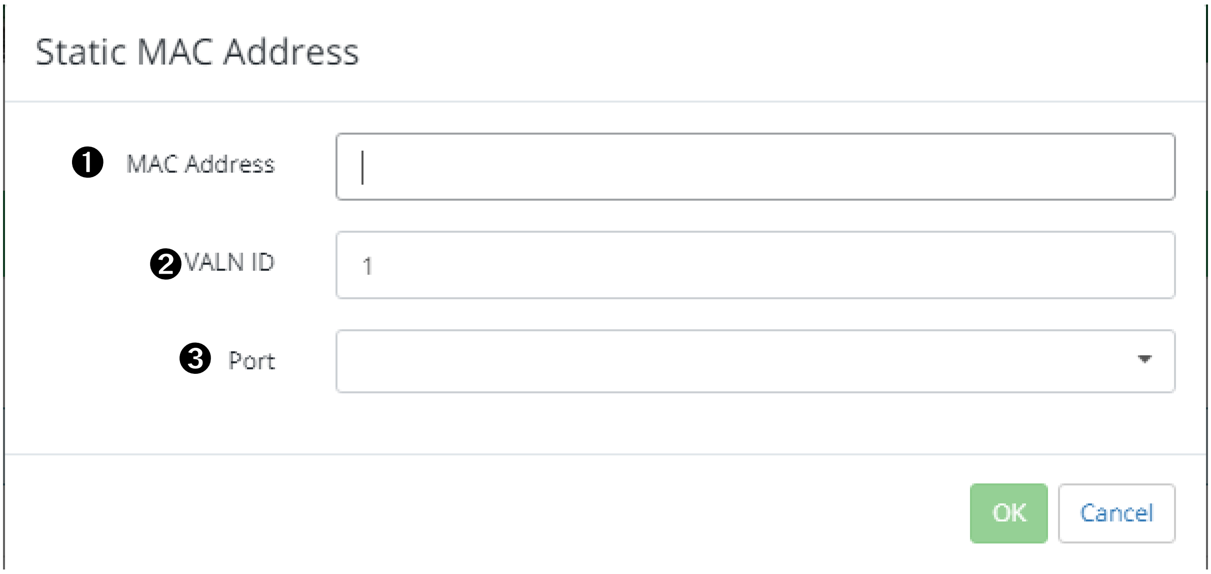
- Mac Address Tables
- Access Control List
- IEEE 802.1X Radius Server
- IP Security

15.1 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.



Static MAC Address

❶ MAC Address

❷VALN ID 1

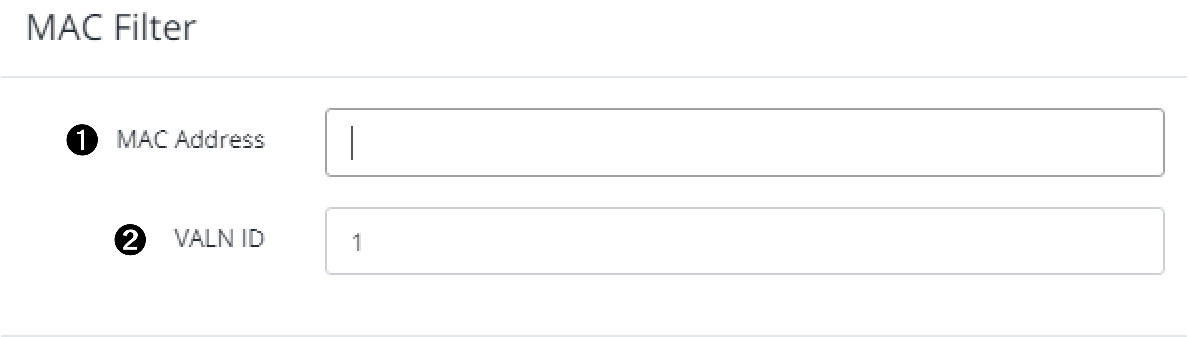
❸ Port

Name	Description
❶ **Mac**	Enter the MAC address of the port that should permanently

Address:	forward traffic.
❷ **VLAN ID:**	Enter the corresponding VLAN ID.
❸ **Port :**	Drop down menu for selecting the port.

MAC Filtering

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



MAC Filter

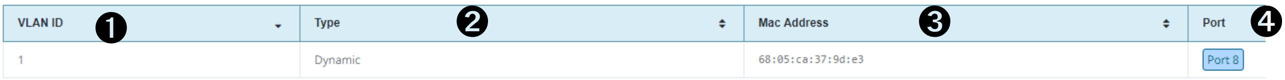
❶ MAC Address |

❷ VALN ID 1

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.



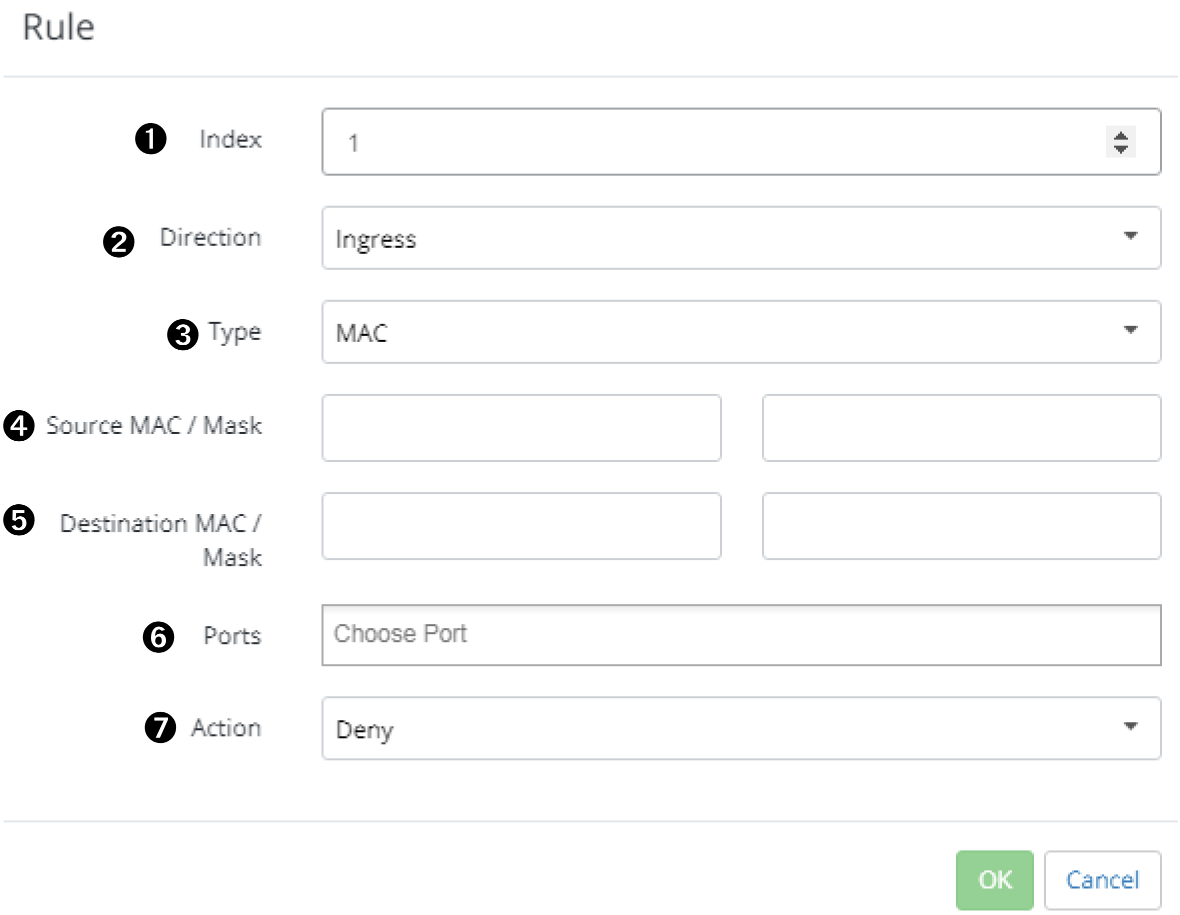
VLAN ID ❶	Type ❷	Mac Address ❸	Port ❹
1	Dynamic	68:05:ca:37:9d:e3	Port 8

