Lantech

IPES-3408GSFP

4 1000 SFP +8 10/100TX L2 + PoE Industrial Managed Switch

User Manual

Beta.04

July. 2013

Recommendation for Shielded network cables

STP cables have additional shielding material that is used to reduce external interference. The shield also reduces the emission at any point in the path of the cable. Our recommendation is to deploy an STP network cable in demanding electrical environments. Examples of demanding indoor environments are where the network cable is located in parallel with electrical mains supply cables or where large inductive loads such as motors or contactors are in close vicinity to the camera or its cable. It is also mandatory to use an STP cable where the power device (like IP camera) is used outdoors or where the network cable is routed outdoors.

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

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

Chapter 1 Introduction

The IPES-3408 series Managed Industrial Switch is a cost-effective solution and meets the high reliability requirements demanded by industrial applications. Using fiber port can extend the connection distance that increases the network elasticity and performance.

1.1 Hardware Features

Standard	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX IEEE802.3z Gigabit fiber IEEE802.3x Flow Control and Back Pressure IEEE802.3ad Port trunk with LACP IEEE802.1d Spanning Tree IEEE802.1w Rapid Spanning Tree IEEE802.1s Multiple Spanning Tree IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.1AB Link Layer Discovery Protocol (LLDP) IEEE 802.1X User Authentication (Radius) IEEE802.1p Class of Service IEEE802.1Q VLAN Tag IEEE802.3at/af Power over Ethernet IEEE 802.3az Efficient Energy Ethernet
Switch Architecture	Back-plane (Switching Fabric): 9.6Gbps Packet throughput ability (Full-Duplex): 23.8Mpps @64bytes
Transfer Rate	14,880pps for Ethernet port 148,800pps for Fast Ethernet port 1,488,000pps for Gigabit Fiber Ethernet port
MAC Address	16K MAC address table

Connector	10/100TX: 8 x RJ-45 type connector Mini-GBIC: 4 x 1000 SFP Sockets Power & P-Fail connector: 1 x 6-pole terminal block RS-232 connector: 1 x RJ-45 type connector
Network Cable	10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable EIA/TIA-568 100-ohm (100m) 100Base-TX: 2-pair UTP/STP Cat. 5/ 5E cable EIA/TIA-568 100-ohm (100m)
Optical Fiber	Multi-mode: 50/125um~62.5/125um; Single mode: 9/125um Wavelength: 850nm (Multi-mode) / 1310nm (Single-mode)
Protocol	CSMA/CD
LED	Per unit: Power 1 (Green), Power 2 (Green), P-Fail (Red) Ethernet port: Link/Activity (Green), Speed (Green); Mini-GBIC: Link/Activity (Green)
Power Supply	48~56VDC, Redundant power input with 1500VDC isolation -48VDC is single power input
Power Consumption	10Watts (switch)/ 240Watts(with PoE)
Operating Humidity	5% to 95% (Non-condensing)
Operating Temperature	-20^{o}C ~ 60^{o}C
Storage Temperature	-40^{o}C ~ 85^{o}C
Case Dimension	Metal case. IP-30, 65 (W) x 105 (D) x 152 (H) mm
Installation	DIN rail and wall mount ear
EMI	FCC Class A, CE EN61000-4-2, CE EN61000-4-3, CE EN-61000-4-4, CE EN61000-4-5, CE EN61000-4-6, CE EN61000-4-8, CE EN61000-4-11, CE EN61000-4-12, CE EN61000-6-2, CE EN61000-6-4

Stability Testing	IEC60068-2-32 (Free fall), IEC60068-2-27 (Shock), IEC60068-2-6 (Vibration)

1.2 Software Features

Management	SNMP v1 v2c, v3/ Web/Telnet/CLI
SNMP MIB	RFC 1215 Traps MIB, RFC 1213 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 1643 EtherLike, RFC 1757 RMON, RSTP MIB, Private MIB, LLDP MIB
ITU G.8032	Support ITU G.8032 v2 for Ring protection in less than 10ms for self-heal recovery < 256 switches which can be compatible with other ITU G.8032 metro switches Support various ring/chain topologies Ring covers data & multicast* packets
Pro-Ring 2se*	Self-healing recovery in less than 20ms for Single Ring topology < 50switches
User friendly UI	● Auto topology drawing ● Topology demo ● Auto configuration for G.8032*
Port Trunk with LACP	LACP Port Trunk: 4 Trunk groups/Maximum 4 trunk members Load balancing through LACP to distribute load*
LLDP	Supports LLDP to allow switch to advise its identification and capability on the LAN

CDP	Cisco Discovery Protocol for topology mapping
PoE Management	● PoE Detection to check if PD is hang up then restart the PD ● PoE Scheduling to On/OFF PD upon routine time table
VLAN	Port Based VLAN IEEE 802.1Q Tag VLAN (256 entries)/ VLAN ID (Up to 4K, VLAN ID can be assigned from 1 to 4096.) GVRP (256 Groups)*,GMRP*, MVRP (Multi VLAN Registeration)*, QinQ
IPv6	Support dual stack for IPv4 and IPv6 Support Plug and Play function IPv6 Logo Committee certified Perform with following RFCs: 1. RFC 2460 – IPv6 Specification 2. RFC 4861 – Neighbor Discovery for IPv6 3. RFC 4862 – IPv6 Stateless Address Auto-configuration 4. RFC 1981 – Path MTU Discovery for IPv6
Network Security	Support 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder. 802.1X access control for port based and MAC based authentication/MAC-IP-Port binding Management access control with priority * 256 Policy based Access Control List* SSL/ SSH for Management

	TACACS+ for Authentication*
SMTP/Text SMS	Supports SMTP Server and 6 e-mail accounts for receiving event alert; can send SMS text alert via mobile
Spanning Tree	Supports IEEE802.1d Spanning Tree and IEEE802.1w Rapid Spanning Tree, IEEE802.1s Multiple Spanning Tree
Quality of Service	The quality of service determined by port, Tag and IPv4 Type of service, IPv4 Different Service
Class of Service	Supports IEEE802.1p class of service, per port provides 4 priority queues
IP Security	Supports 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder.
Login Security	Supports IEEE802.1X Authentication/RADIUS
Port Mirror	Support 3 mirroring types: “RX, TX and Both packet”
IGMP	Support IGMP snooping v1,v2,v3; Supports IGMP static route 256 multicast groups and IGMP query
Multicast VLAN Registration*	MVR enables multicast packets go through VLAN for VOD application
Bandwidth Control	Support ingress packet filter and egress packet limit. The egress rate control supports all of packet type. Ingress filter packet type combination rules are Broadcast/Multicast/Flooded Unicast packet, Broadcast/Multicast packet, Broadcast packet only and all types of packet. The packet filter rate can be set an accurate value through

	the pull-down menu for the ingress packet filter and the egress packet limit.
RTC	Built-in Real Time Clock to keep track of time always
Flow Control	Supports Flow Control for Full-duplex and Back Pressure for Half-duplex
System Log	Supports System log record and remote system log server
SMTP	Supports SMTP Server and 6 e-mail accounts for receiving event alert
Relay Alarm	Provides one relay output for port breakdown, power fail Alarm Relay current carry ability: 1A @ DC24V
SNMP Trap	1. Topology Change 2. Power Trap 3. MAC-Violation
DHCP	Provides DHCP Client/ DHCP Server/ Port and IP Binding
DNS	Provides DNS client feature and supports Primary and Secondary DNS server
SNTP	Supports SNTP to synchronize system clock in Internet
Firmware Update	Supports TFTP firmware update, TFTP backup and restore.
Configuration Upload/Download	Supports text configuration file for system quick installation; Support factory reset button to restore all settings back to factory default.

ifAlias	Each port allows an alphabetic string of 128-byte assigned as its own unique name via the SNMP or CLI interface

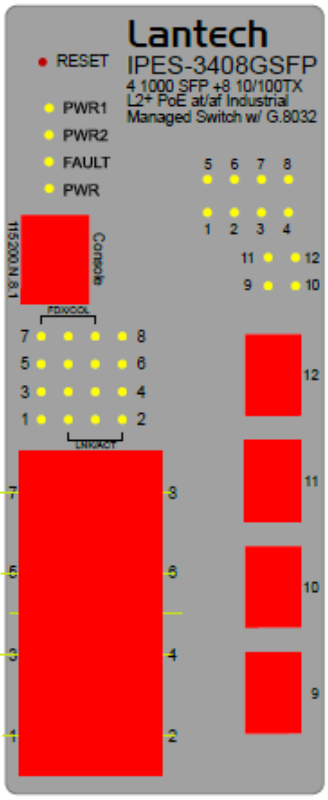
Chapter 2 Hardware Description

In this paragraph, it will describe the Industrial switch's hardware spec, port, cabling information, and wiring installation.

2.1 Physical Dimension

65 (W) x 105 (D) x 152 (H) mm

2.2 Front Panel



Front Panel of the industrial switch

2.3 Top View

The top panel of the Industrial Managed Industrial Switch has one terminal block connector of two DC power inputs and one fault alarm.

Top Panel of the industrial switch

2.4 LED Indicators

The diagnostic LEDs that provide real-time information of system and optional status are located on the front panel of the industrial switch. The following table provides the description of the LED status and their meanings for the switch.

LED	Color	Status	Meaning
PWR	Green	On	The switch unit is power on
		Off	No power
PWR1	Green	On	Power 1 is active
		Off	Power 1 is inactive
PWR2	Green	On	Power 2 is active
		Off	Power 2 is inactive
FAULT	Red	On	Power or port failure
		Off	No failure
P1 ~ P12	Link/Ack	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
	FDX/COL	On	The port is operating in full-duplex mode.
		Blinking	Collision of Packets occurs.
		Off	The port is in half-duplex mode or no device is attached.

Chapter 3 Hardware Installation

In this paragraph, we will describe how to install the IPES-3408 series Managed Industrial Switch and the installation points attended to it.

3.1 Installation Steps

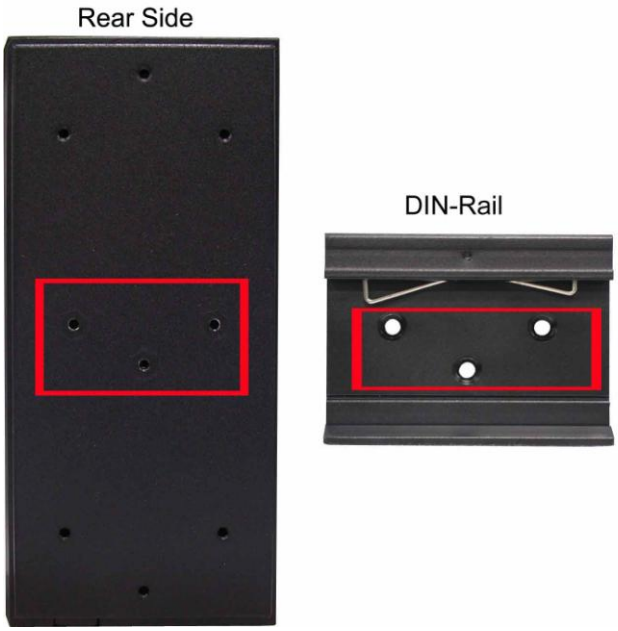
1. Unpack the Industrial switch
2. Check if the DIN-Rail is screwed on the Industrial switch or not. If the DIN-Rail is not screwed on the Industrial switch, please refer to **DIN-Rail Mounting** section for DIN-Rail installation. If users want to wall mount the Industrial switch, please refer to **Wall Mount Plate Mounting** section for wall mount plate installation.
3. To hang the Industrial switch on the DIN-Rail track or wall.
4. Power on the Industrial switch. Please refer to the **Wiring the Power Inputs** section for knowing the information about how to wire the power. The power LED on the Industrial switch will light up. Please refer to the **LED Indicators** section for indication of LED lights.
5. Prepare the twisted-pair, straight through Category 5 cable for Ethernet connection.
6. Insert one side of RJ-45 cable (category 5) into the Industrial switch Ethernet port (RJ-45 port) and another side of RJ-45 cable (category 5) to the network device's Ethernet port (RJ-45 port), ex: Switch PC or Server. The UTP port (RJ-45) LED on the Industrial switch will light up when the cable is connected with the network device. Please refer to the **LED Indicators** section for LED light indication.

[NOTE] Make sure that the connected network devices support MDI/MDI-X. If it does not support, use the crossover category-5 cable.

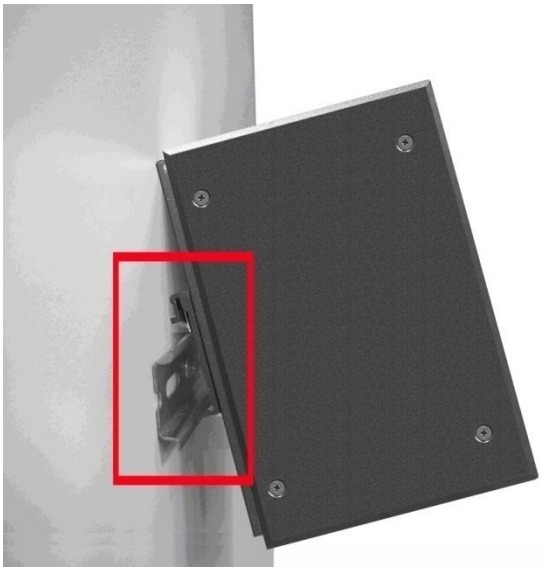
7. When all connections are set and LED lights all show in normal, the installation is complete.

3.2 DIN-Rail Mounting

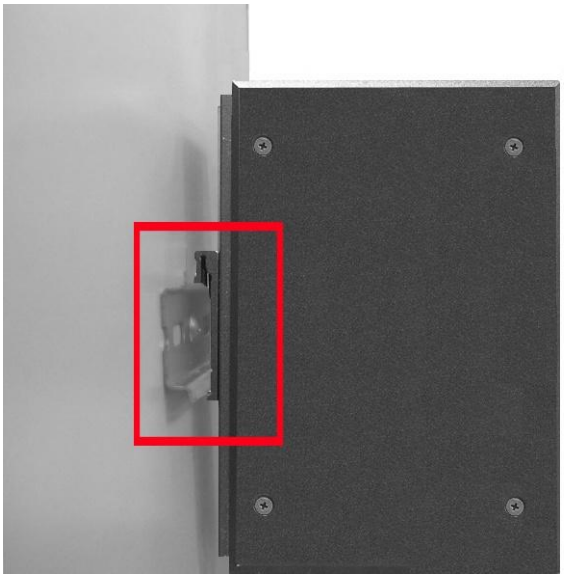
The DIN-Rail is screwed on the industrial switch when out of factory. If the DIN-Rail is not screwed on the industrial switch, please see the following pictures to screw the DIN-Rail on the switch. Follow the steps below to hang the industrial switch.



1. First, insert the top of DIN-Rail into the track.



2. Then, lightly push the DIN-Rail into the track.

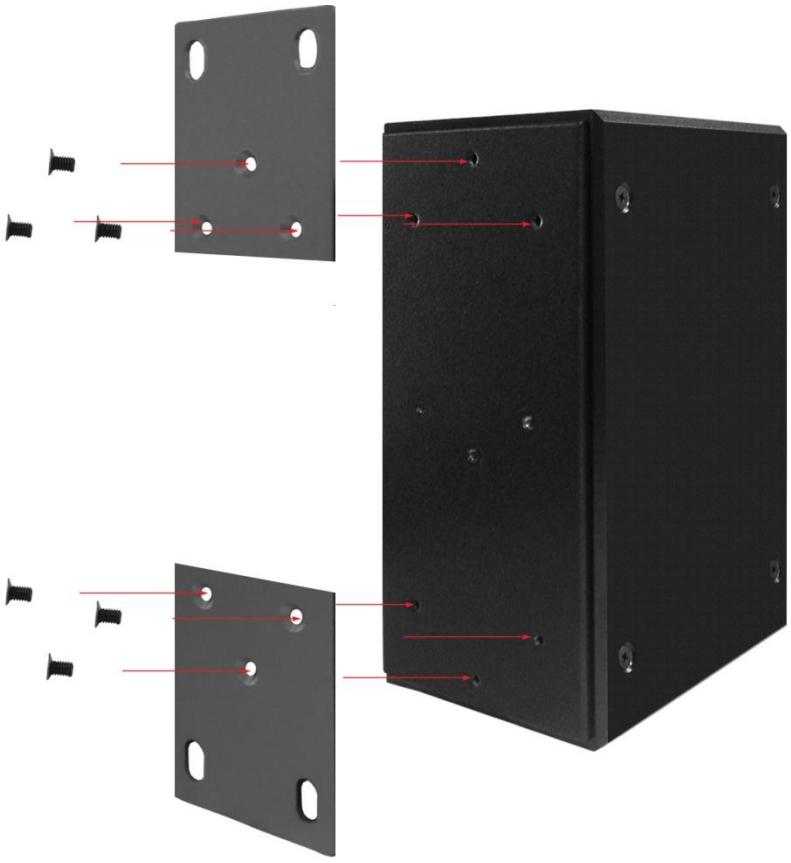


3. Check if the DIN-Rail is tightened on the track or not.
4. To remove the industrial switch from the track, reverse above steps.

3.3 Wall Mount Plate Mounting

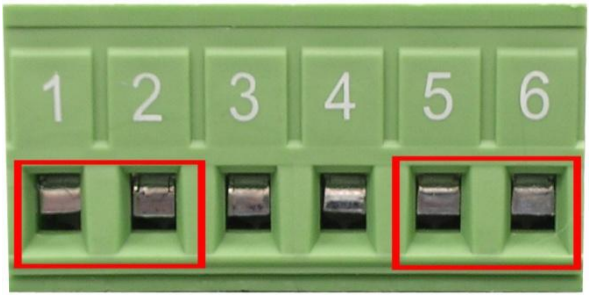
Follow the steps below to mount the industrial switch with wall mount plate.

1. Remove the DIN-Rail from the industrial switch; loose the screws to remove the DIN-Rail.
2. Place the wall mount plate on the rear panel of the industrial switch.
3. Use the screws to screw the wall mount plate on the industrial switch.
4. Use the hook holes at the corners of the wall mount plate to hang the industrial switch on the wall.
5. To remove the wall mount plate, reverse the above steps.

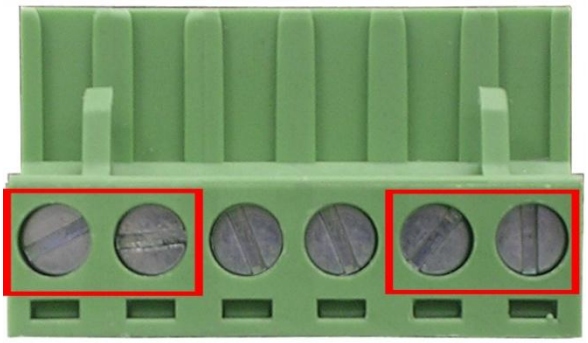


3.4 Wiring the Power Inputs

Please follow the steps below to insert the power wire.



1. Insert AC or DC power wires into the contacts 1 and 2 for power 1, or 5 and 6 for power.



2. Tighten the wire-clamp screws for preventing the wires from loosing.

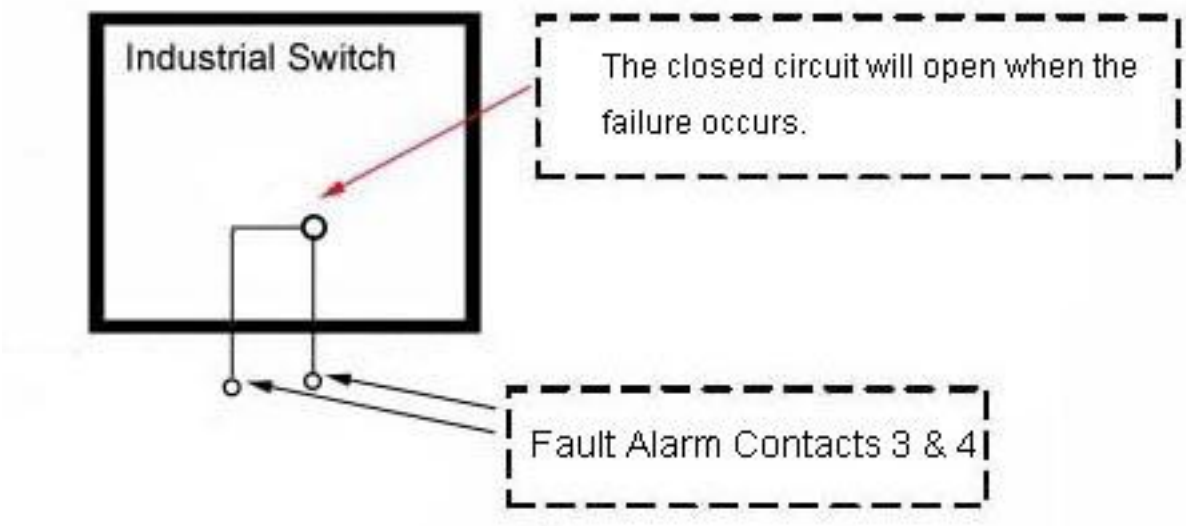
[NOTE] The wire gauge for the terminal block should be in the range between 12 ~ 24 AWG.