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.

15.2 Access Control List

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



Rule

❶ Index: 1

❷ Direction: Ingress

❸ Type: MAC

❹ Source MAC / Mask:

❺ Destination MAC / Mask:

❻ Ports: Choose Port

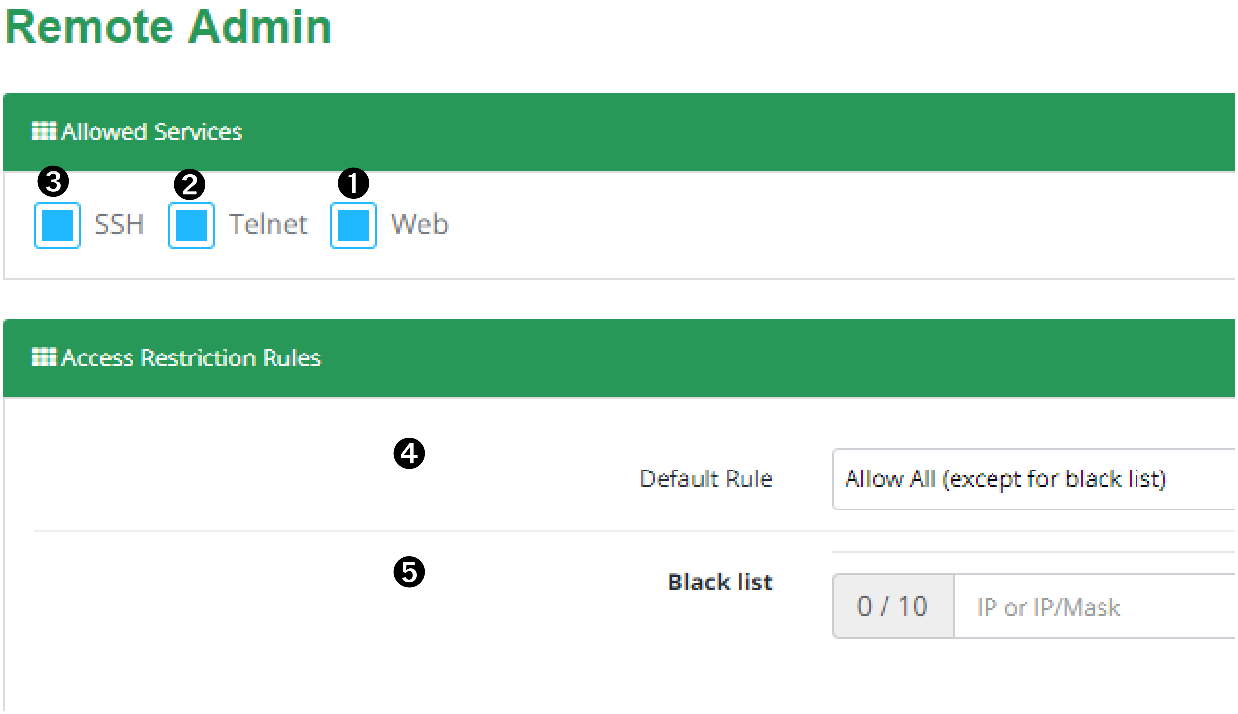
❼ Action: Deny

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>❶ <b>Index:</b></td><td>Index number of ACL rule.</td></tr>
<tr><td>❷ <b>Direction:</b></td><td>Set ACL is to be applied to Ingress or Egress traffic.
<table>
<tr><th>Options</th><th>Default Setting</th></tr>
<tr><td>Ingress/Egress</td><td>Ingress</td></tr>
</table></td></tr>
<tr><td>❸ <b>Type:</b></td><td>Set ACL to check the IP address or MAC address of packets.
<table>
<tr><th>Options</th><th>Default Setting</th></tr>
<tr><td>IP/MAC</td><td>MAC</td></tr>
</table></td></tr>
</table>

<table>
<tr><td><b>❹ Source MAC/MASK:</b></td><td>Set the source address (MAC or IP) to be processed by ACL.</td></tr>
<tr><td><b>❺ Destination MAC/MASK:</b></td><td>Set the destination address (MAC or IP) to be processed by ACL.</td></tr>
<tr><td><b>❻ Ports:</b></td><td>Set which port you want to be filtered by ACL rule.</td></tr>
<tr><td><b>❼ Action:</b></td><td>Action to be taken by ACL.<table><tr><th>Actions</th><th>Default Setting</th></tr><tr><td>Deny/Permit</td><td>Permit</td></tr></table></td></tr>
</table>

15.3 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.



Remote Admin

Allowed Services

☑ SSH ☑ Telnet ☑ Web

Access Restriction Rules

Default Rule: Allow All (except for black list)

Black list: 0 / 10 IP or IP/Mask

Name	Description
❶ Web:	Check this option to make web access available for further setting.

❷ Telnet: Check this option to make Telnet access available for further setting.

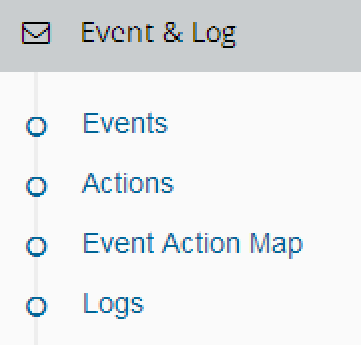
❸ SSH: Check this option to make SSH access available for further setting.

❹ Default Rule: Following IP list should be allowed or denied with web/Telnet/SSH access.

Actions	**Default Setting**
Allow All/Deny All	Allow All

❺ Black List: Assign up to 10 specific IP addresses to be allowed or denied to access the admin service(s).

16. Event & Log

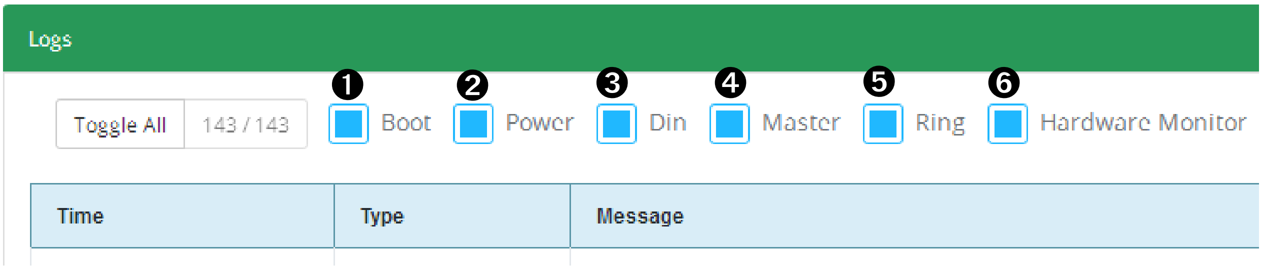


The Event & Log displays the following information

- Occur time
- Event type
- Event description

16.1 View Logs

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



Name	Description
❶ **Boot:**	System Boot
❷ **Power:**	Power condition
❸ **Din:**	Digital Input Event is triggered
❹ **Master:**	Master of ITU-Ring has been changed
❺ **Ring:**	Topology of ITU-Ring has been changed
❻ **Hardware Monitor:**	Event of hardware monitor has been triggered

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

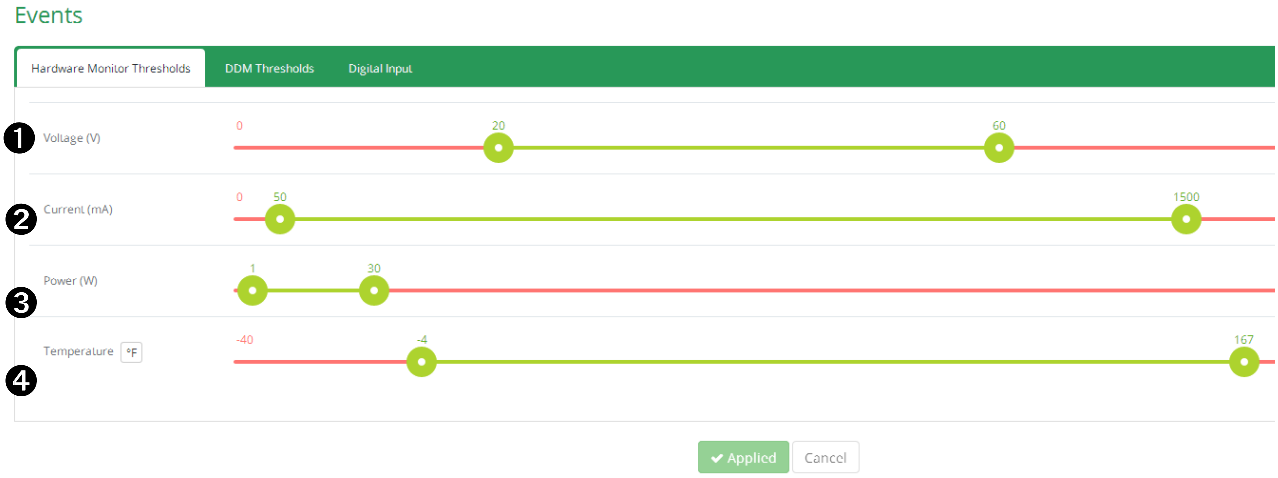
16.2. Events

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

- Environment Monitoring Event
- SFP Digital Diagnostic Monitor Event

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.



Voltage (V) 0 20 60

Current (mA) 0 50 1500

Power (W) 1 30

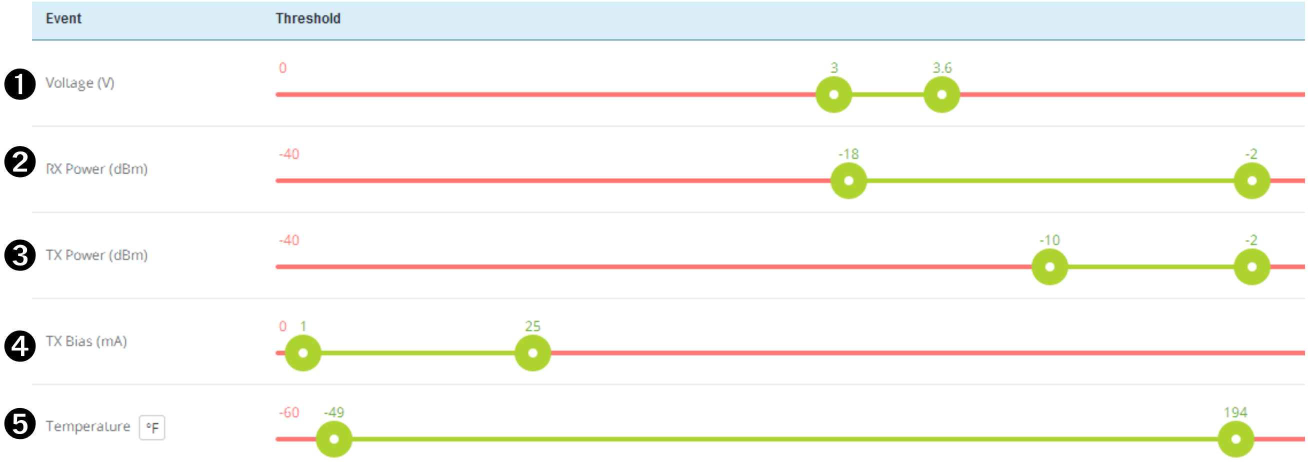
Temperature °F -40 -4 167

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.