3.5 Wiring the Fault Alarm Contact

The fault alarm contacts are in the middle of the terminal block connector as the picture shows below. Inserting the wires, the switch will detect the fault status of the power failure, or port link failure (available for managed model) and then forms an open circuit. The following illustration shows an application example for wiring the fault alarm contacts.

Insert the wires into the fault alarm contacts

[NOTE] The wire gauge for the terminal block should be in the range between 12 ~ 24 AWG.



3.6 Cabling

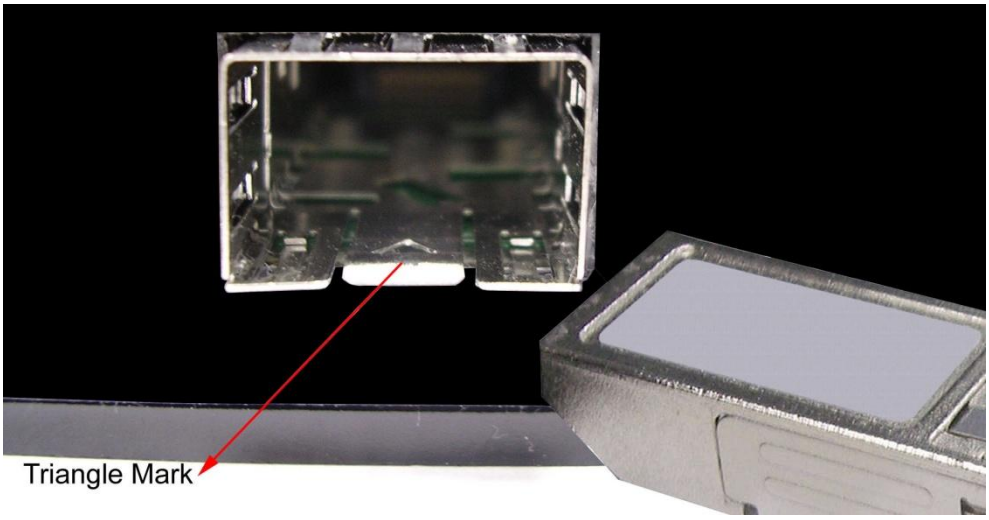
- Use four twisted-pair, Category 5e or above cabling for RJ-45 port connection. The cable between the switch and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) long.
- Fiber segment using **single-mode** connector type must use 9/125 µm single-mode fiber cable. User can connect two devices in the distance up to **30km**.
- Fiber segment using **multi-mode** connector type must use 50 or 62.5/125 µm multi-mode fiber cable. User can connect two devices up to **2km** distances.
- **Gigabit Copper/SFP (mini-GBIC) combo port:**

The Industrial switch has the auto-detected Giga port—Gigabit Copper/SFP combo ports. The Gigabit Copper (10/100/1000T) ports should use Category 5e or above UTP/STP cable for the connection up to 1000Mbps. The small form-factor pluggable (SFP) is a compact optical transceiver used in optical communications for both telecommunication and data communications. The SFP slots supporting dual mode can switch the connection speed between 100 and 1000Mbps. They are used for connecting to the network segment with single or multi-mode fiber. You can choose the appropriate SFP transceiver to plug into the slots. Then use proper multi-mode or single-mode fiber according to the transceiver. With fiber optic, it transmits at speed up to 1000 Mbps and you can prevent noise interference from the system.

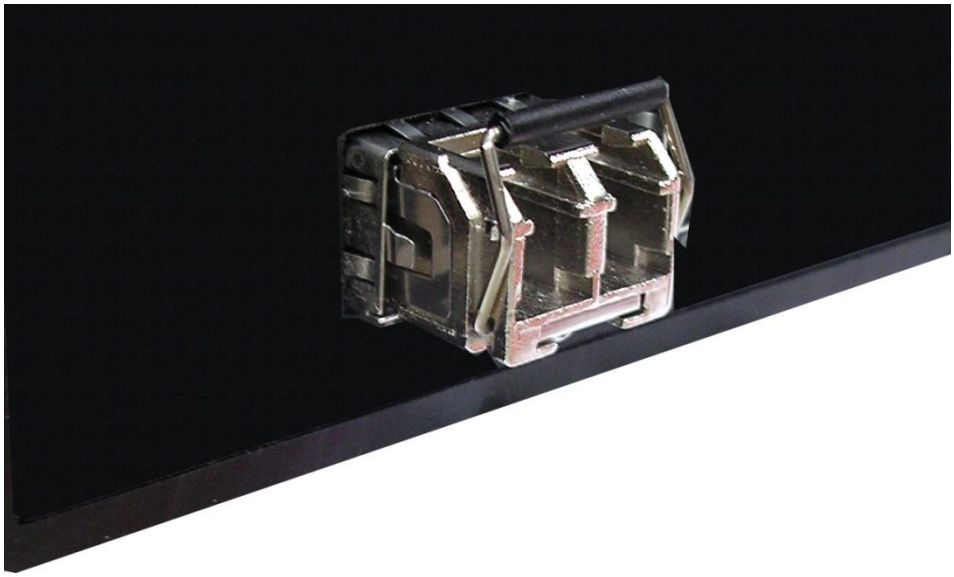
Note	*The SFP/Copper Combo port can't both work at the same time. The SFP port has the higher priority than copper port; if you insert the **1000M** SFP transceiver (which has connected to the remote device via fiber cable) into the SFP port, the connection of the accompanying copper port will link down.* *If you insert the **100M** SFP transceiver into the SFP port even without a fiber connection to the remote, the connection of the accompanying copper port will link down immediately.*

To connect the transceiver and LC cable, please follow the steps shown below:

First, insert the transceiver into the SFP module. Notice that the triangle mark is the bottom of the module.

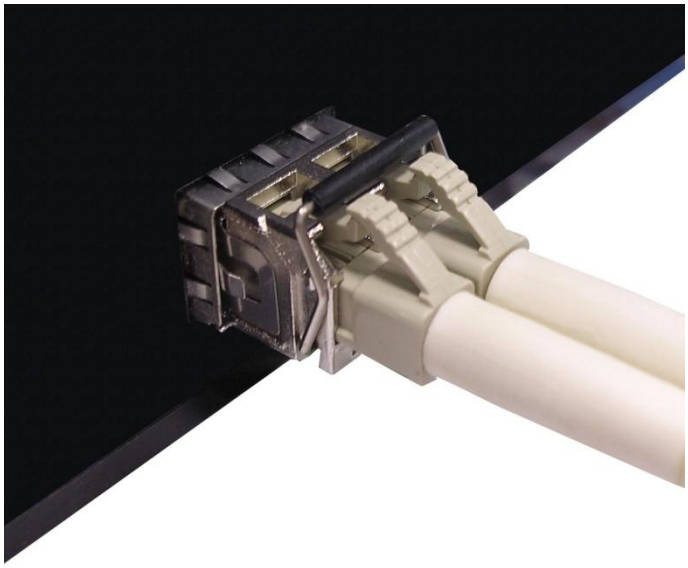


Transceiver to the SFP module



Transceiver Inserted

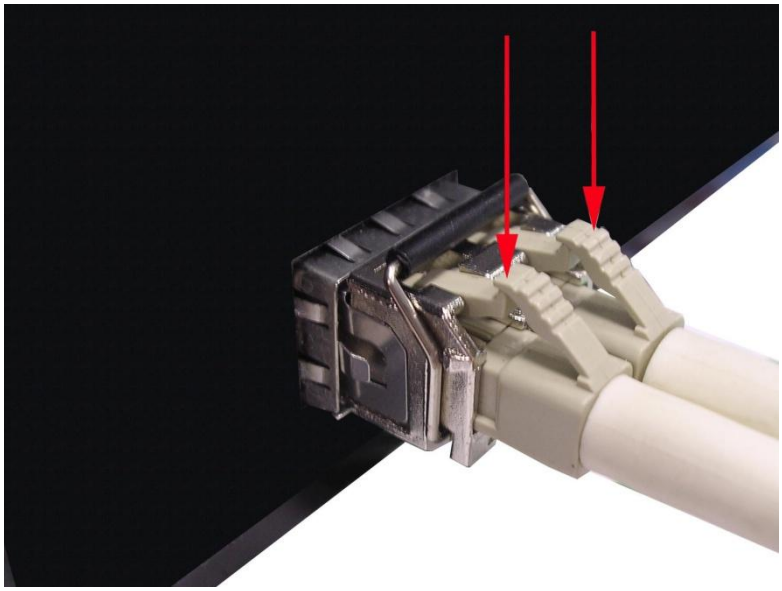
Second, insert the fiber cable of LC connector into the transceiver.



LC connector to the transceiver

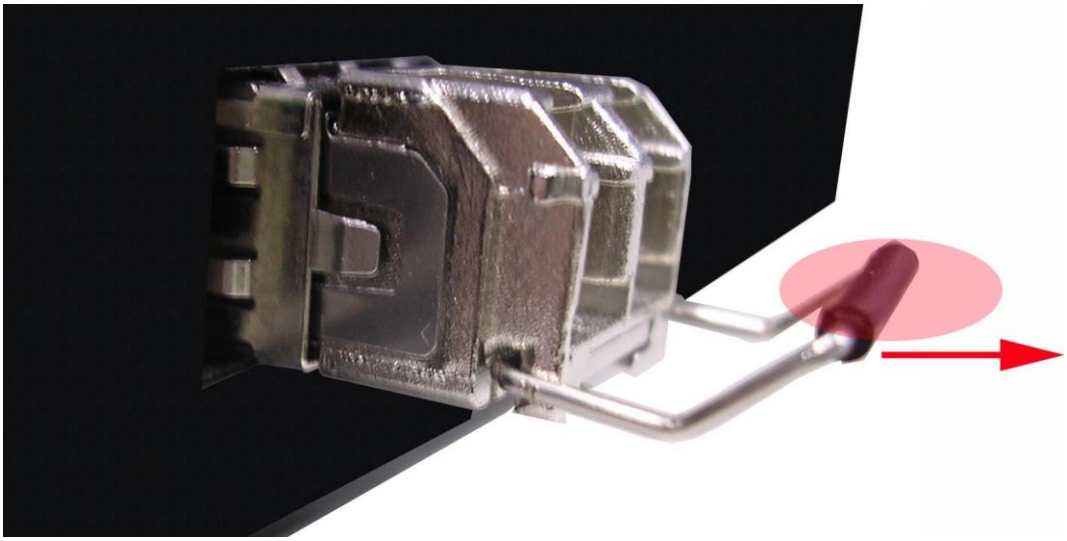
To remove the LC connector from the transceiver, please follow the steps shown below:

First, press the upper side of the LC connector to release from the transceiver and pull it out.



Remove LC connector

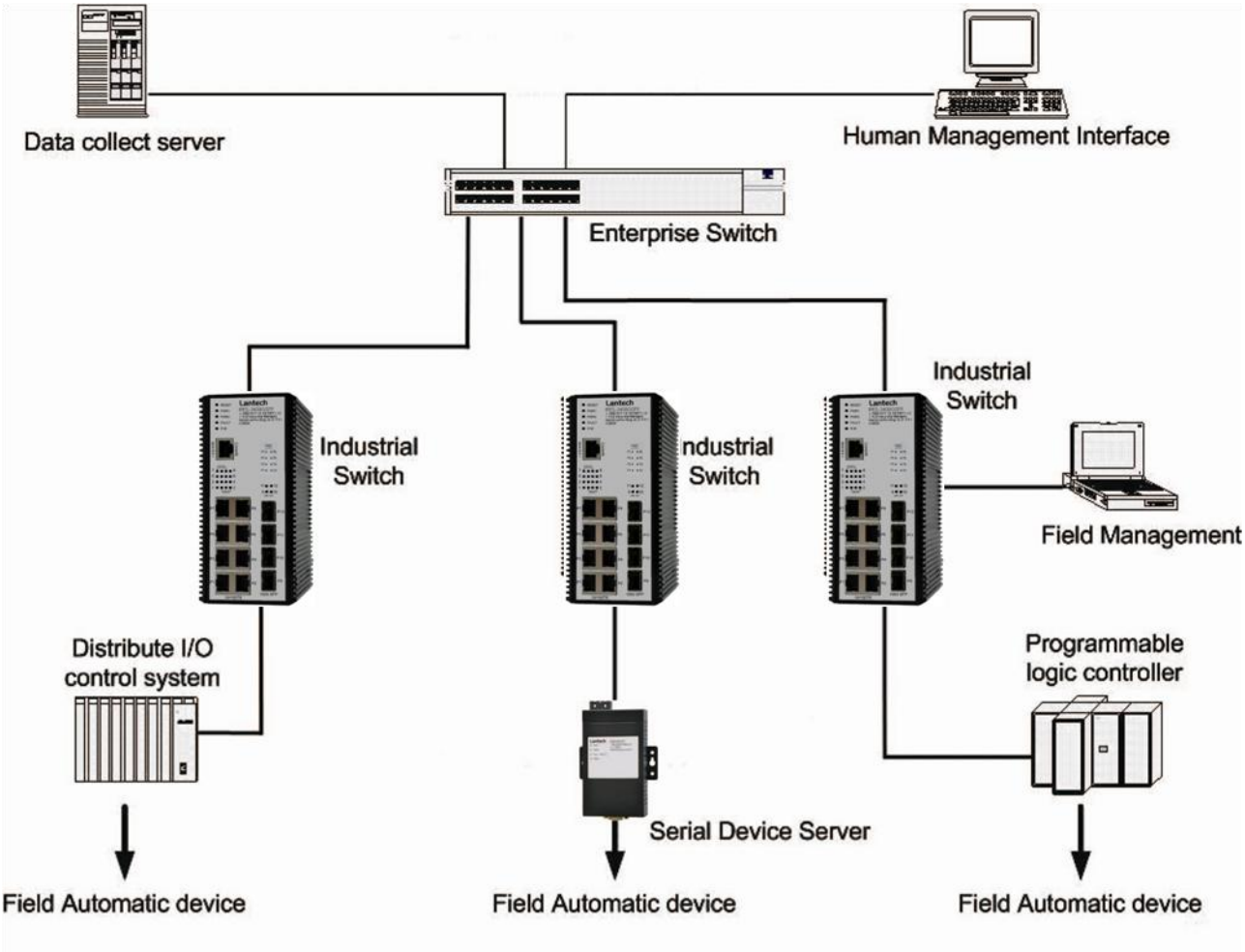
Second, push down the metal loop and pull the transceiver out by the plastic handle.



Pull out from the transceiver

Chapter 4 Network Application

This chapter provides some sample applications to help user to have more actual idea of industrial switch function application. A sample application of the industrial switch is as below:



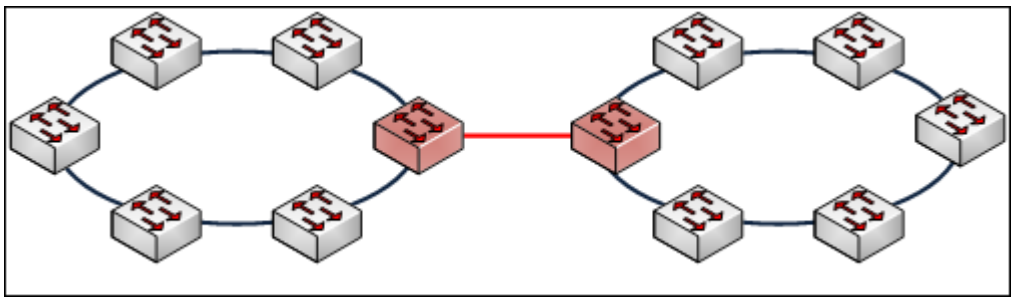
4.1 ITU G.8032 Scheme

Lantech G.8032 protocol is following ITU (International Telecommunication Unit) G.8032 v2 draft. The benefits of G.8032 are:

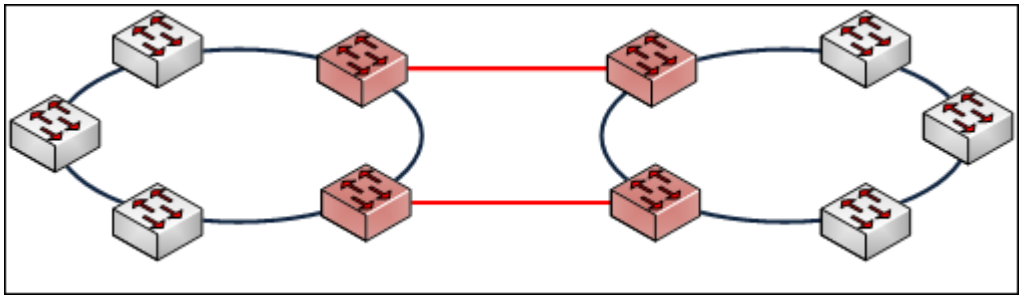
1. <50ms recovery time when failover
2. G.8032 is the standard protocol which can interact amongst different brands without being tie up by the same supplier to ensure the best investment
3. G.8032 has defined the protocol scheme, parameters, functions, test measures to be unified that the users can evaluate the possible network infrastructure without literally testing each brand in large scale.