SFP Digital Diagnostic Monitor Event

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



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

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

16.3. Actions

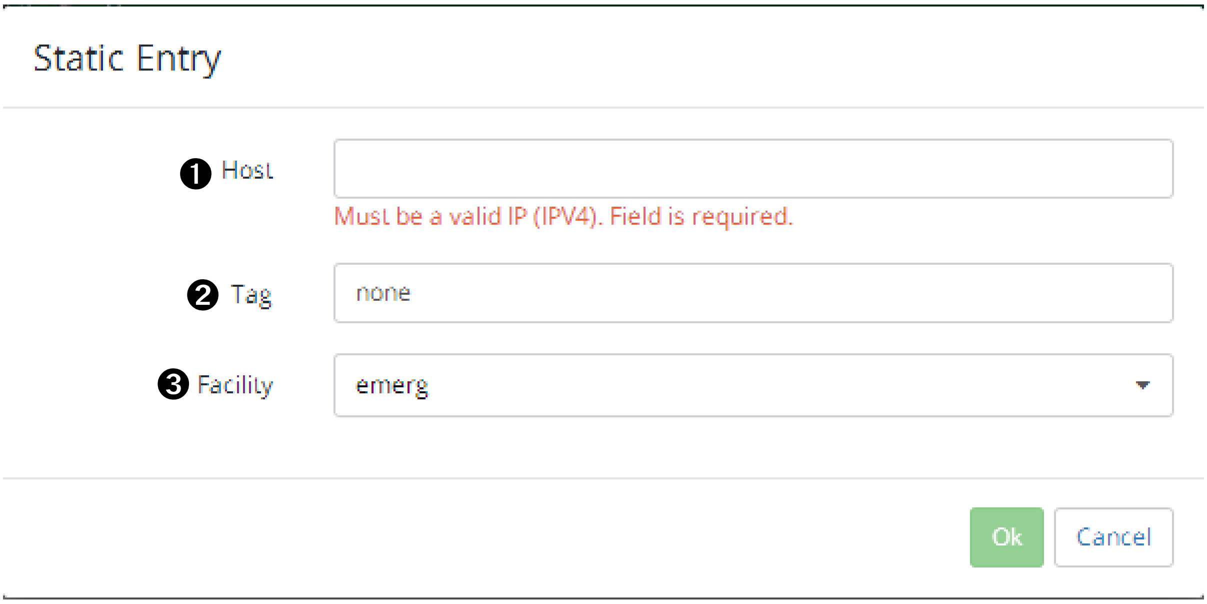
When switch find event, it will trigger the follow-by action pre-set.

You can find all reactive actions as follows:

- Syslog Action
- Email Action
- SMS Action
- DOUT Action

16.3.1. 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.



Static Entry

❶ Host

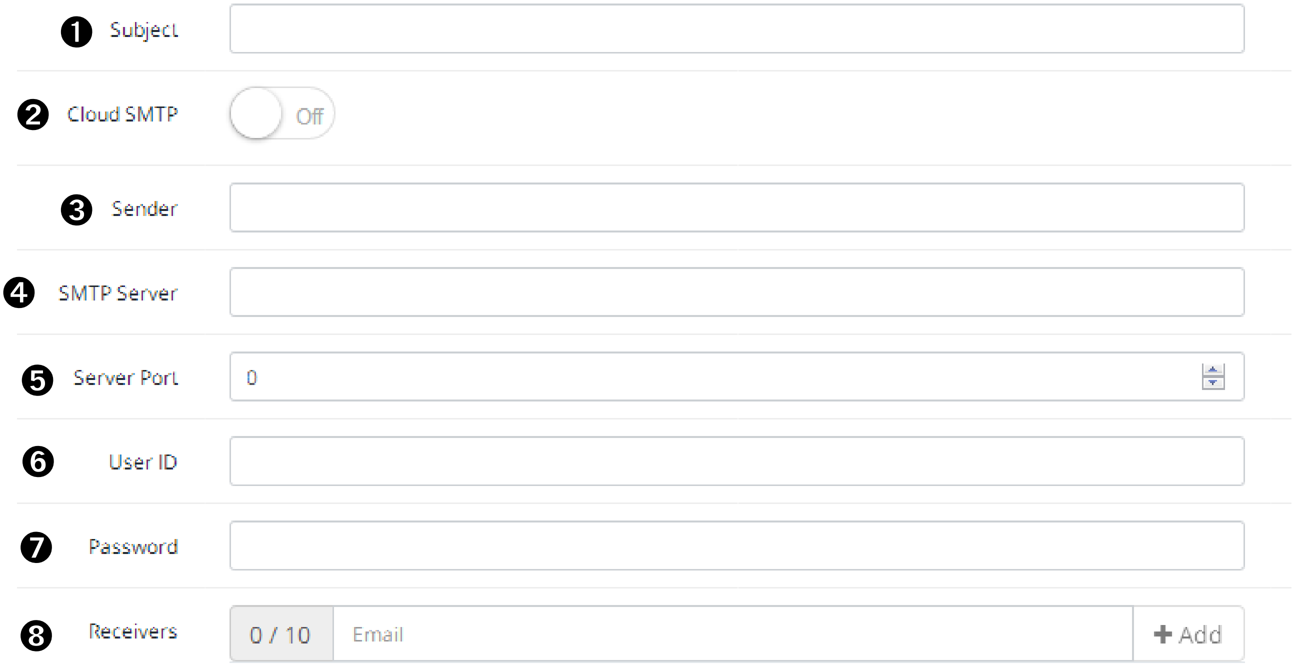
Must be a valid IP (IPV4). Field is required.

❷ Tag: none

❸ Facility: emerg

Name	Description
❶ **Host:**	IP address of Syslog server
❷ **Tag:**	Tag of event
❸ **Facility:**	Facility of event

16.3.2. Email Action



❶ Subject

❷ Cloud SMTP: Off

❸ Sender

❹ SMTP Server

❺ Server Port: 0

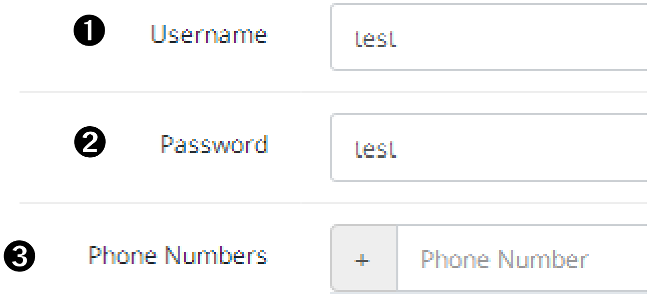
❻ User ID

❼ Password

❽ Receivers: 0 / 10

Name	Description
❶ **Subject:**	Subject of email
❷ **Cloud SMTP:**	Send Email via Lantech Cloud SMTP server
❸ **Sender:**	Sender of Email
❹ **SMTP server:**	If you don't prefer to use Cloud SMTP, please input the IP address of your SMTP server in here
❺ **Server Port:**	Socket port of your SMTP server
❻ **User ID:**	User account of your SMTP server
❼ **Password:**	Password of user account
❽ **Receivers:**	Email address of receiver

16.3.3. SMS Action



❶ Username: test

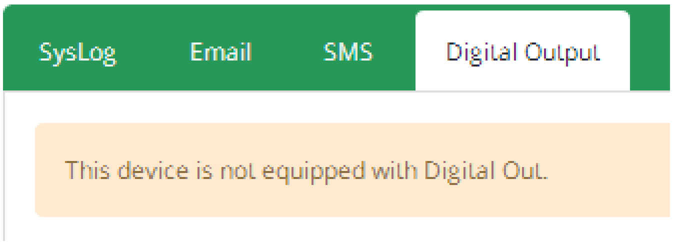
❷ Password: test

❸ Phone Numbers: + Phone Number

Name	Description
❶ **Username:**	User name of SMS account
❷ **Password:**	Password of SMS account
❸ **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.

16.3.4. DOUT Action

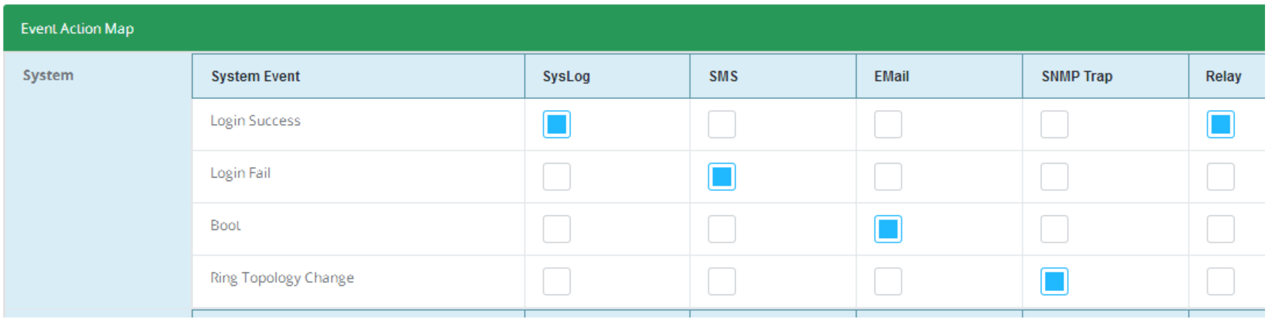


This device is not equipped with Digital Out.

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

16.4. Event Action Map

You can combine event and action setting here.



Event Action Map

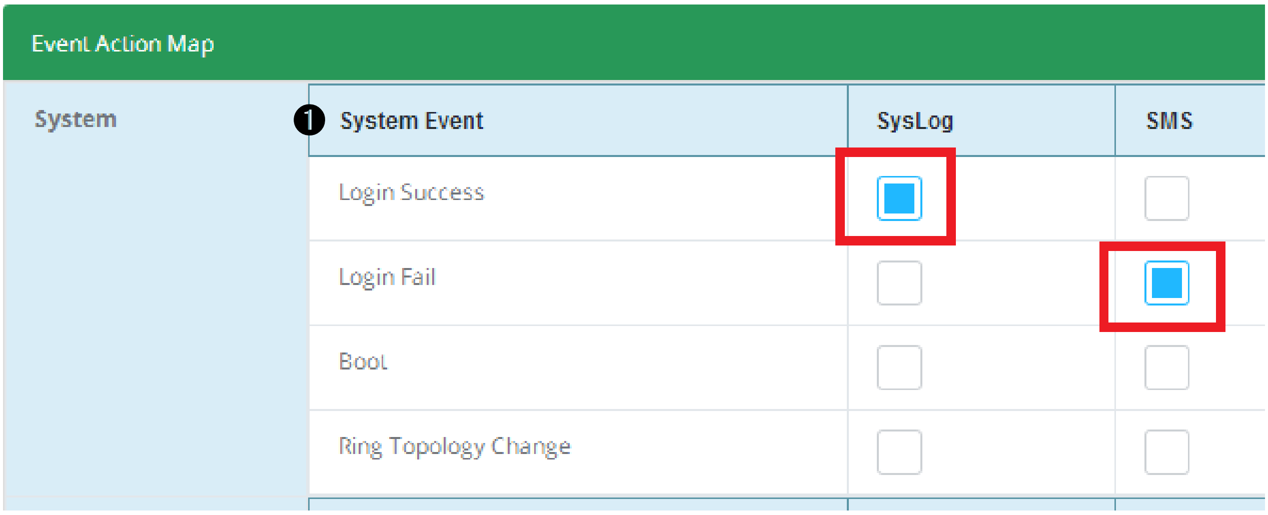
System

System Event	SysLog	SMS	EMail	SNMP Trap	Relay
Login Success	☑	□	□	□	☑
Login Fail	□	☑	□	□	□
Boot	□	□	☑	□	□
Ring Topology Change	□	□	□	☑	□

Event Actions:

Please follow the steps below to set the event actions:

A. Choose the event which you want to activate.



Event Action Map

System

❶ System Event	SysLog	SMS
Login Success	☑	□
Login Fail	□	☑
Boot	□	□
Ring Topology Change	□	□

Name	Description	Possible values	Default setting
❶ **System Event**:	Which event will be combined with desired action	Boot Hardware Monitor Ring Topology change DDM5 DDM6 Login fail Login success Port break down Power1 Power2	None

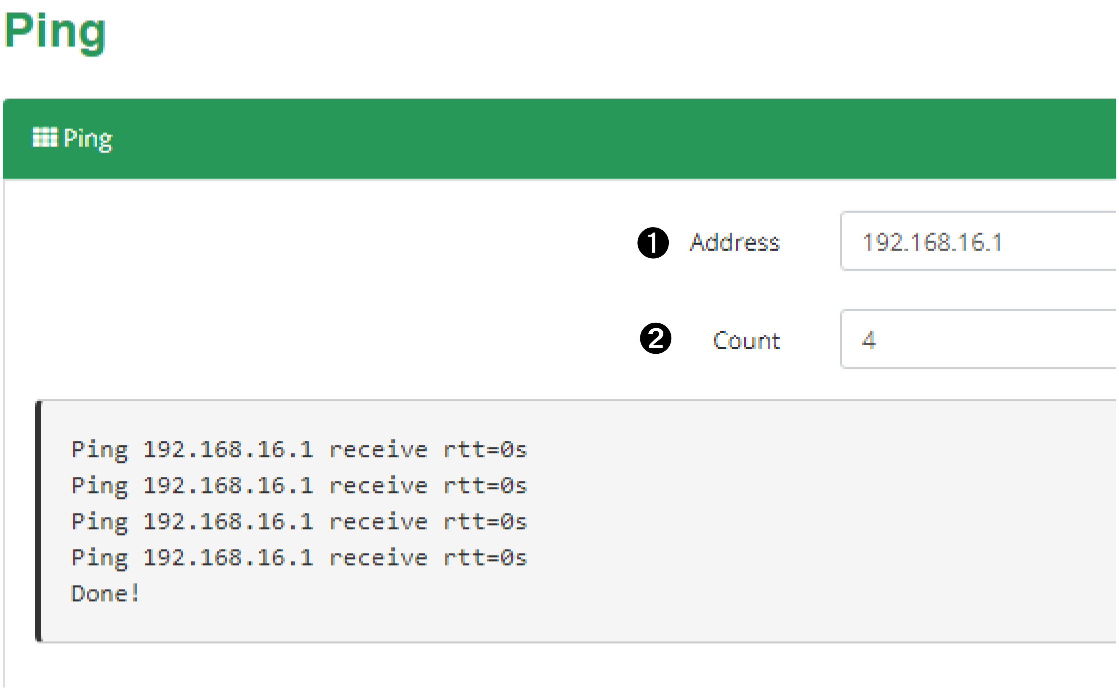
B. Find the selected event and combine with dedicated action.