1-Ring Coupling

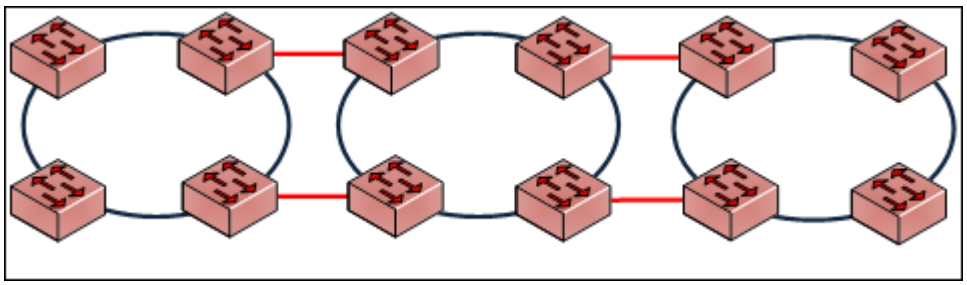
1-1. Single Coupling



1-2. Redundant Coupling

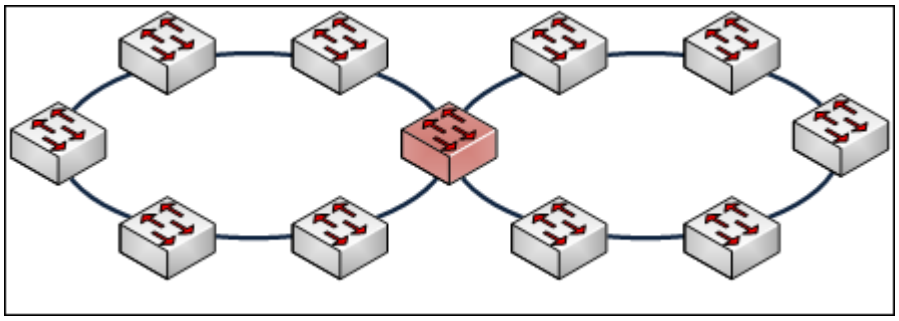


1-3. Redundant Coupling with Multiple Rings

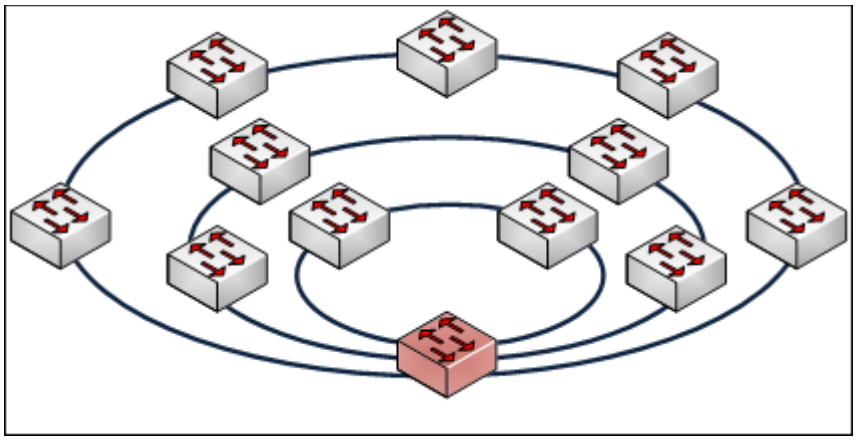


2- Multiple Rings

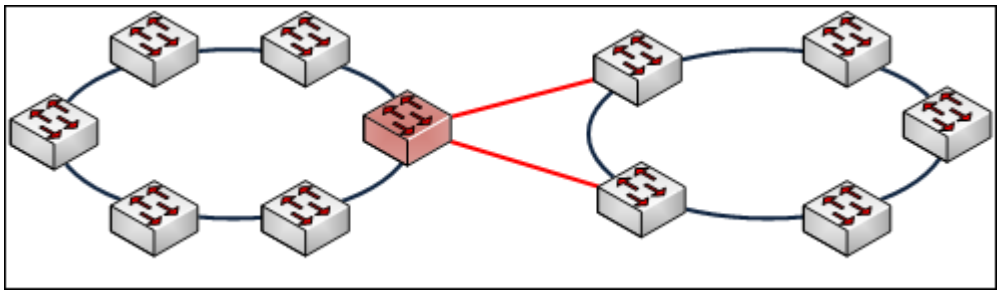
2-1. Dual Rings



2-2. Multiple Rings

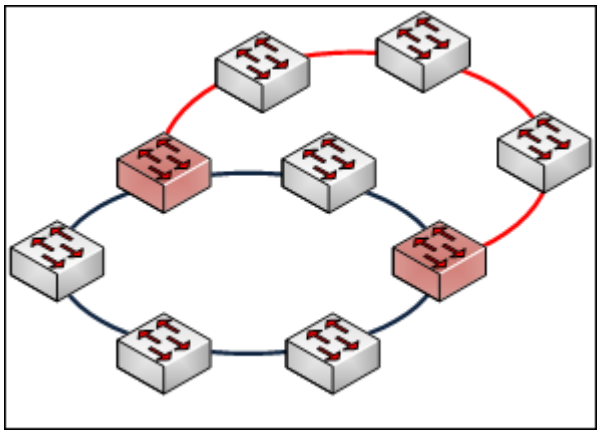


3- Dual Homing

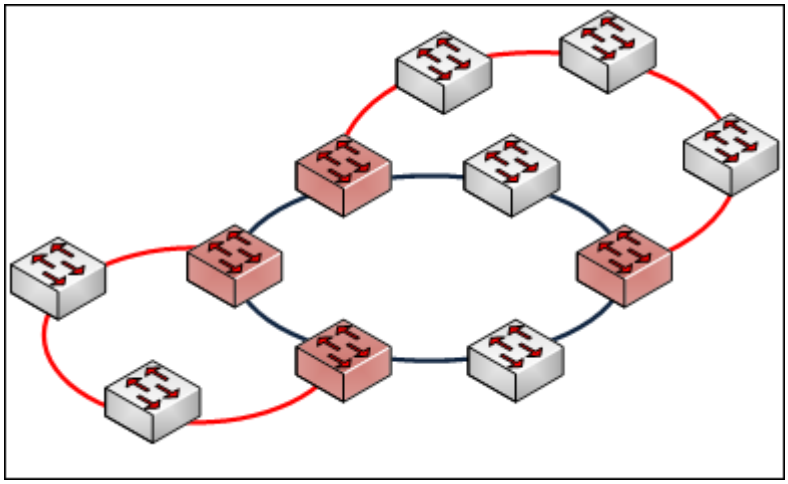


4- Chain

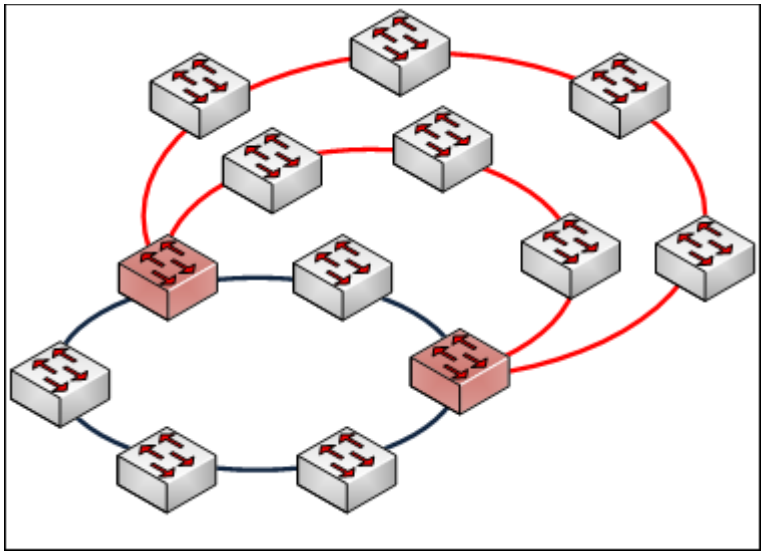
4-1. Single Chain



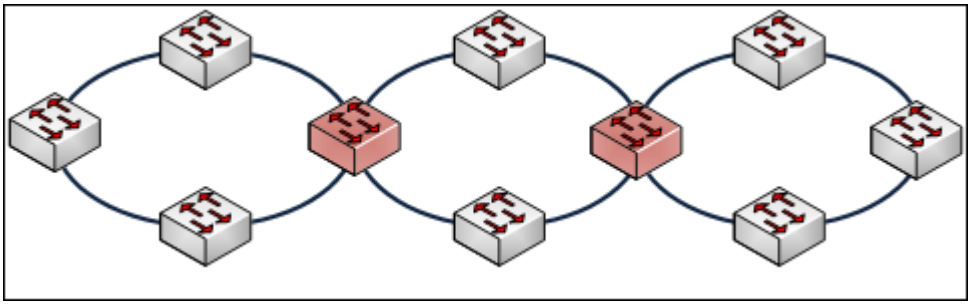
4-2. Multiple Chains



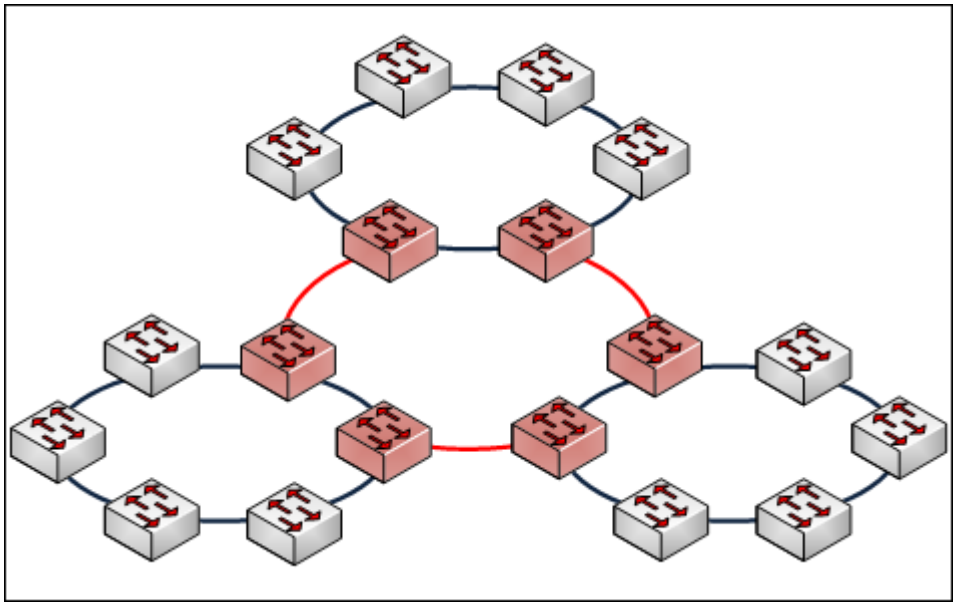
4-3. Multiple Chains Share Common Ends



4-4. Cascade Chain



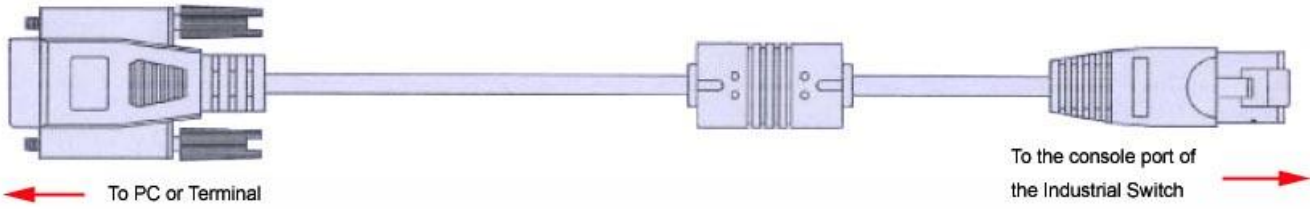
4-5. Chain in Chain

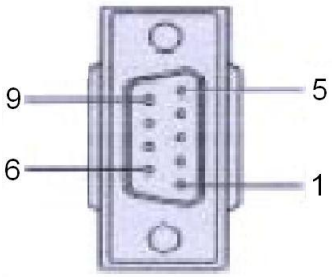


Chapter 5 Console Management

5.1 Connecting to the Console Port

The supplied cable which one end is RS-232 connector and the other end is RJ-45 connector. Attach the end of RS-232 connector to PC or terminal and the other end of RJ-45 connector to the console port of the switch. The connected terminal or PC must support the terminal emulation program.





DB 9-pin Female

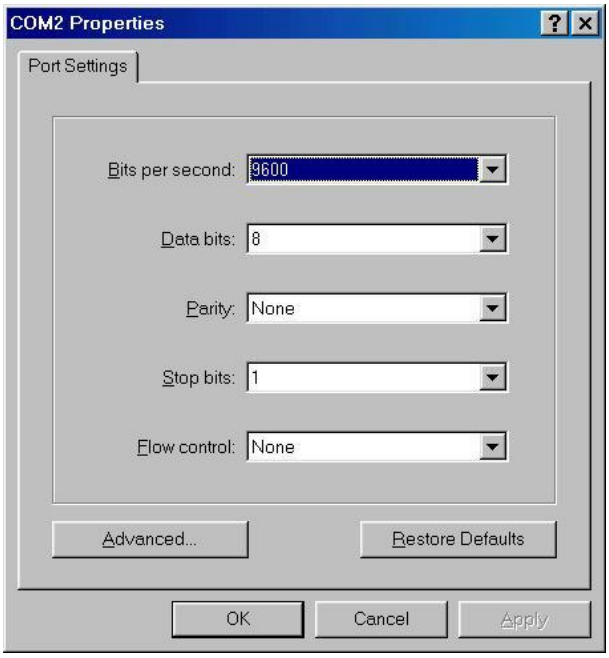
5.2 Pin Assignment

DB9 Connector	RJ-45 Connector	
NC	1	Orange/White
2	2	Orange
3	3	Green/White
NC	4	Blue
5	5	Blue/White
NC	6	Green
NC	7	Brown/White
NC	8	Brown

5.3 Login in the Console Interface

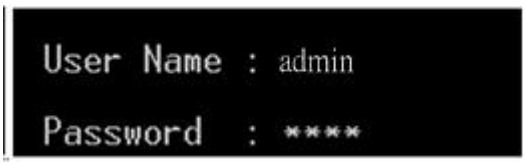
When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

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



The settings of communication parameters

Having finished the parameter settings, click '**OK**'. When the blank screen shows up, press Enter key to have the login prompt appears. Key in '**admin**' (default value) for both User name and Password (use **Enter** key to switch), then press Enter and the Main Menu of console management appears. Please see below figure for login screen.



Console login interface

Chapter 6 Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

6.1 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 Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0 or later version. And, it is applied for Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

6.2 Preparing for Web Management

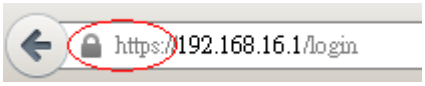
Before using the web management, install the industrial switch on the network and make sure that any one of the PCs on the network can connect with the industrial switch through the web browser. The industrial switch default value of IP, subnet mask, username and password are listed as below:

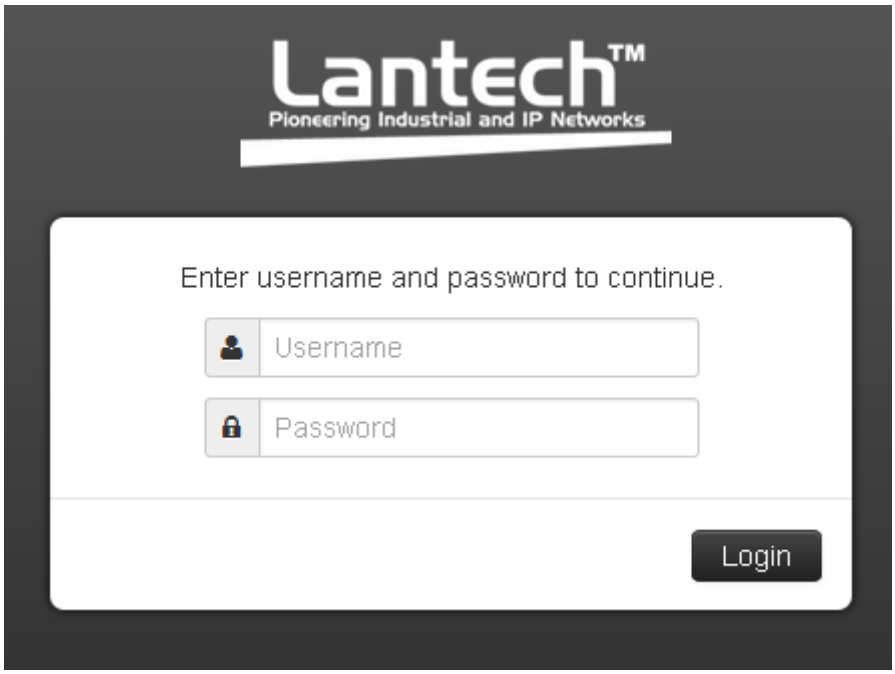
- IP Address: **192.168.16.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.16.254**
- User Name: **admin**
- Password: **admin**

6.3 System Login

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

3. The login screen will appear right after
4. Key in the user name and password. The default user name and password are the same as ‘**root**’.
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 “, amd press “Enter”





Login screen

6.4 System

6.4.1 System Identification Configuration

Name:

An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first or last character must not be a minus sign. The allowed string length is 0 to 255.

Description:

Display the description of switch. The allowed string length is 0 to 255.

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.

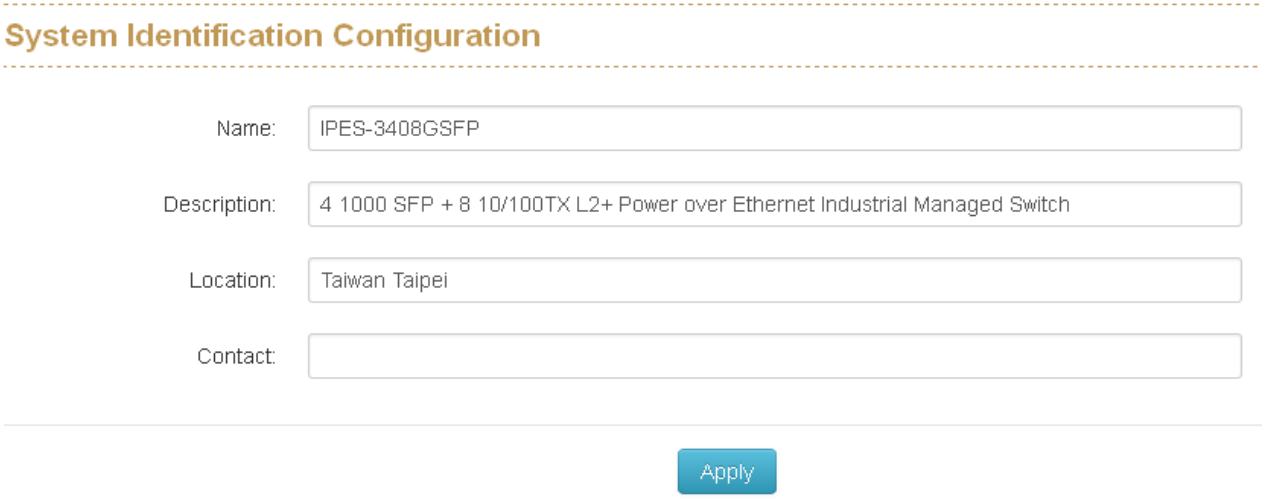
Contact:

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.

Time zone Offset:

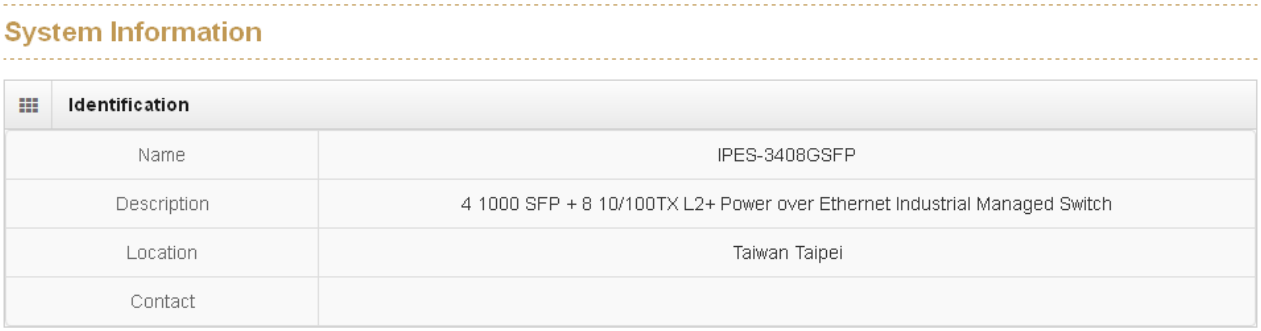
A region on Earth that has a uniform standard time for legal, commercial, and social purposes.

.



6.4.2 Switch Information

This function will show you the basic information of switch.



6.4.3 IP configuration

DHSP client:

Set the switch as DHCP client, it will get the IP address from DHCP server.

IP Address:

Input the IP address of switch

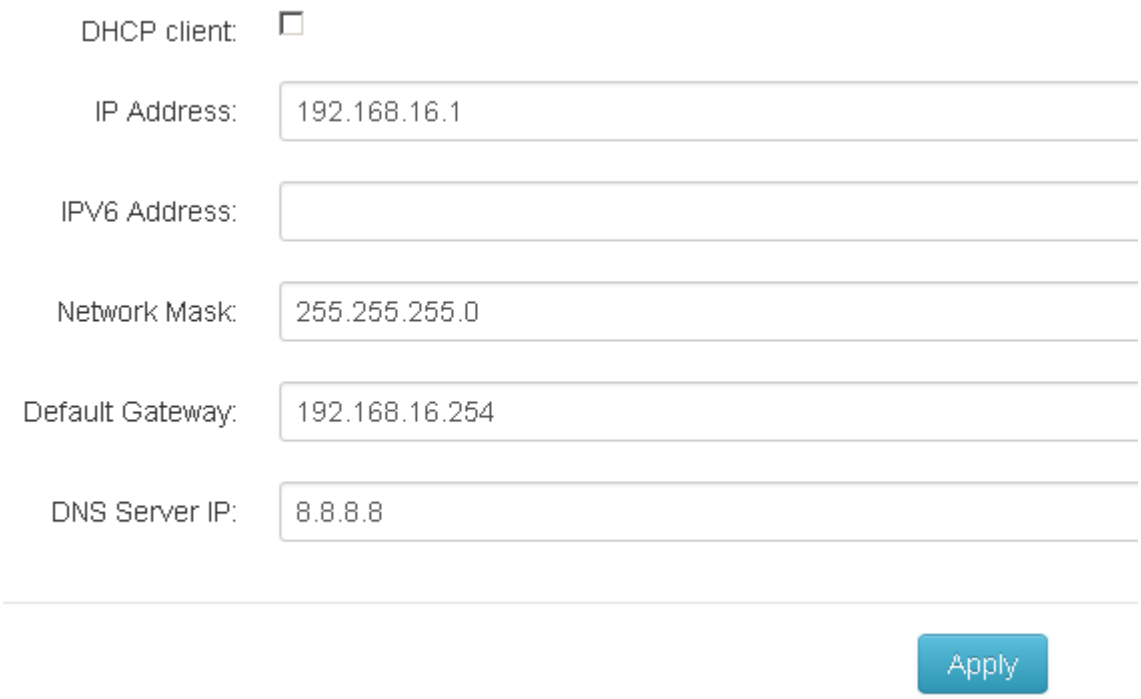
IPV6 Address:

You can input the IP address of IPV6 standard of switch in here.

Network Mask:
The network mask of IP address.

Default Gateway:
The IP address of network gateway, if you need switch to connect with internet, please input correct IP address.

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



6.4.4 DHCP server

Enable DHCP Server:
Enable the DHCP server function of switch

IP Range:
Define the IP range which will assigned to DHCP client from switch.

Subnet Maske:

Define the Subnet Mask which will be assigned to DHCP client.

Gateway:

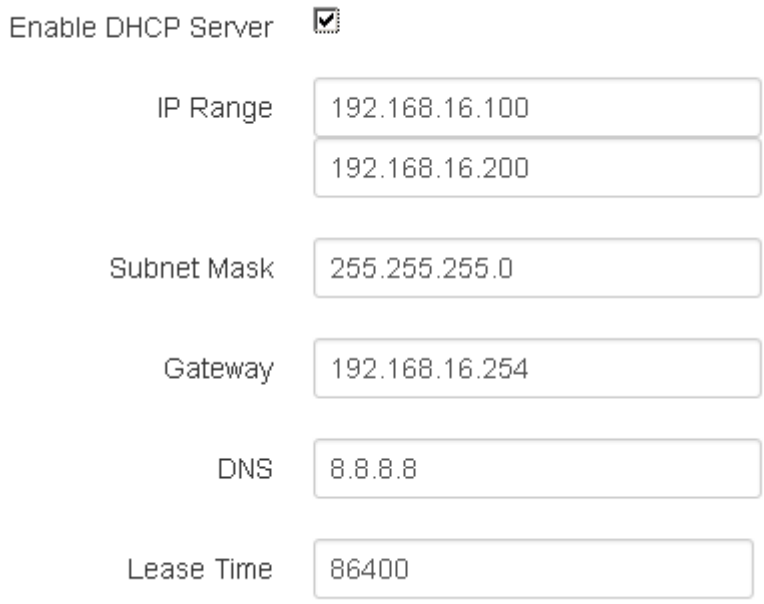
Define the gateway which will be assigned to DHCP client.

DNS:

Define the DNS which will be assigned to DHCP client.

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.



i. System Time

Time Zone:

Universal Time Coordinated. Set the switch location time zone. The following able lists the different location time zone for your reference.

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

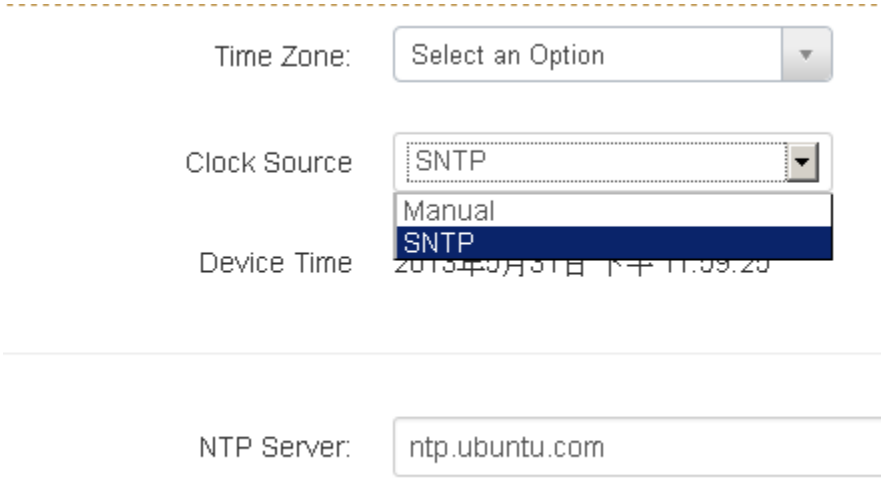
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

Clock Source:

You can set Manual to set the time of switch manually or set SNTP to let the switch synchro the time with NTP server via internet.

NTP server:

The IP address of NTP server.



ii. SNMP Configuration

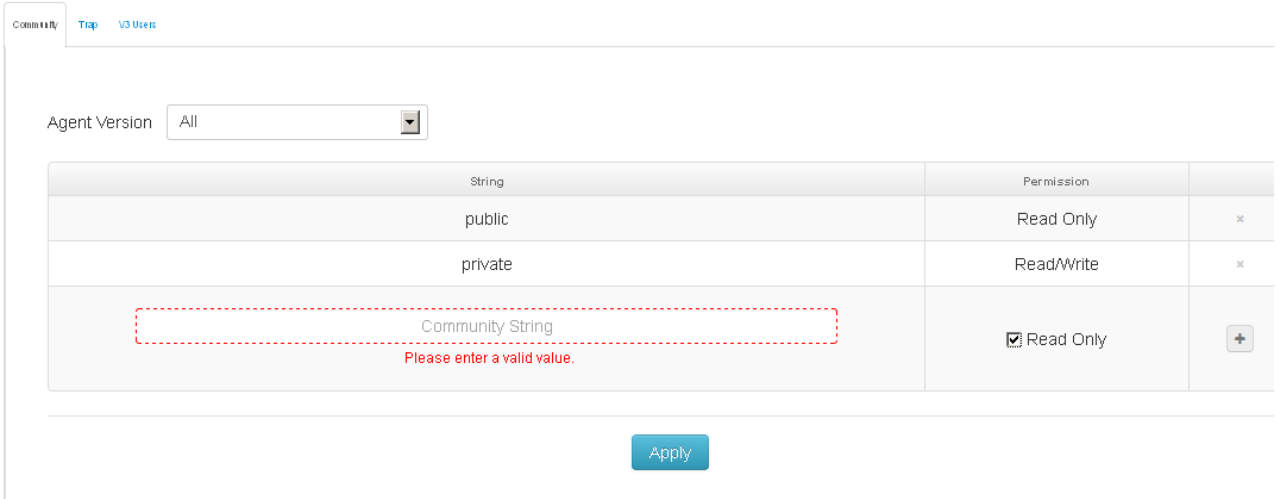
Community

Agent version:

Choose the SNMP V1 or V2c or V3

String:

Set the community string of SNMP protocol with read only persimission or read/write permission.



TRAP

IP address:

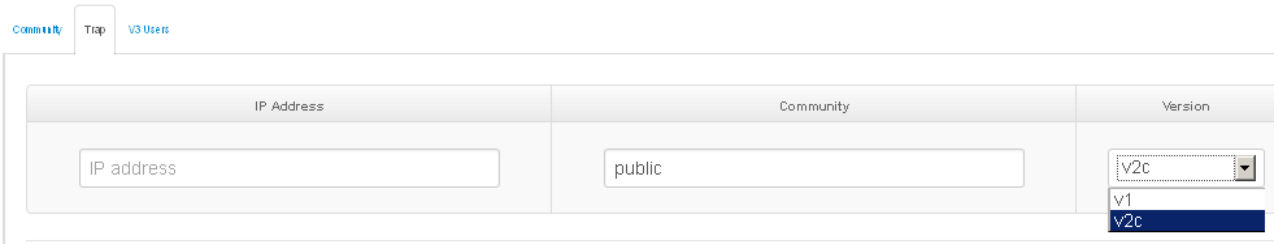
The IP address of trap destination (usually will be the PC of manager).

Community:

The community string of SNMP trap.

Version:

Select the SNMP trap version.



V3 User

User name:

Set the user name.

Security Level:

Set up the access level, you can choose Authentication or Privacy or Both.

Authentication Protocol:

Set the authenticated way, the default value was MD5

Authentication Password:

Set the password of authentication.

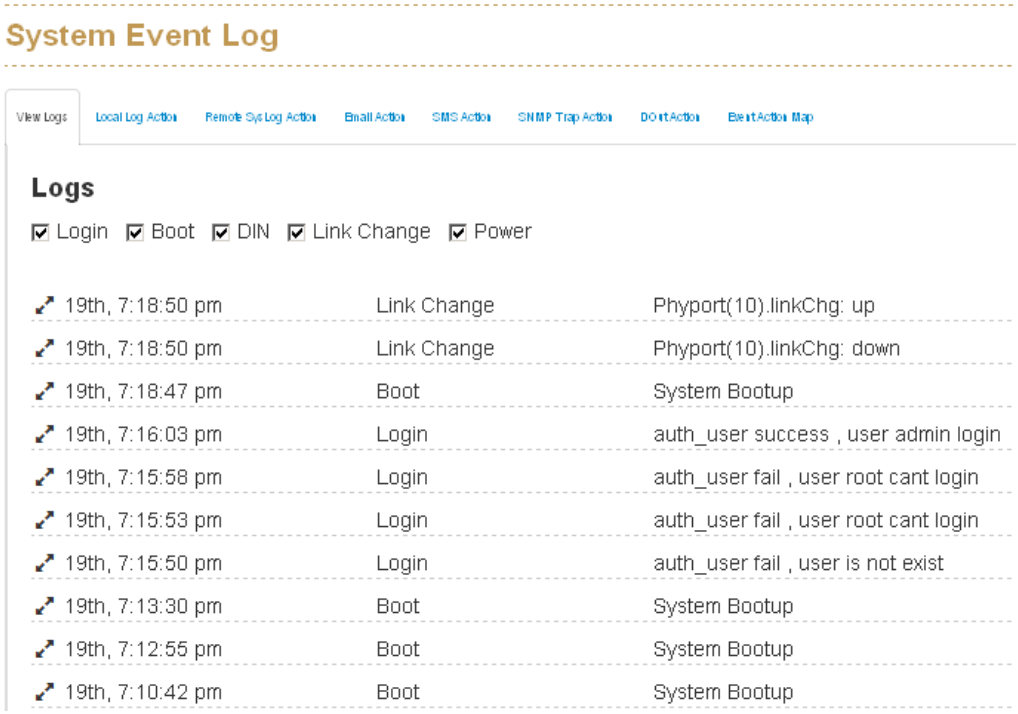
Privacy protocol:

Set the security way, the default value was DES.

Privacy Password:

Set the password of Privacy.

6.4.6 System Event Log



View Logs

Logs

The action of the system log entry. The following action types are supported:

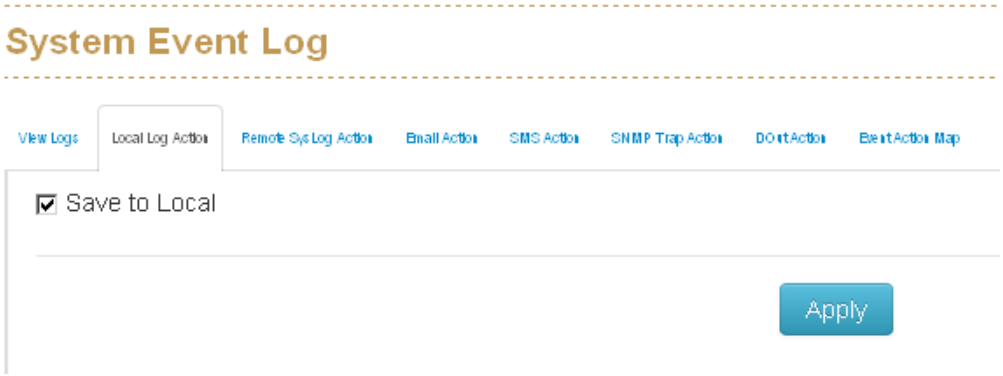
<0> Login: User Login.

<1> Boot: System Boot.

<2> Din: Din Event is triggered.

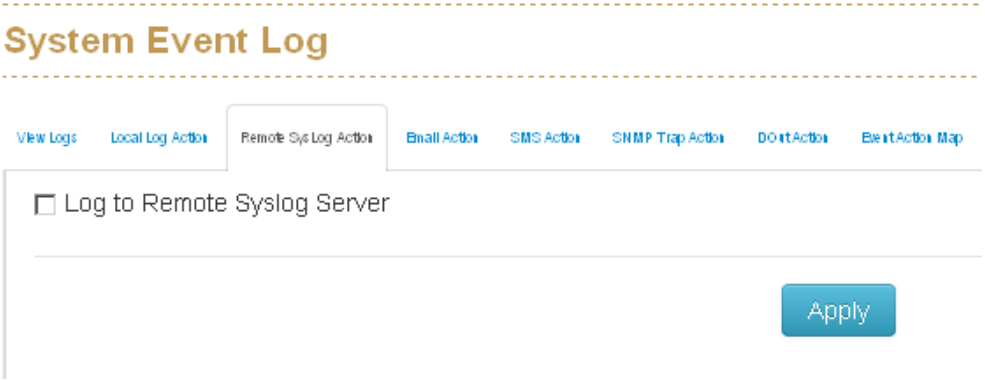
<3> Link Change: Link change.

<4> Power: Power conditions.



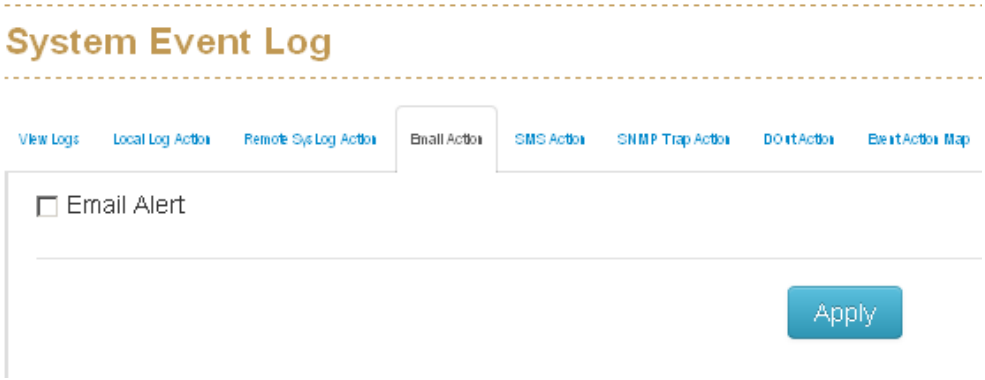
Local Log Action

Save to Local: Save log to local file



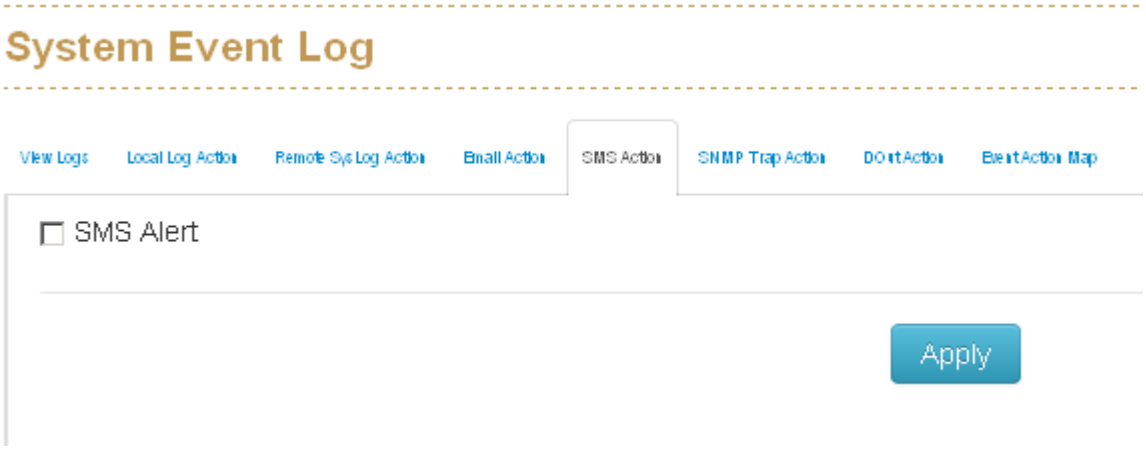
Remote Syslog Action

Log to Remote Syslog Server: Save log to Syslog Server



Email Action

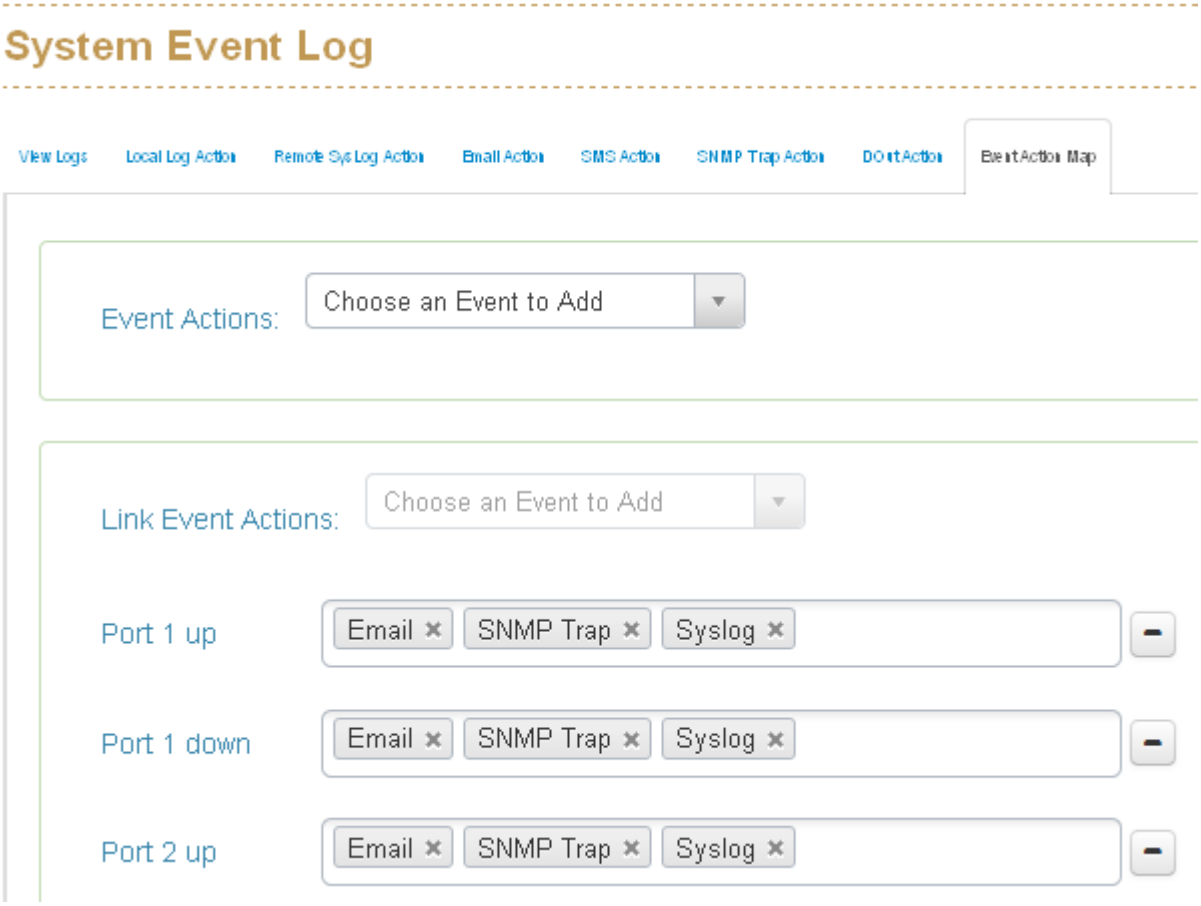
Email Alert: Sent log via Email



SMS Action

SMS Alert: Sent log via SMS service.

(The user must let the switch connect with internet and define the SMS server then the user can use this function)



Event Action Map

Event Actions

Select an Event to Add.

<0> Login: User Login.

<1> Boot: System Boot.

<2> Din1: Din Event 1 is triggered.

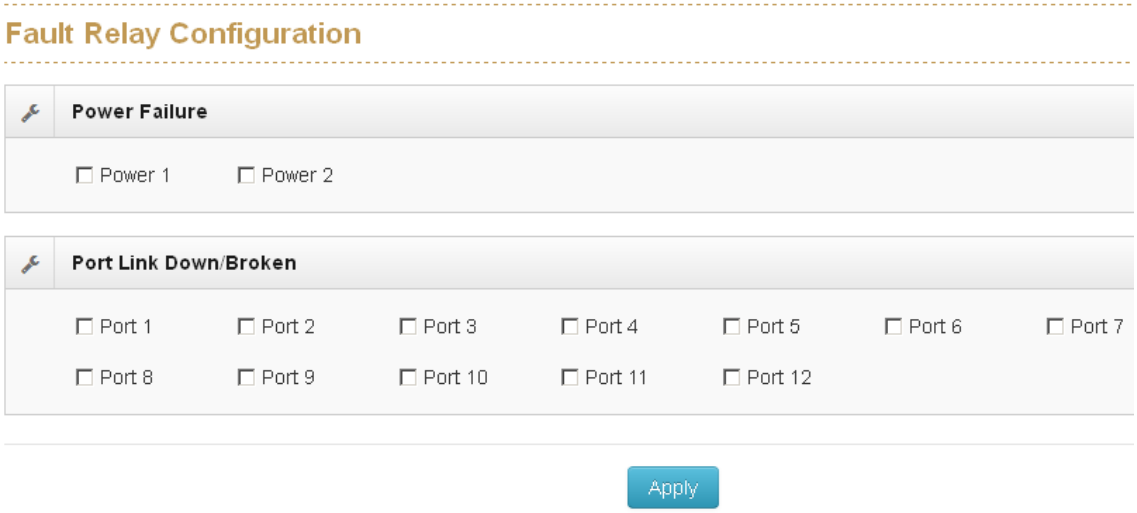
<3> Din2: Din Event 2 is triggered.

<4> Power1: Power 1 conditions.

<5> Power2: Power 2 conditions.

Link Event Actions

Select an Event to Add.