17. Diagnostics

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

- Ping
- ARP Table

Ping



Address: 192.168.16.1

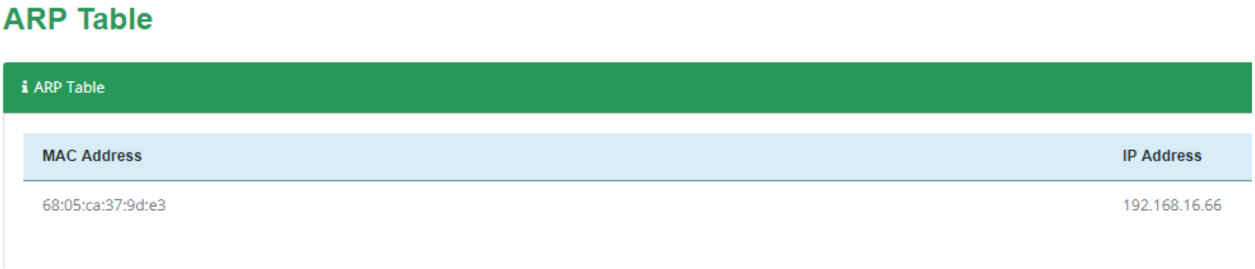
Count: 4

```
Ping 192.168.16.1 receive rtt=0s
Ping 192.168.16.1 receive rtt=0s
Ping 192.168.16.1 receive rtt=0s
Ping 192.168.16.1 receive rtt=0s
Done!
```

Name	Description
❶ **Address:**	Enter the IP address to ping.
❷ **Count:**	Enter how many times to ping the address.

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.



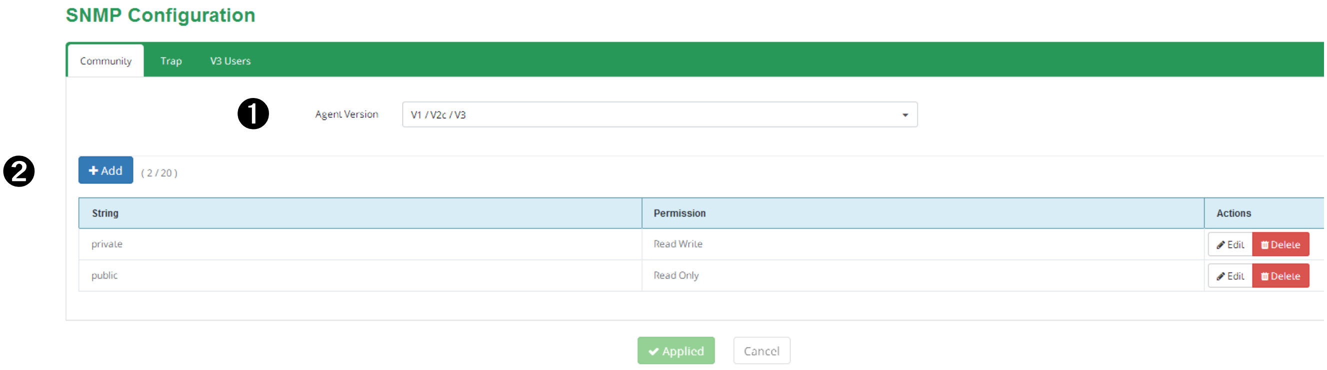
ARP Table

ℹ ARP Table

MAC Address	IP Address
68:05:ca:37:9d:e3	192.168.16.66

18. 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.



SNMP Configuration

Community | Trap | V3 Users

Agent Version: V1 / V2c / V3

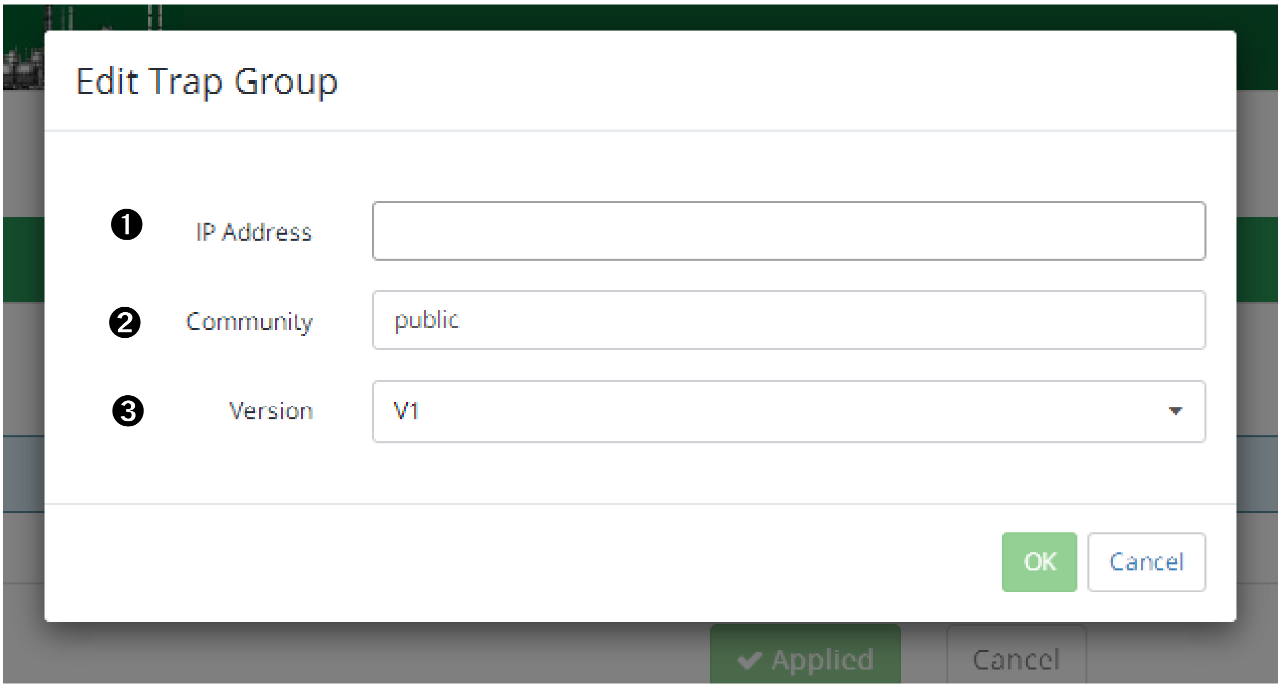
+ Add (2 / 20)