Fault Relay Configuration

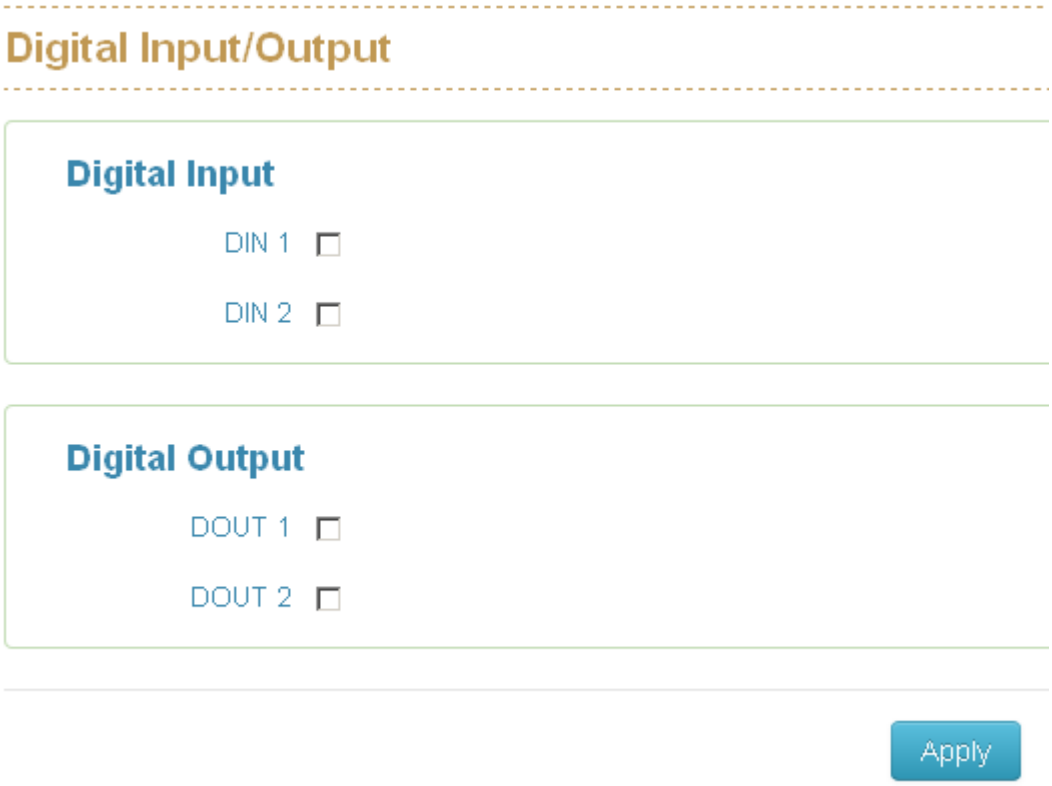
Configure Fault Relay on this page.

Power Failure:

Power: It's triggered when power failure.

Port Link Down/Broken

Port: It's triggered when port link down.



6.4.7 Digital Input / Output Configuration

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

Digital Input

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

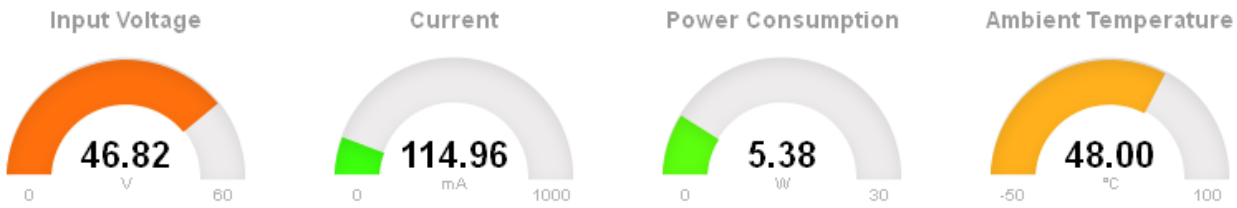
Low->High: Having focused this radio button, DI0/DI1 will only report the status when the external device's voltage changes from low to high.
High->Low: Having focused this radio button, DI0/DI1 will only report the status when the external device's voltage changes from high to low.
Event Description: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

Digital Output

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

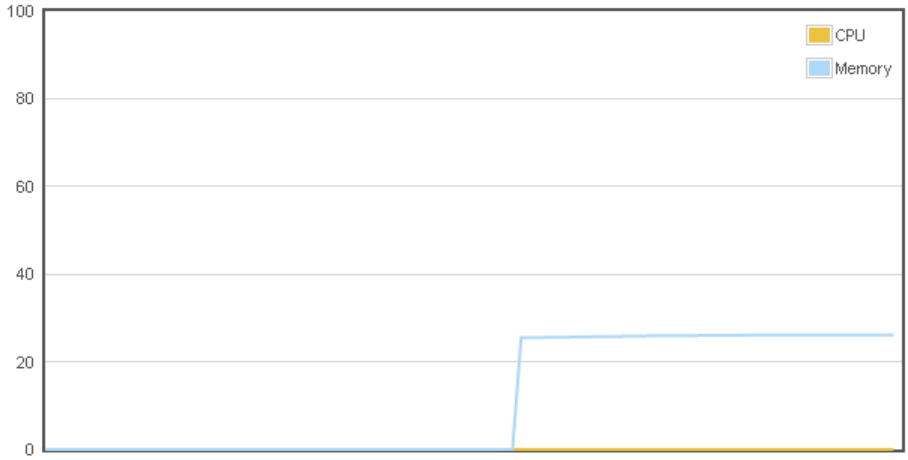
Action: Choose the output type of electrical signal.
Low->High: Having focused this radio button, DO0/DO1 will output an electrical signal of Low-to-High when the condition of the ticked checkbox is met (port/power failure occurs).
High->Low: Having focused this radio button, DO0/DO1 will output an electrical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

6.4.8 Environment Monitoring
Environment Monitoring
You can see the hardware status of switch in here.
Notice: This function was optional, if you are interesting about this, please contact the sales window.



System Utilization
You can see the using rate of switch CPU and memory.

System Utilization



6.5 Ports

Device Settings

NO	Description	Enabled	Flow Control	Speed
Port 1	#1	☑	☐	Auto
Port 2	#2	☑	☐	Auto
Port 3	#3	☑	☐	Auto
Port 4	#4	☑	☐	Auto
Port 5	#5	☑	☐	Auto

6.5.1 Port 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.

No:

This is the logical port number for this row.

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 speeds supported by the specific port is shown. Possible speeds are:

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.

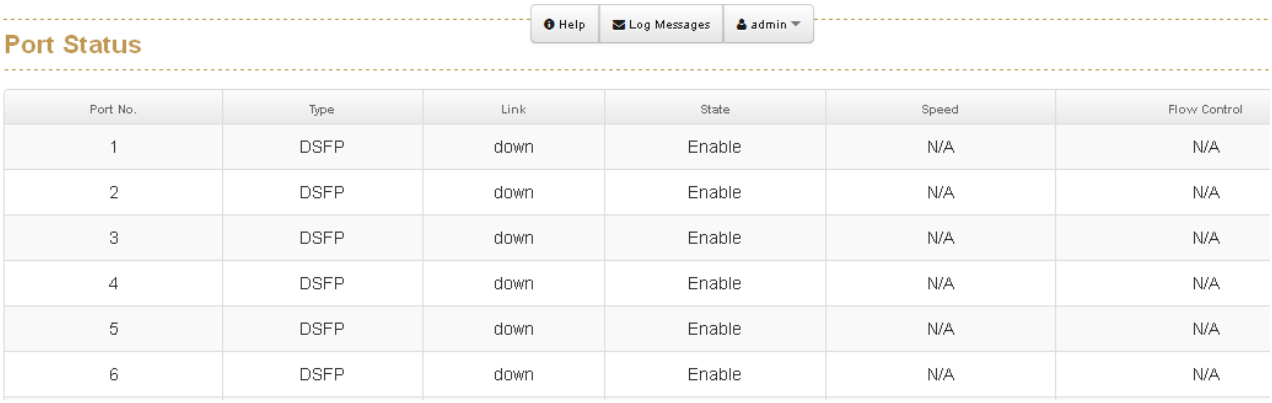
10Mbps HDX - Forces the cu port in 10Mbps half duplex mode.

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.



Port No.	Type	Link	State	Speed	Flow Control
1	DSFP	down	Enable	N/A	N/A
2	DSFP	down	Enable	N/A	N/A
3	DSFP	down	Enable	N/A	N/A
4	DSFP	down	Enable	N/A	N/A
5	DSFP	down	Enable	N/A	N/A
6	DSFP	down	Enable	N/A	N/A

6.5.2 Port Status

Port No:

This is the logical port number for this row.

Type:

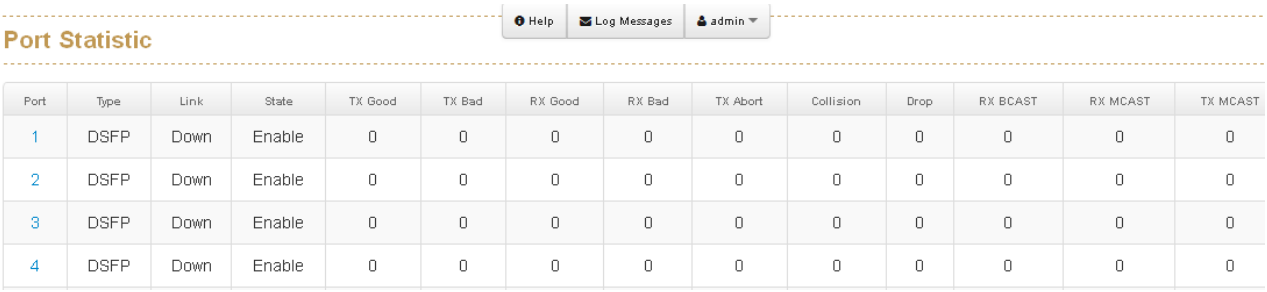
This is the logical port type.

Link Status:

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.



Port	Type	Link	State	TX Good	TX Bad	RX Good	RX Bad	TX Abort	Collision	Drop	RX BCAST	RX MCAST	TX MCAST
1	DSFP	Down	Enable	0	0	0	0	0	0	0	0	0	0
2	DSFP	Down	Enable	0	0	0	0	0	0	0	0	0	0
3	DSFP	Down	Enable	0	0	0	0	0	0	0	0	0	0
4	DSFP	Down	Enable	0	0	0	0	0	0	0	0	0	0

6.5.3 Port Statistics

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:

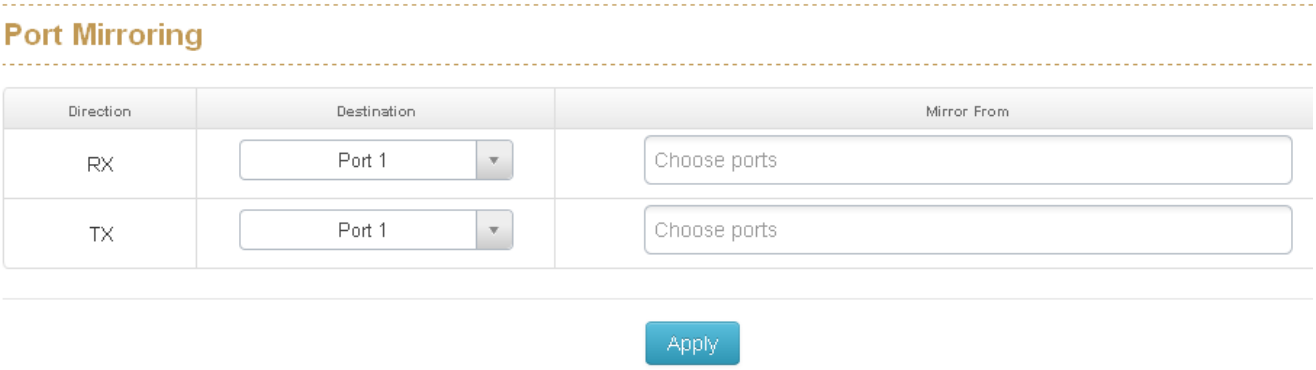
The counts of dropped packet.

Rx Bcast Packet:

The counts of broadcast packet.

Rx Mcast Packet:

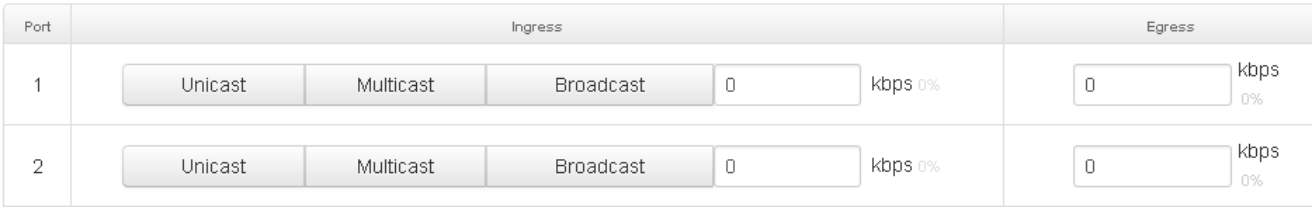
The counts of multicast packet.



6.5.4 Port 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.

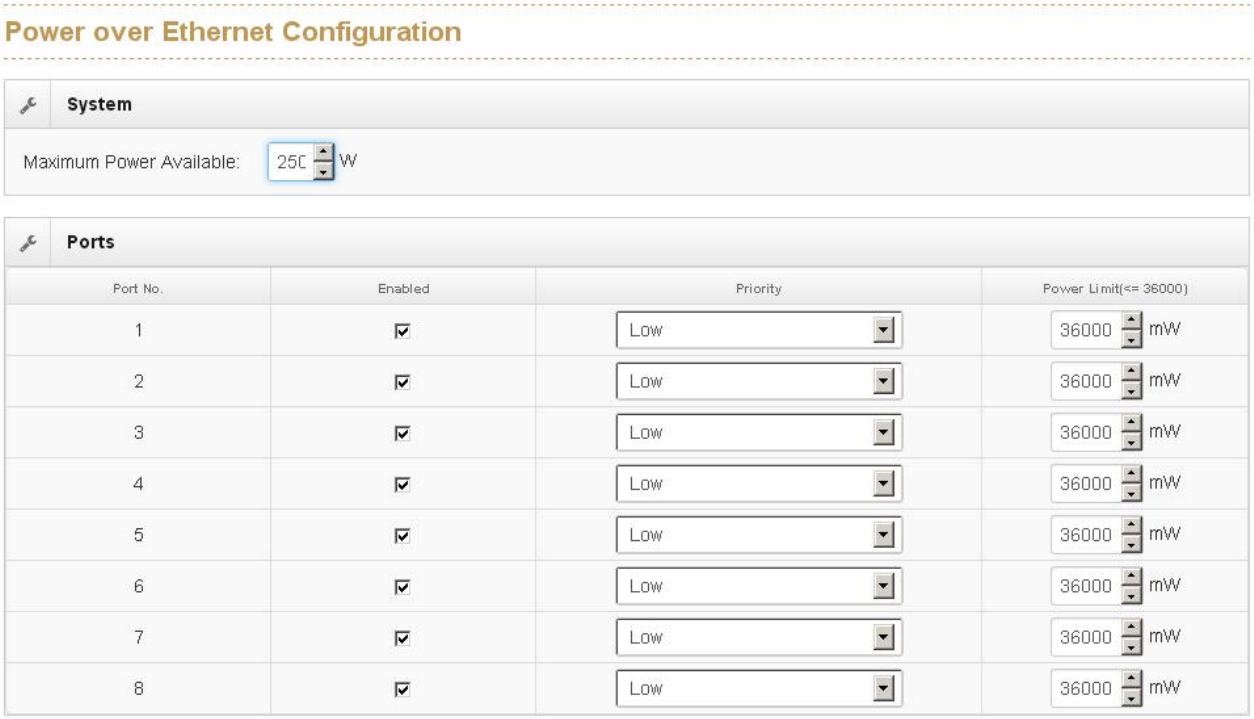


Port Rate Limiting

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.
Band Width: 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
Ingress: Enter the port effective ingress rate(The default value is "0").
Egress: Enter the port effective egress rate(The default value is "0").

6.6 Power over Ethernet



Maximum Power Available:

This function can limit the total power consumption, please don't over 250W.

Port No.

The number of each PoE port

Enable

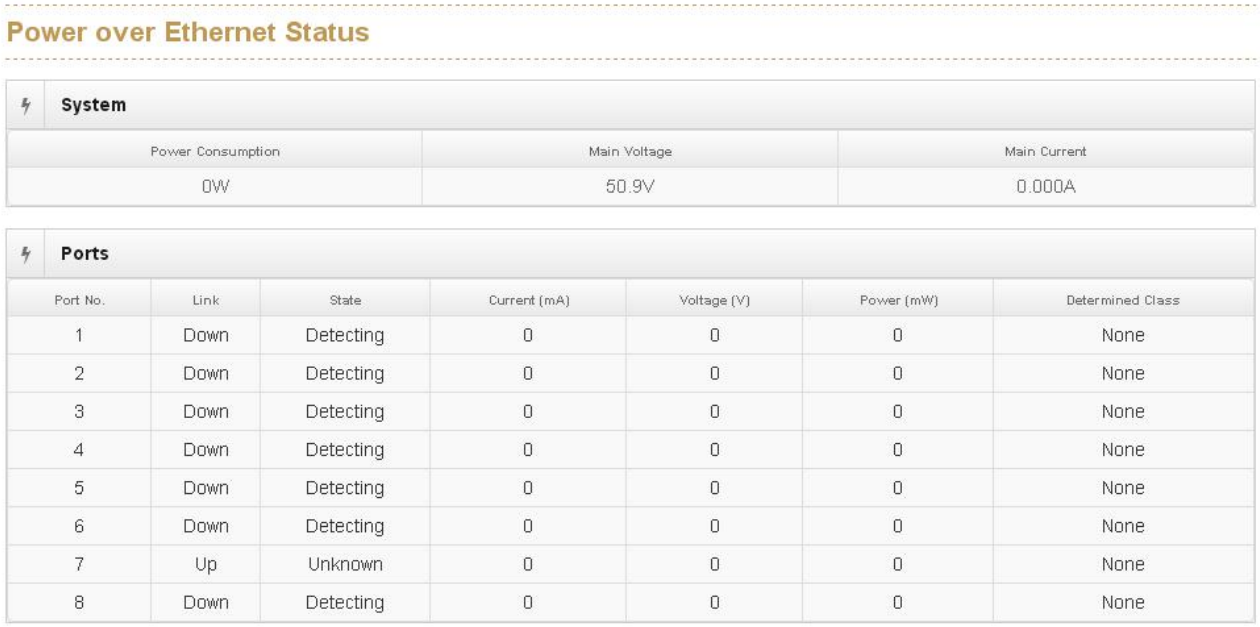
Enable/disable the PoE function of each PoE port

Priority

Set the priority of power supply, if the total power consumption of all PoE ports was over the value of maximum power available, the switch will offer the power to the high priority PoE port and stop to supply power to the low priority PoE port.

Power Limit

Set the Maximum power of each PoE port



Power Consumption:

Total power consumption of all PoE ports

Main Voltage:

The output voltage of each PoE port.

Main Current

The output current of each PoE port.

Port No.

The number of each PoE port.

Link

The connection status of each PoE port.

State

The PoE status of the ending device.(Unknown means the ending device was none-PD device)

Current

Output current of each PoE port

Voltage

Output Voltage of each PoE port

Power

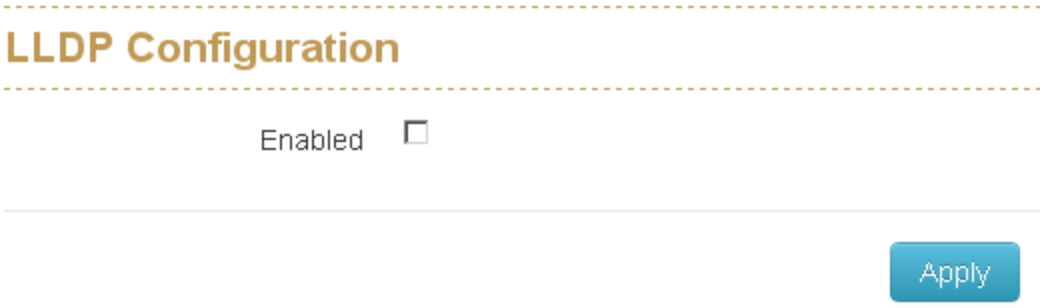
Power consumption of each PoE port

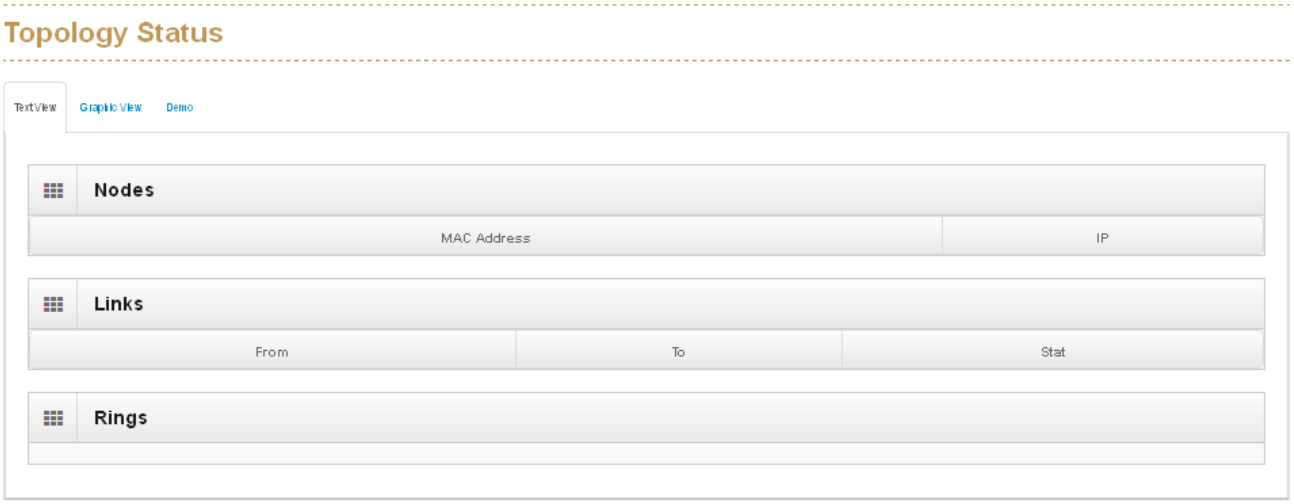
Detection Class

The PoE class of each PD device which connect with switch.

6.7 Topology

This function can help the user build the network topology drawing of field in switch, please remember to enable **LLDP** function before you using this application.

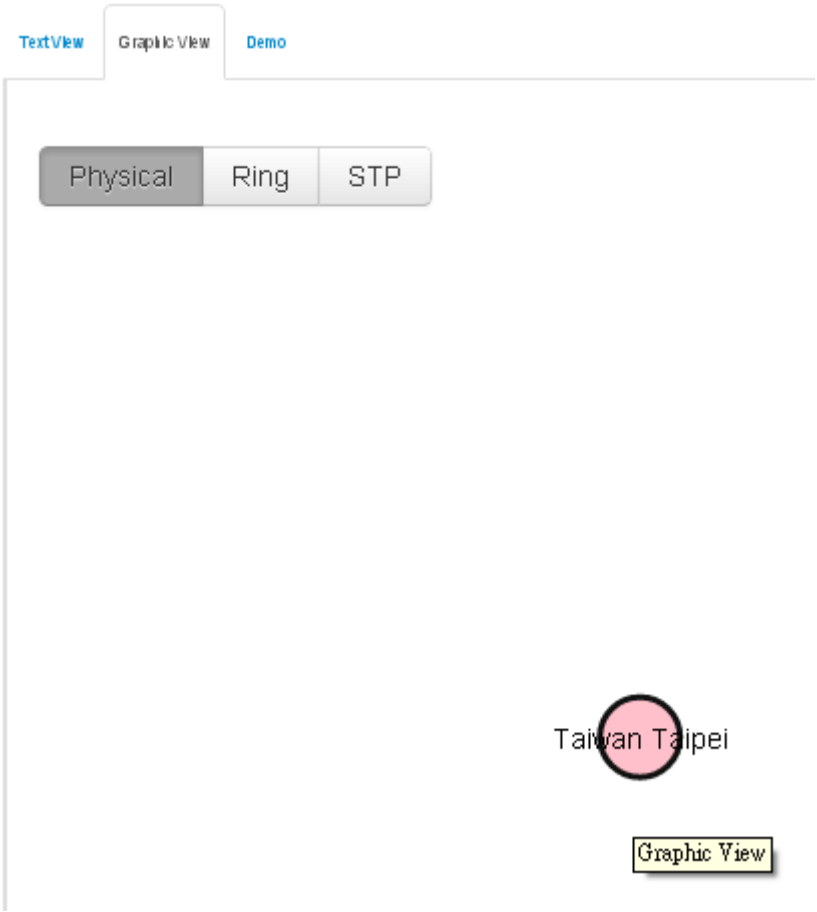




Topology Status

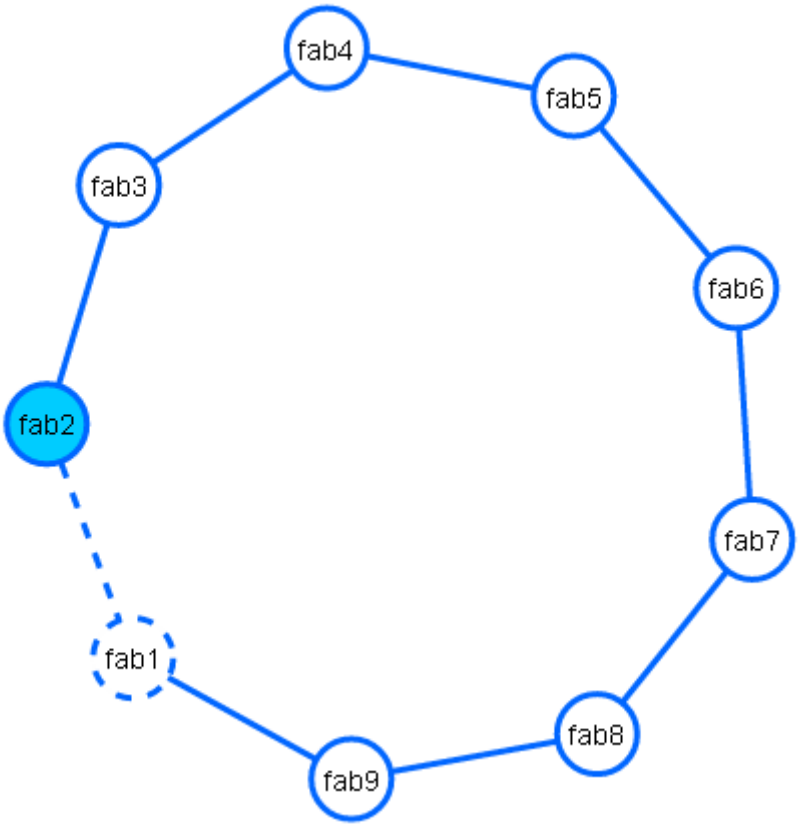
Text View: Display each switch in your network by text.

The Topology was build with the information from LLDP, this function can let you see the information of LLDP from other switches.



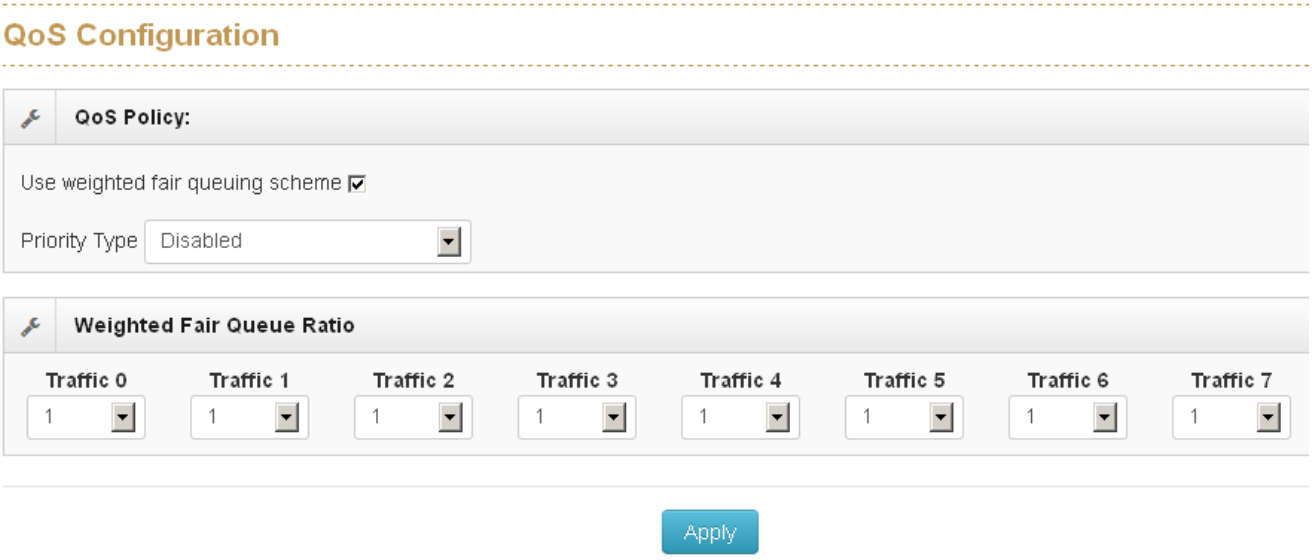
Graphic View: Display each switch in your network by graphic.

You can see the topology diagram which build by the LLDP information in here.



Demo: Demo display each topology in different application.

6.8 QoS



QoS Policy

Using the weight fair queue scheme

the switch will follow 1:1 rate to process priority queue from High to lowest queue.

Priority Type

Port-base: the port priority will follow the default port priority that you have assigned - High, center, low, or lowest. CoS only: the port priority will only follow the CoS priority that you have assigned. ToS only: the port priority will only follow the ToS priority that you have assigned. CoS first: the port priority will follow the CoS priority first, and then other priority rule. ToS first: the port priority will follow the ToS priority first, and the other priority rule

Port Base Priority

Port : it has 8 priority levels - 0~7

Cos

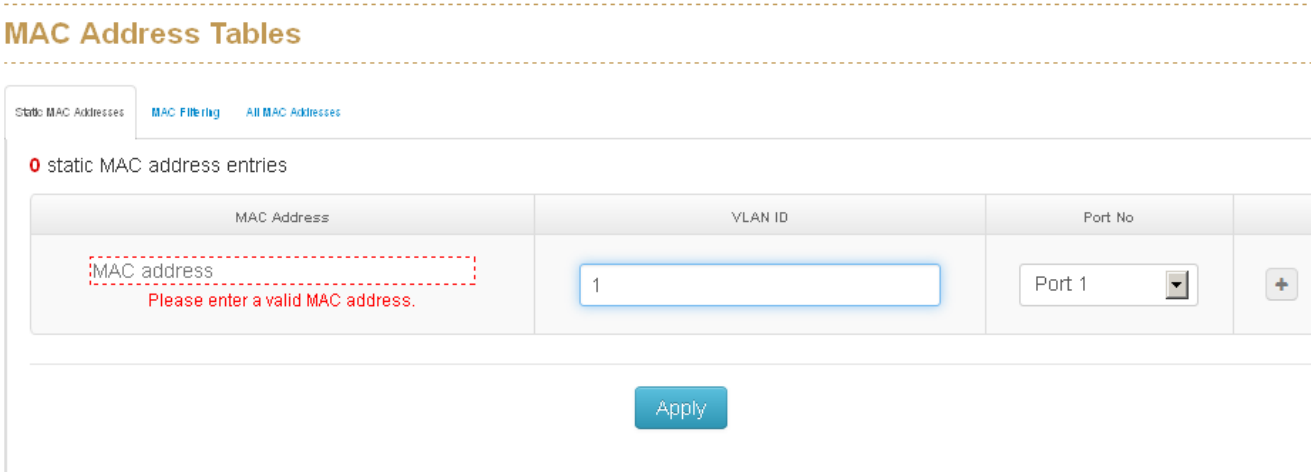
Set the CoS priority level 0~7.

Tos

ToS priority: the 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.

6.9 Security



6.9.1 MAC Address Tables

Use the MAC address table to ensure the port security.

Static MAC Address

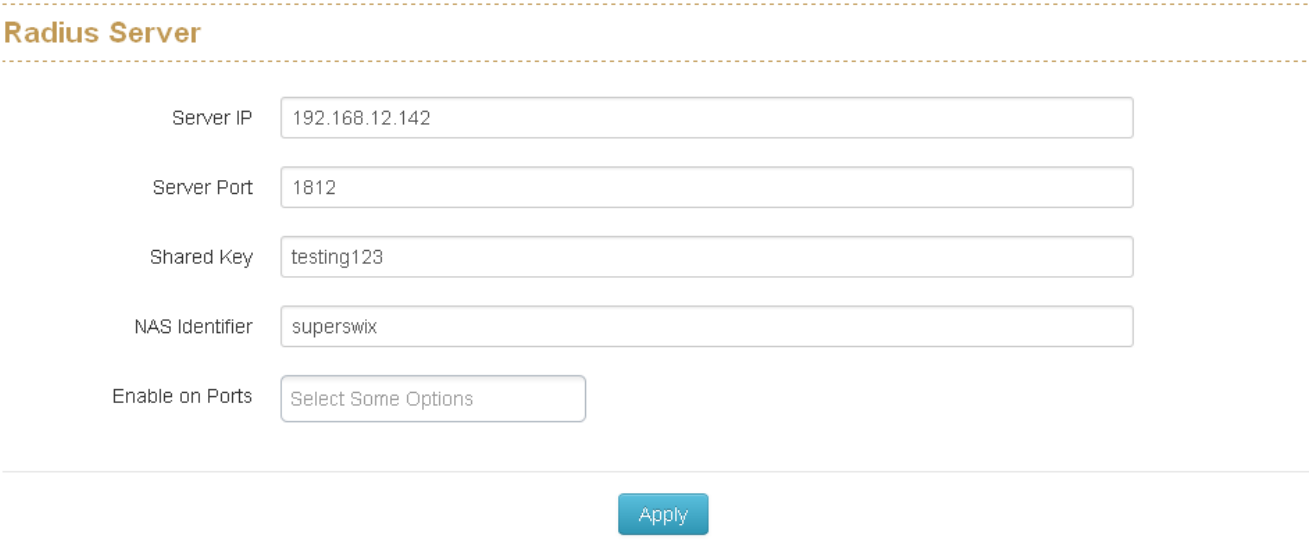
You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address. MAC Address: Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity. VLAN ID : Entering the VLAN ID. Port No : pull down the selection menu to select the port number.

MAC Filtering

By filtering MAC address, the switch can easily filter pre-configure MAC address and reduce the un-safety. You can add and delete filtering MAC address. MAC Address: Enter the MAC address that you want to filter.

All MAC Addresses

ou can view the port that connected device's MAC address and related device's MAC address.



6.9.2 Access Control List

You can use ACL feature to deny the access from the specified IP address or MAC address.

6.9.2.1 ACL with Layer2 (MAC)

No: The number of ACL record.

Port: assign the port which you want to enable the ACL function.

Direction: let the switch check the destination address or source address of packet.

Address: assign the MAC address which you want to deny.

Mask: set the mask to filter the MAC range.

No	Port	Direction	Address	Mask	Action
1	Port 1	Source	00:00:00:00:00:00	ff:ff:ff:fe:00:00	Deny

6.9.2.2 ACL with Layer3 (IP)

No: The number of ACL record.

Port: assign the port which you want to enable the ACL function.

Direction: let the switch check the destination address or source address of packet.

Address: assign the IP address which you want to deny.

Mask: set the mask to filter the IP range.

No	Port	Direction	Address	Mask	Action
1	Port 1	Source	192.168.16.1	255.255.255.0	Deny

6.9.3 IEEE 802.1X Radius Server

802.1X makes use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails. To enable 802.1X, you still to fill in the authentication server information.

Server IP

The ip address of the authentication server.

Server Port

The UDP port number used by the authentication server to authenticate.

Shared Key

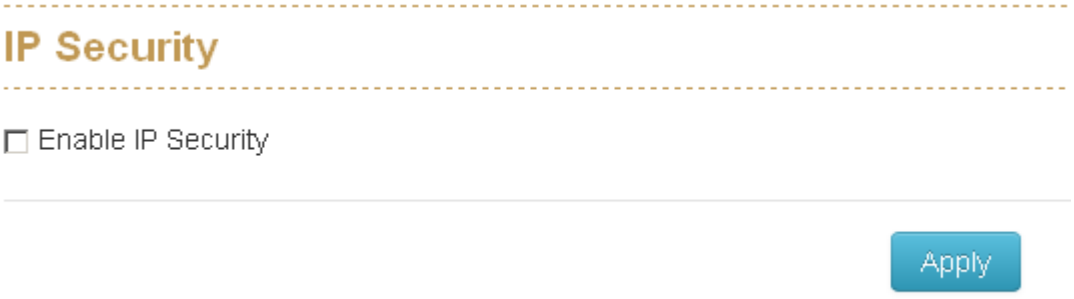
When this check box is checked, the IP addresses among IP permit list will be allowed to access via telnet service.

NAS Identifier

A string used to identify this switch.

Enable on Ports

You can select the specific port and configure the authorization state.



6.9.4 IP Security Help

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.

Enable IP Security

When this option is in Enable mode, the Enable Web Server and Enable Telnet Server and Enable SSH Server check boxes will then be available.

Enable Web Server

When this check box is checked, the IP addresses among IP permit list will be allowed to access via web service.

Enable Telnet Server

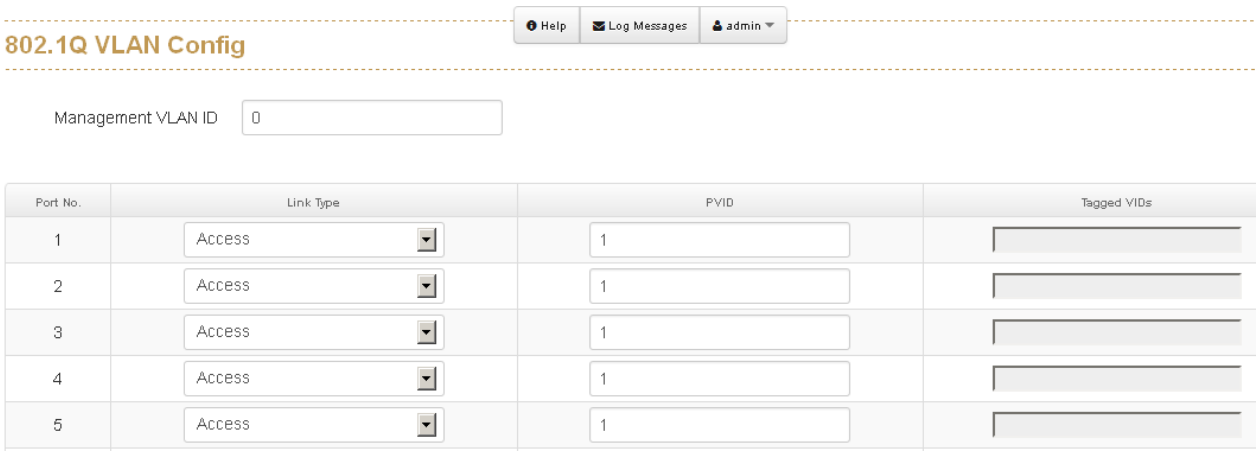
When this check box is checked, the IP addresses among IP permit list will be allowed to access via telnet service.

Enable SSH Server

When this check box is checked, the IP addresses among IP permit list will be allowed to access via ssh service.

IP permit list

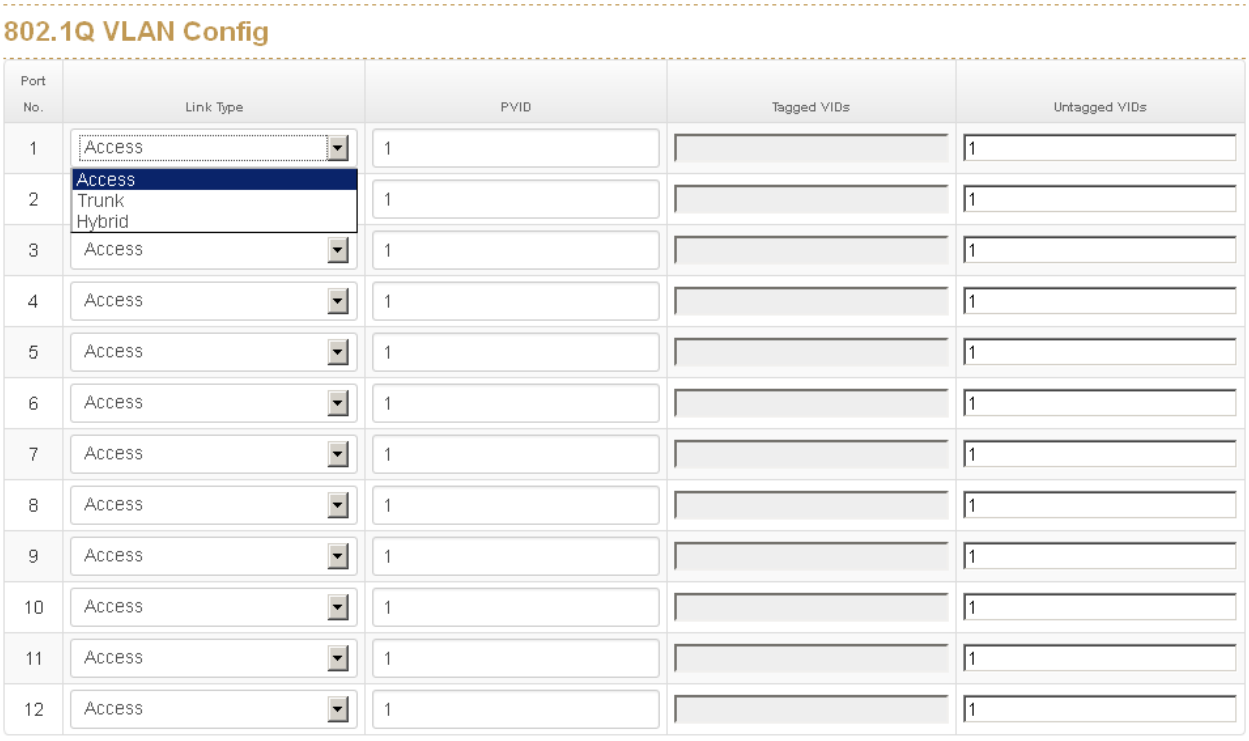
Assign up to 20 specific IP address. Only these 10 IP address can access and manage the switch through the Web browser



6.10.VLAN

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

802.1Q VLAN Config



Link Type: There are 3 types of link type.