String	Permission	Actions
private	Read Write	Edit Delete
public	Read Only	Edit Delete

✓ Applied | Cancel

Community

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>❶ <b>Agent version:</b></td><td>Detected by system automatically.
<table>
<tr><th>Possible Values</th><th>Default Setting</th></tr>
<tr><td>V1/ V2c/ V3</td><td>Detected by system automatically.</td></tr>
</table></td></tr>
<tr><td>❷ <b>Add:</b></td><td>add the community string of SNMP protocol with read only permission or read/write permission.</td></tr>
</table>



Edit Trap Group

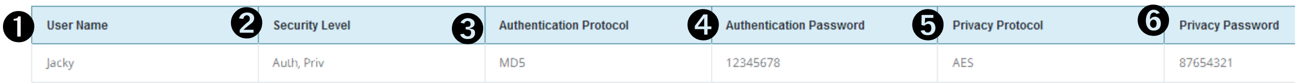
❶ IP Address:

❷ Community: public

❸ Version: V1

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. **Possible Values**: V1 or V2c **Default Setting**: V2c



❶ User Name	❷ Security Level	❸ Authentication Protocol	❹ Authentication Password	❺ Privacy Protocol	❻ Privacy Password
Jacky	Auth, Priv	MD5	12345678	AES	87654321

V3 Users

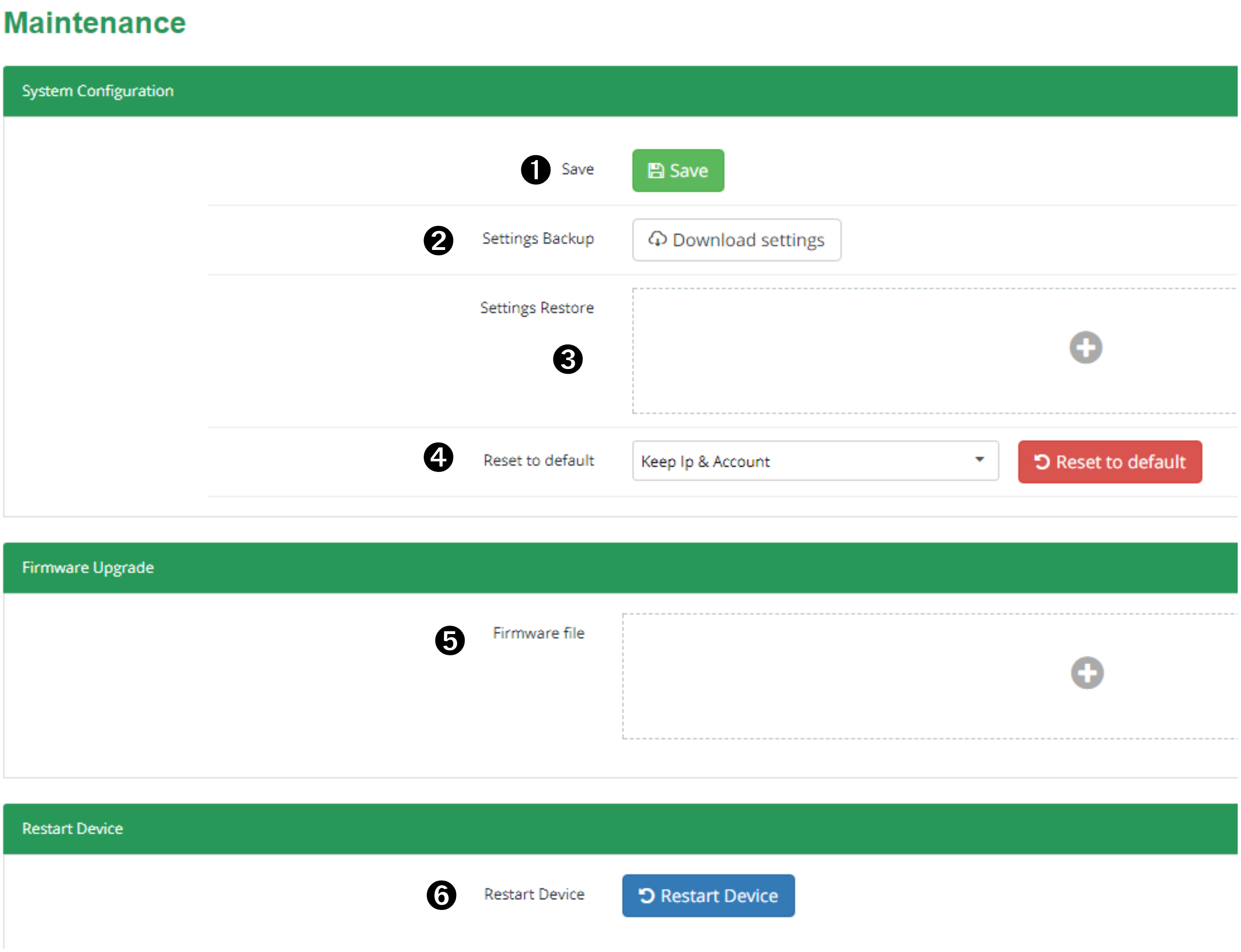
Name	Description
❶ **User name:**	Set the user name.
❷ **Security Level:**	Set up the access level, you can choose Authentication or Privacy or Both.
❸ **Authentication Protocol:**	Set the authenticated way, the default value was MD5

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.

19. 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.



Name	Description
❶ **Save:**	Save configuration file to system.
❷ **Settings Backup:**	Download/ export the configuration from switch for back up.
❸ **Settings**	Upload/ import a previous configuration to startup.

Restore:

❹ Reset to default: Reset the switch with four resetting options.

Resetting Options	Default Setting
Keep IP & Account, Keep User Accounts, Keep Network Configs, Restore Everything	Keep IP & Account

❺ Firmware update: Update new firmware to switch

❻ Restart Device: Reboot switch.