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

Note: Because the access port doesn't have an understanding of tagged frame, the column field of Tagged VID is not available.

2. Trunk Link: A segment which provides the link path for one or more VLAN-aware devices (switches). A Trunk Port, connected to the trunk link, has an understanding of tagged frame, which is used for the communication among VLANs across switches. Which frames of the specified VIDs will be forwarded depends on the values filled in the Tagged VID column field. Please insert a comma between two VIDs.

Note:

A trunk port doesn't insert tag into an untagged frame, and therefore the untagged VID column field is not available.

It's not necessary to type '1' in the tagged VID. The trunk port will forward the frames of VLAN 1.

The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.

3. Hybrid Link: A segment which consists of Access and Trunk links. The hybrid port has both the features of access and trunk ports. A hybrid port has a PVID belonging to a particular VLAN, and it also forwards the specified tagged-frames for the purpose of VLAN communication across switches.

PVID

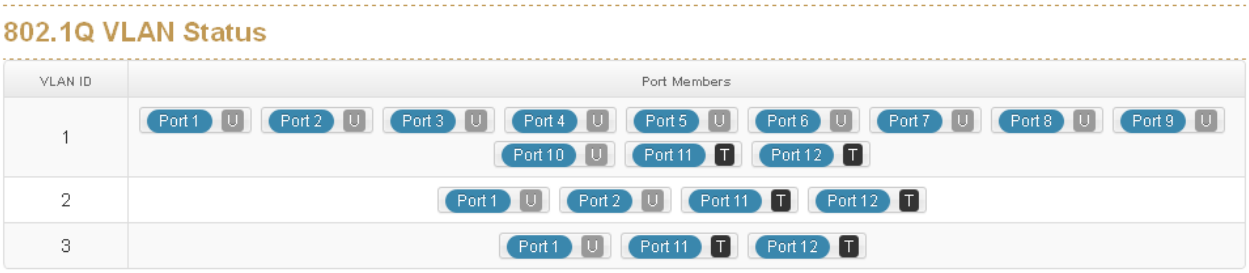
Indicates the VLAN ID of this particular VLAN.

Tagged VID:

This column field is available when Link Type is set as Trunk Link and Hybrid Link. Assign a number in the range between 1 an 4094.

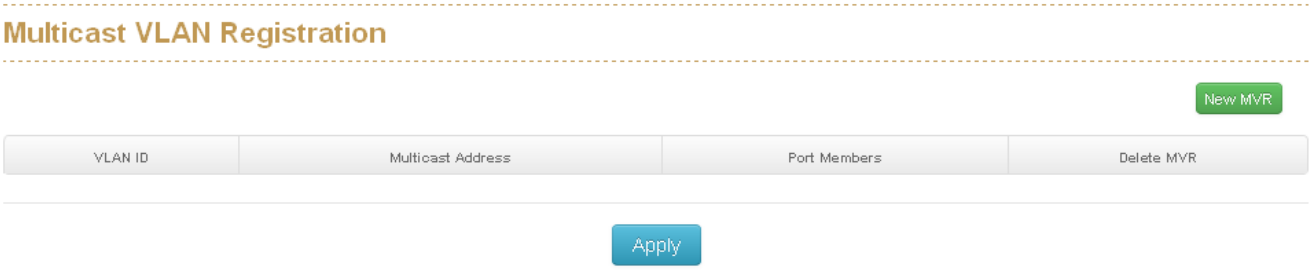
Untagged VID:

This function was designed for extend VLAN application, don't change it !!



802.1Q VLAN Status

You can see the status of each VLAN group in here.



6.11.MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

VLAN ID

Specify the Multicast VLAN ID.

Multicast Addresses

Multicast Addresses of the group displayed.

Port Members

Ports under this group.

6.12.LLDP

6.12.1 LLDP Configuration

Enabled

Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbours.

Tx Interval

The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds.

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

Port No

The switch port number of the logical LLDP port.

Port Id

Enter characters to be id name for the logical LLDP port.

Mode

Select LLDP mode.

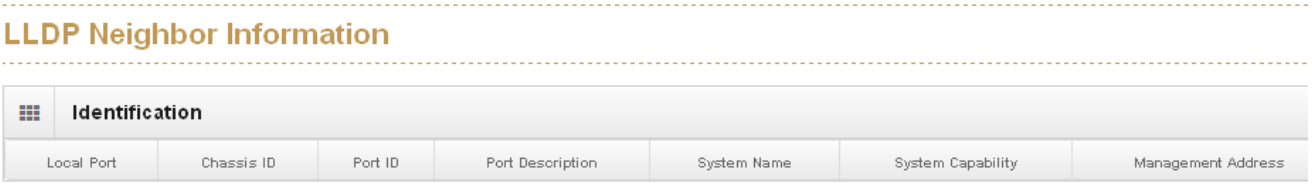
Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.

Tx only The switch will drop LLDP information received from neighbors, but will send out **LLDP information.**

Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors.

Both The switch will send out LLDP information, and will analyze LLDP information

received from neighbors.



6.12.2. LLDP Neighbor

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:

Local Port

The port on which the LLDP frame was received.

Chassis ID

The **Chassis ID** is the identification of the neighbor's LLDP frames.

Remote Port ID

The **Remote Port ID** is the identification of the neighbor port.

Port Description

Port Description is the port description advertised by the neighbor unit.

System Name

System Name is the name advertised by the neighbour unit.

System Capabilities

System Capabilities describes the neighbour unit's capabilities. The possible capabilities are:

1. Other

2. Repeater

3. Bridge

4. WLAN Access Point

5. Router

6. Telephone

7. DOCSIS cable device

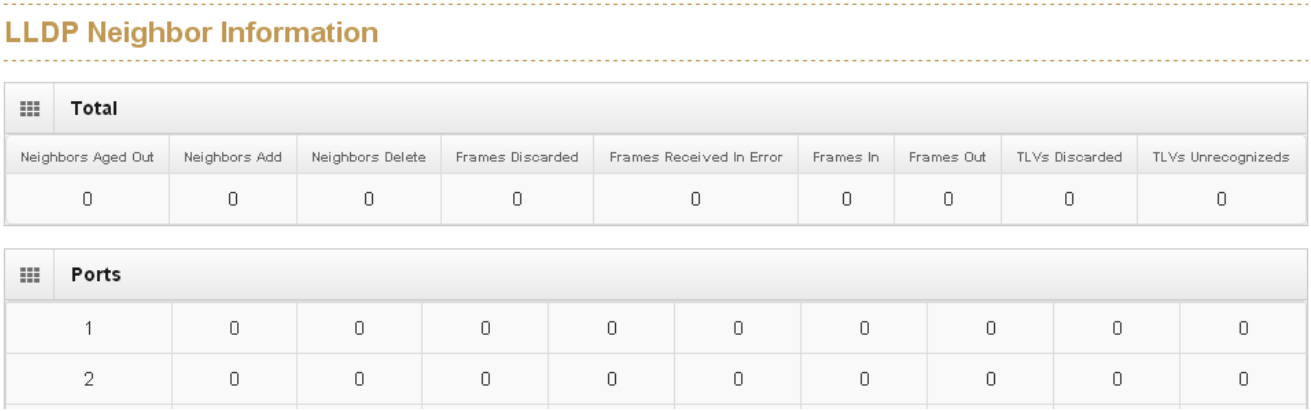
8. Station only

9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

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.



6.12.3. LLDP Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. **Total** are counters that refer to the whole stack, switch, while **Port** refer to per port counters for the currently selected switch.

Total

Neighbours Aged Out

Shows the number of entries deleted due to Time-To-Live expiring.

Neighbours Added

Shows the number of new entries added since switch reboot.

Neighbours Deleted

Shows the number of new entries deleted since switch reboot.

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 discarded. This situation is known as "Too Many Neighbours" 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.

Frames Received In Error

The number of received LLDP frames containing some kind of error.

Frames In

The number of LLDP frames received on the port.

Frames Out

The number of LLDP frames transmitted on the port.

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.

TLVs Unrecognized

The number of well-formed TLVs, but with an unknown type value.

Ports

The displayed table contains a row for each port. The columns hold the following information:

Port

The port on which LLDP frames are received or transmitted.

Neighbors Aged Out

Shows the number of entries deleted due to Time-To-Live expiring.

Neighbors Added

Shows the number of new entries added since switch reboot.

Neighbors Deleted

Shows the number of new entries deleted since switch reboot.

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 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.

Frames Received In Error

The number of received LLDP frames containing some kind of error.

Frames In

The number of LLDP frames received on the port.

Frames Out

The number of LLDP frames transmitted on the port.

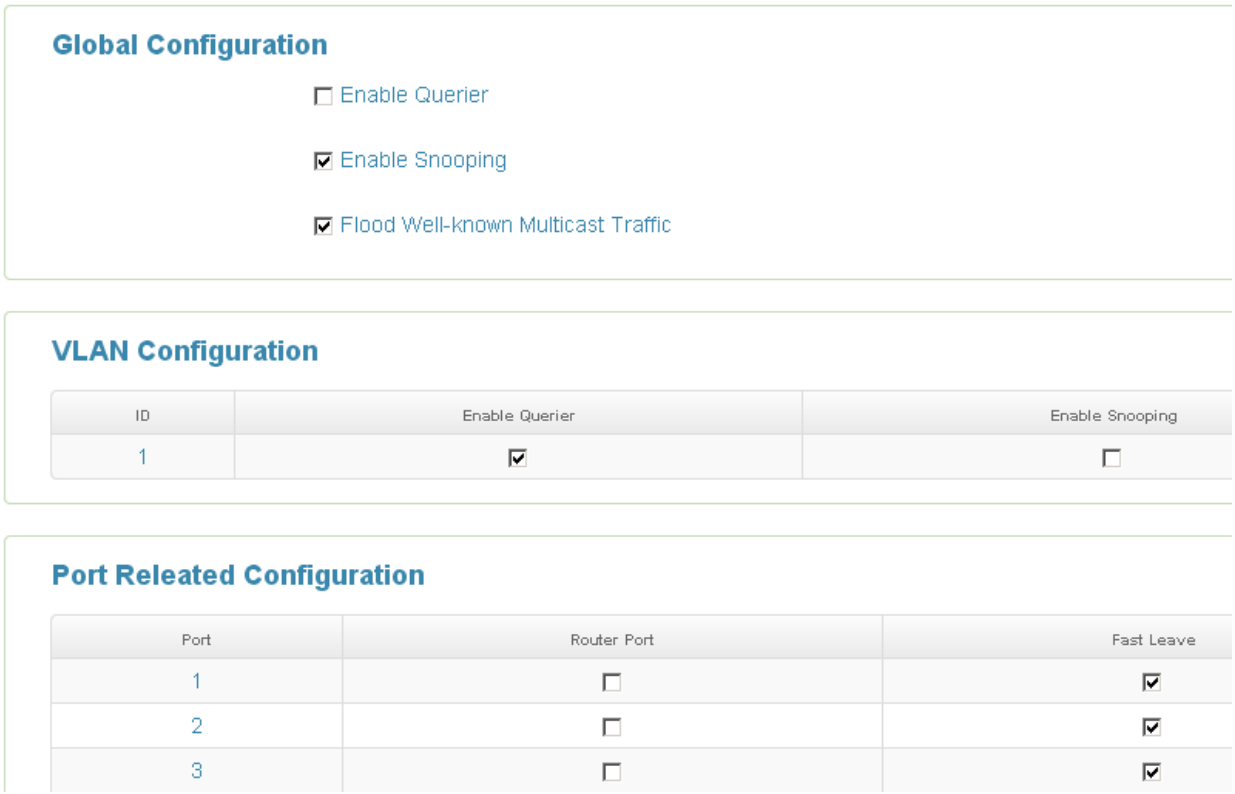
TLVs Discarded

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.

TLVs Unrecognized

The number of well-formed TLVs, but with an unknown type value.

IGMP Snooping Configuration



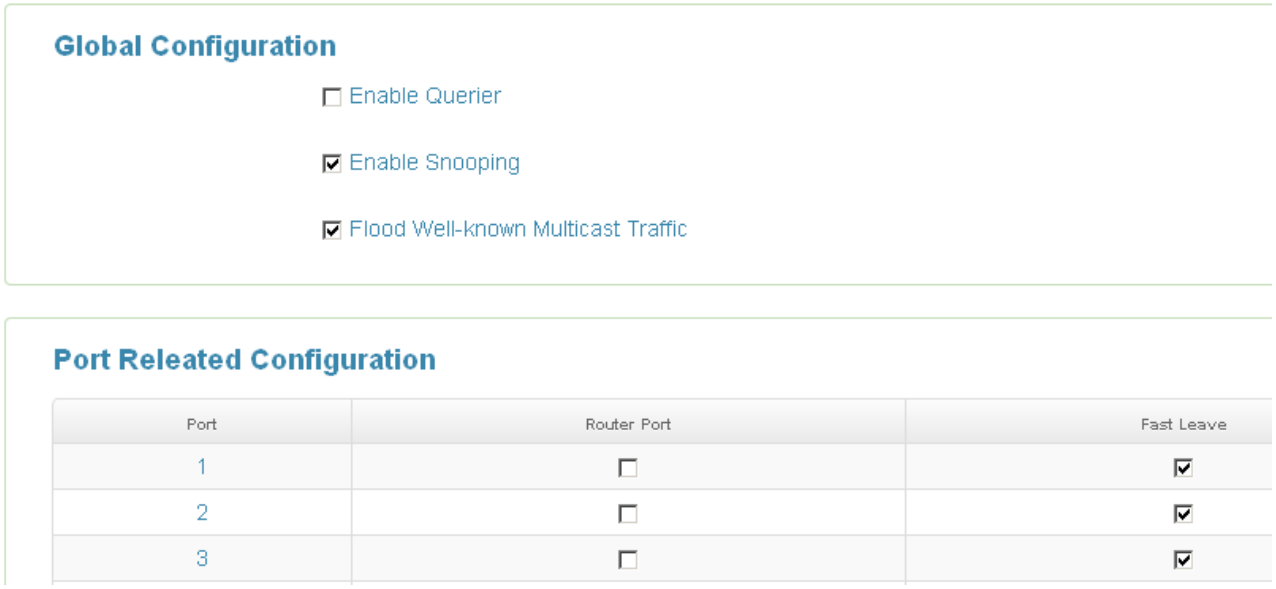
6.13 IGMP Snooping

This page provides IGMP Snooping related configuration.

Notice1: if the IP-CAM use Multicast format to transfer video stream, make sure there is at least one switch has enabled IGMP Querier function and all switches have enabled IGMP snooping function in field.

Notice2: make sure the IGMP querier switch was in root side of your network, if not, please set IGMP router port to let switch know which uplink connection was dedicate to the path to the IGMP querior switch.

6.13.1 IGMP Snooping Configuration



Global Configuration

Enabled Querier

Enable the Global IGMP Querier.

Enabled Snooping

Enable the Global IGMP Snooping.

Flood Well-known Multicast Traffic

Make sure you want to let the Multicast stream flooding all ports of switch.

Port Related Configuration

Port

The switch port number of the logical port.

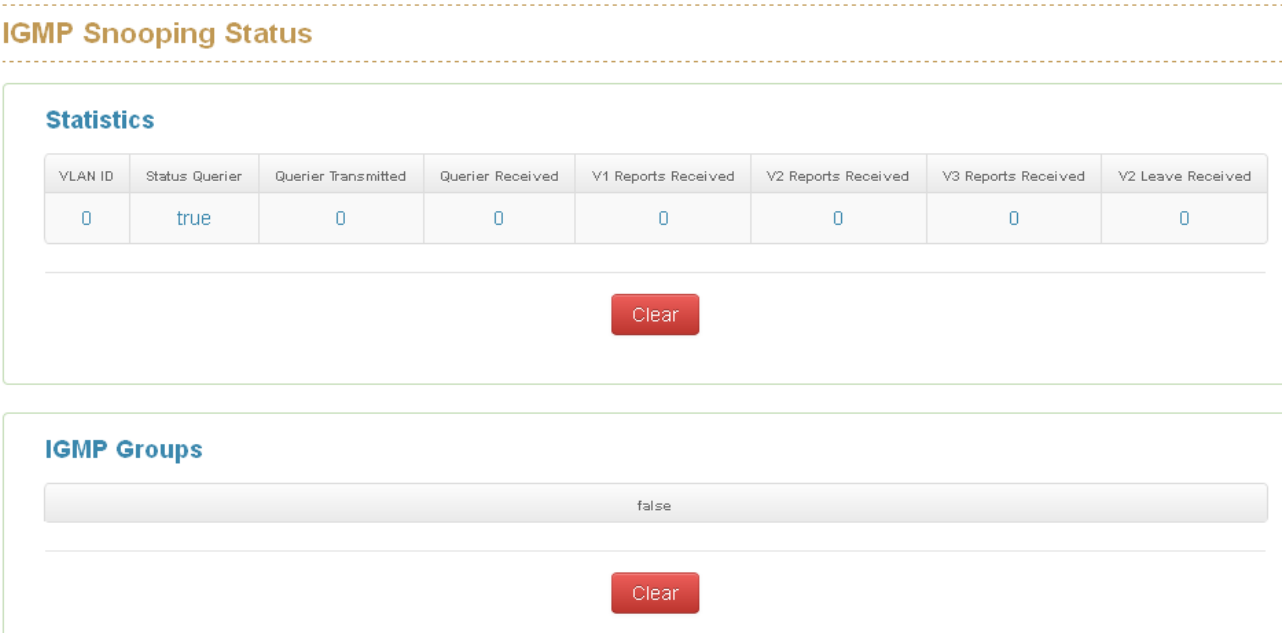
Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.



6.13.2 IGMP Snooping Status

This page provides IGMP Snooping status.

The status related to the currently selected stack unit, as reflected by the page header.

Statistics

VLAN ID

The VLAN ID of the entry.

Status Querier

Shows the Querier status is "ACTIVE" or "IDLE".

"DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V3 Reports Received

The number of Received V3 Reports.

V2 Leaves Received

The number of Received V2 Leaves.

IGMP Groups

Entries in the IGMP Group Table are shown on this page.

VLAN ID

VLAN ID of the group.

Multicast Addresses

Group address of the group displayed.

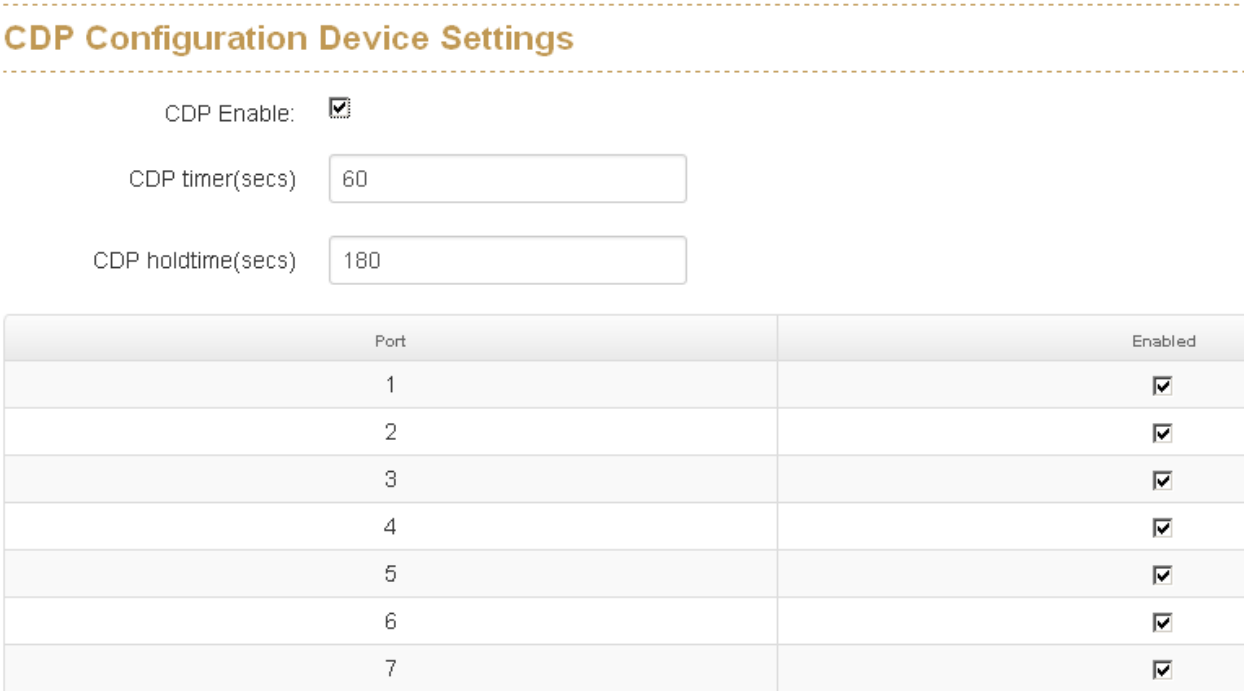
Port Members

Ports under this group.