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:

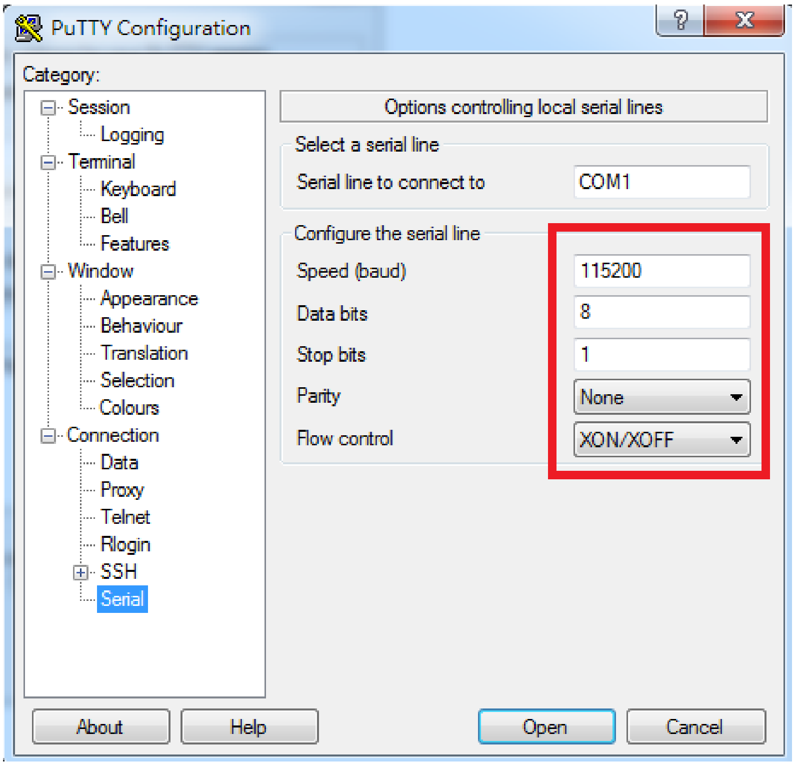
Baud Rate: 115200 bps

Data Bits: 8

Parity: none

Stop Bit: 1

Flow control: None



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM1

Configure the serial line

Speed (baud): 115200

Data bits: 8

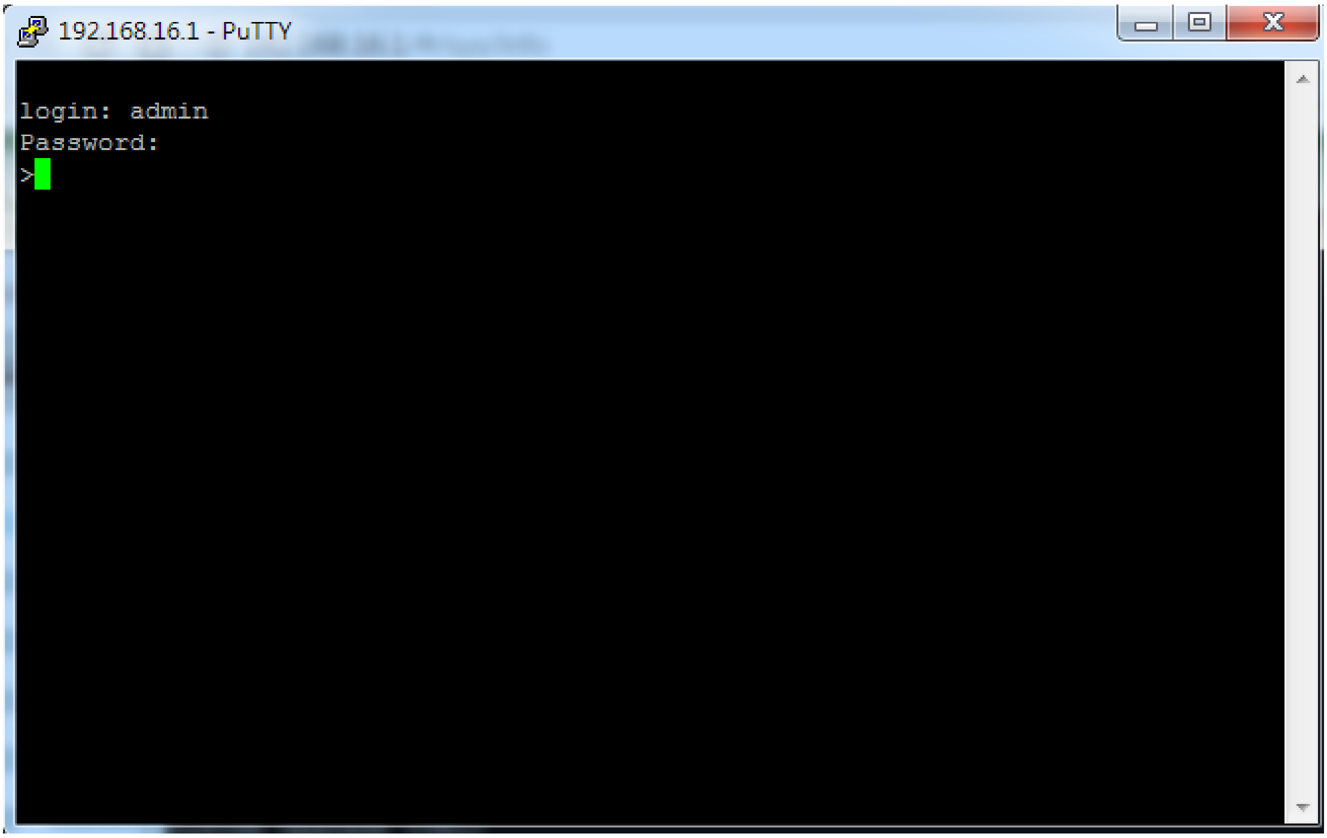
Stop bits: 1

Parity: None

Flow control: XON/XOFF

The settings of communication parameters

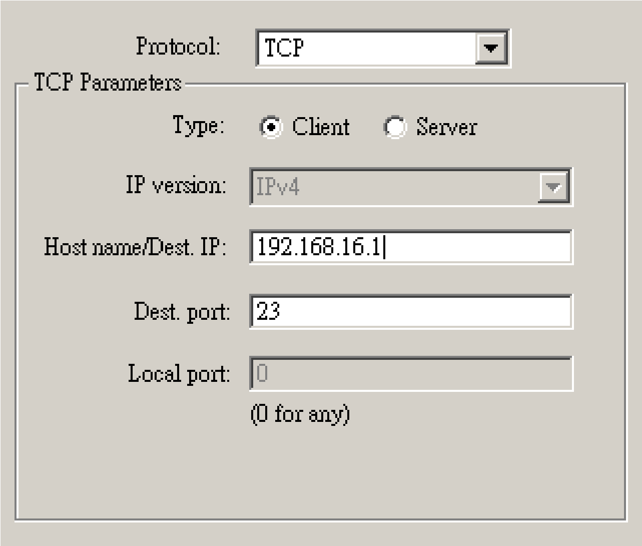
Click '**OK**' to complete the work and the blank screen will show up, when it does then press Enter key to have the login prompt appears. And now please key in "**cli**" to enter the command line mode and then key in '**admin**' (default value) for both Login and Password and press Enter to get to the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



```
login: admin
Password:
>
```

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.



Protocol: TCP

TCP Parameters

Type: ● Client ○ Server

IP version: IPv4

Host name/Dest. IP: 192.168.16.1

Dest. port: 23

Local port: 0

(0 for any)

Lantech

http://www.lantechcom.tw

Technical Assistance

Please contact us directly to reach our technical support team:

Telephone: +886-2-2799-5589

E-mail: support@lantechcom.tw