Membership Interval

The group hold aging out TTL

6.14 CDP



6.14.1 CDP Configuration Device Settings

CDP Enabled

Enabled The switch will send out CDP information, and will analyze CDP information received from neighbors.

Tx Interval(secs)

The switch periodically transmits CDP frames to its neighbours for having the network discovery information up-to-date. The interval between each CDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds.

Tx Holdtime(secs)

Each CDP frame contains information about how long the information in the CDP frame shall be considered valid. The holdtime between each CDP frame is determined by the **Tx Holdtime** value. Valid values are restricted to 5 - 32768 seconds.

CDP Port Configuration

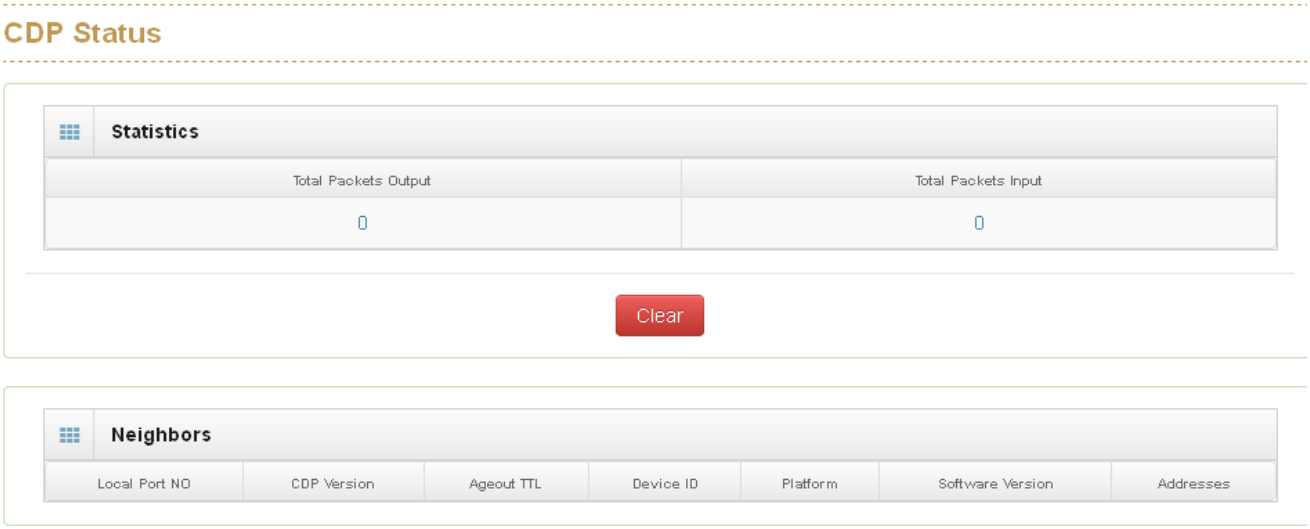
The CDP port settings relate to the currently selected stack unit, as reflected by the page header.

Port

The switch port number of the logical CDP port.

Enabled

The switch will send out CDP information, and will analyze CDP information received from neighbors.



6.14.2. CDP Status

Statistics

Total Packets Output

The number of CDP frames transmitted on the switch.

Total Packets Input

The number of CDP frames received on the switch.

Neighbors

The displayed table contains a row for each port on which an CDP neighbour is

detected. The columns hold the following information:

Local Port

The port on which the CDP frame was received.

Version

Version is the CDP version advertised by the neighbor unit.

Ageout TTL

Ageout TTL is the ageout Time-To-Live advertised by the neighbor unit.

Device ID

The Device ID is the identification of the neighbor's CDP frames.

Platform

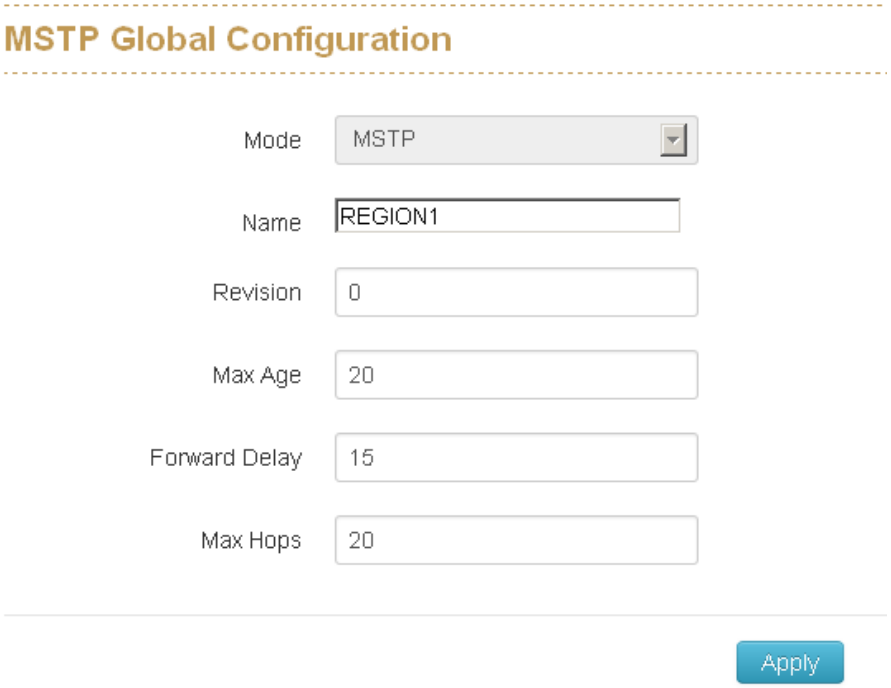
Platform is the description advertised by the neighbor unit.

Software Version

Software Version is the software version advertised by the neighbor unit.

Addresses

Addresses is the neighbour 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.



6.14 MSTP

6.14.1. MSTP Global Configuration

Mode

You can choose STP or RSTP or MSTP redundancy protocol in here.

Name

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Revision

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

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.

Max Age

The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

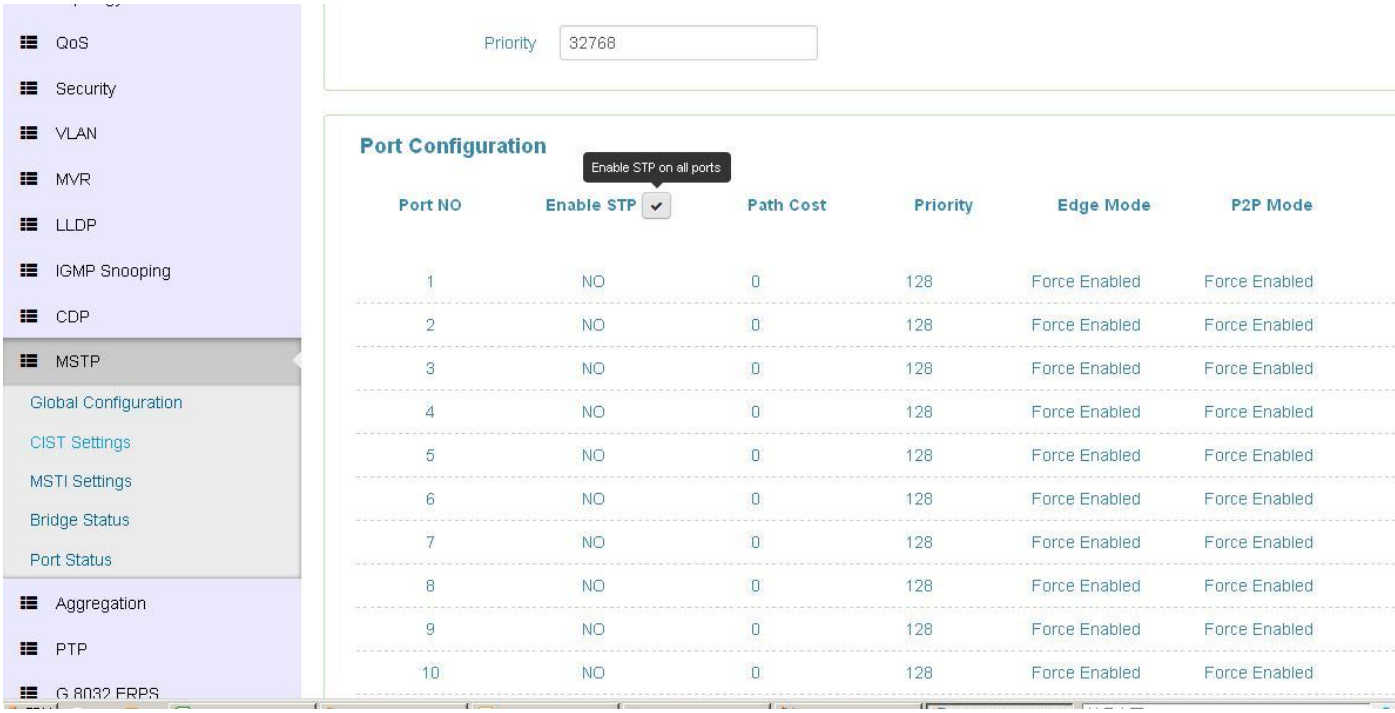
Maximum Hop Count

This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

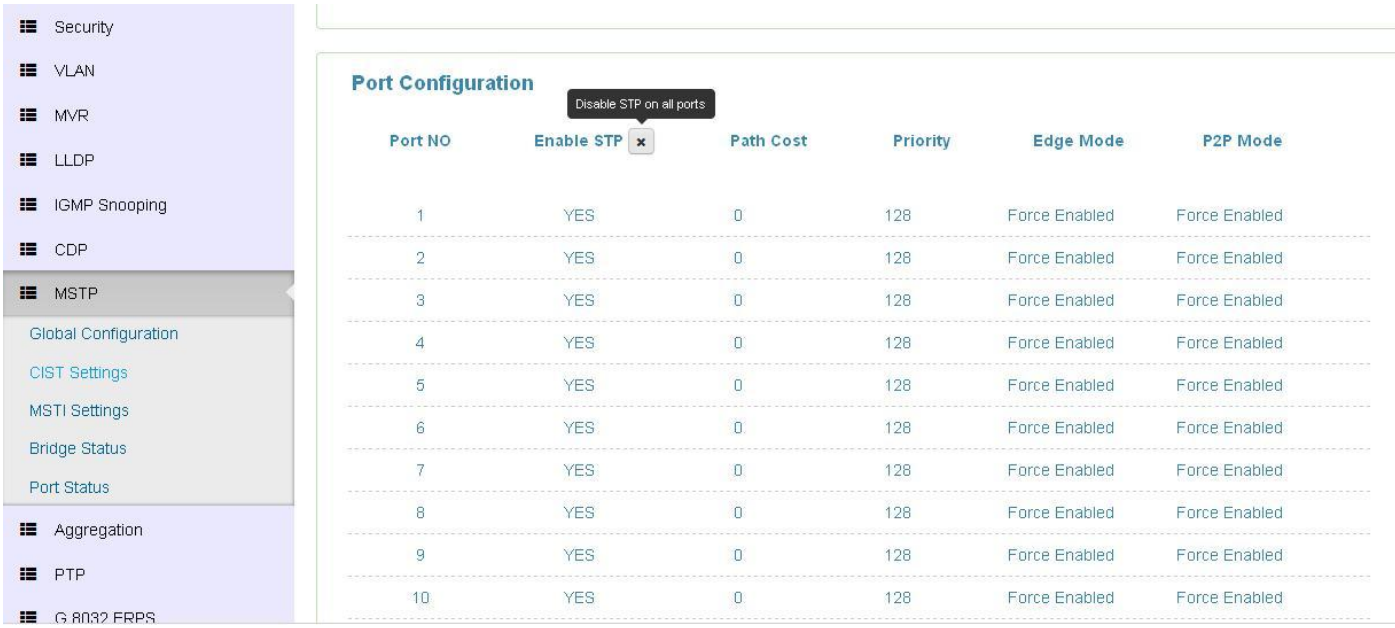
How to enable MSTP

6.14.1.1 Enter MSTP→ CIST Settings , press icon to enable MSTP

PS: (The default was disable with all ports)

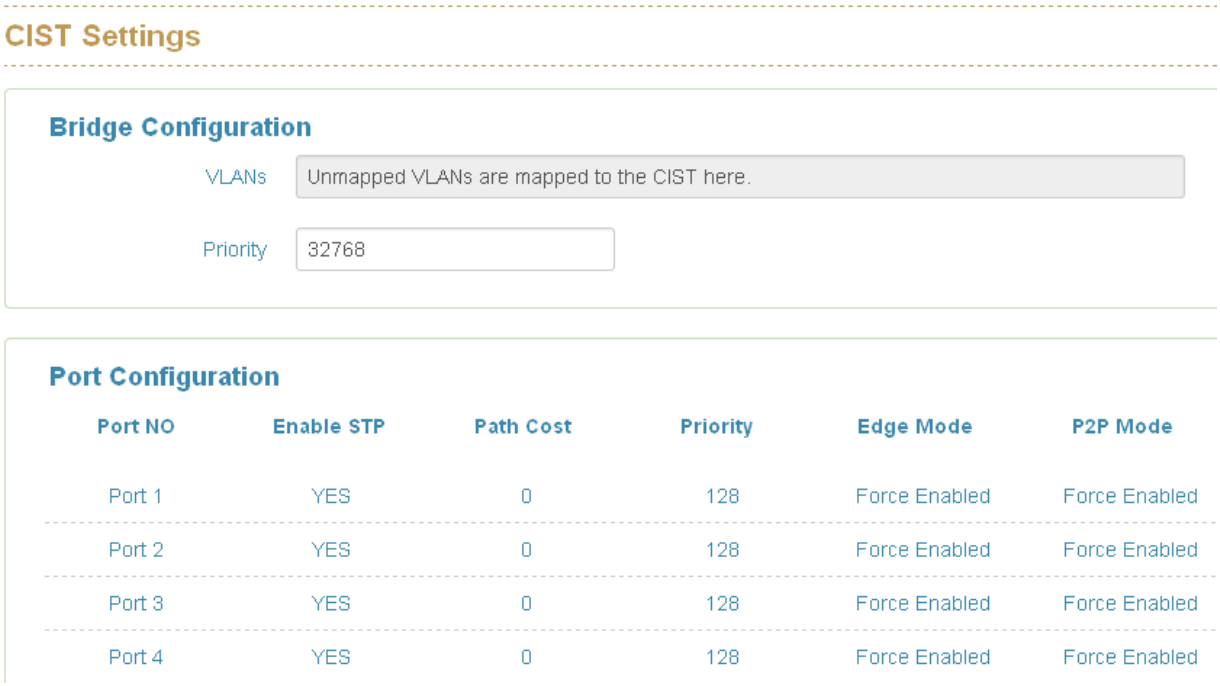


6.14.1.2 Check the status of STP, all ports should display “Yes”



6.14.1.3 Remember to press “Apply”

6.14.1.4 Save setting



6.14.2 CIST Settings

Bridge configuration

VLANs Mapped

The list of VLANs mapped to the MSTI. The VLANs must be separated with comma

and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)
Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Bridge 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.

Port

Port No

The switch port number of the logical STP port.

Enabled STP

Controls whether STP is enabled on this switch port.

Path Cost

Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority

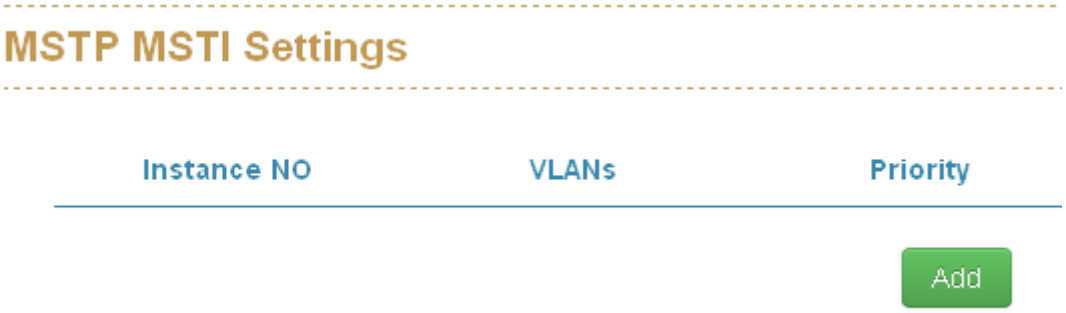
Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

edge_mode

Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized). Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

p2p_mode

description: Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.



6.14.3. MSTP MSTI Settings

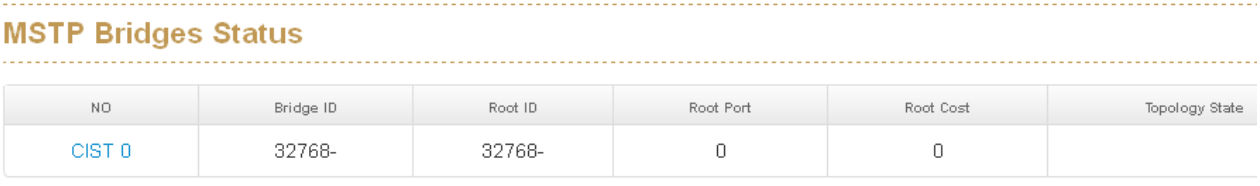
Instance No

VLANs

The list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Unmapped VLANs are mapped to the CIST. (The default bridge instance).

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.



6.14.4. MSTP Bridges Status

Instance

The Bridge Instance. ex: CIST, MSTI1, ...

Bridge ID

The Bridge ID of this Bridge instance.

Root ID

The Bridge ID of the currently elected root bridge.

Root Port

The switch port currently assigned the root port role.

Root Cost

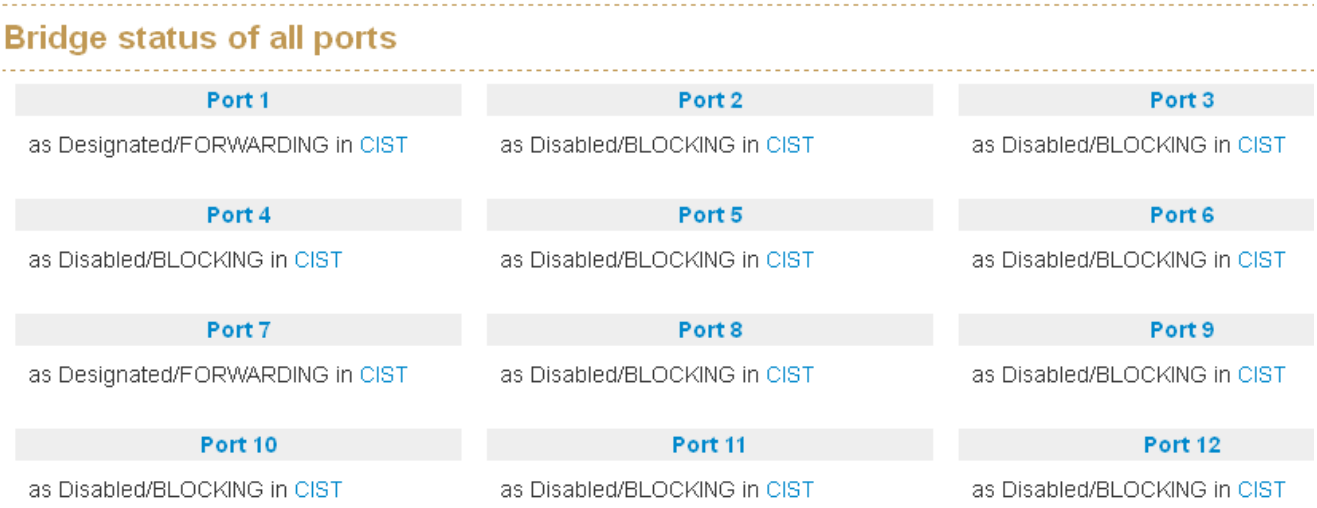
Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology State

The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last

The time since last Topology Change occurred.



6.14.5. Bridge status of all ports

Port

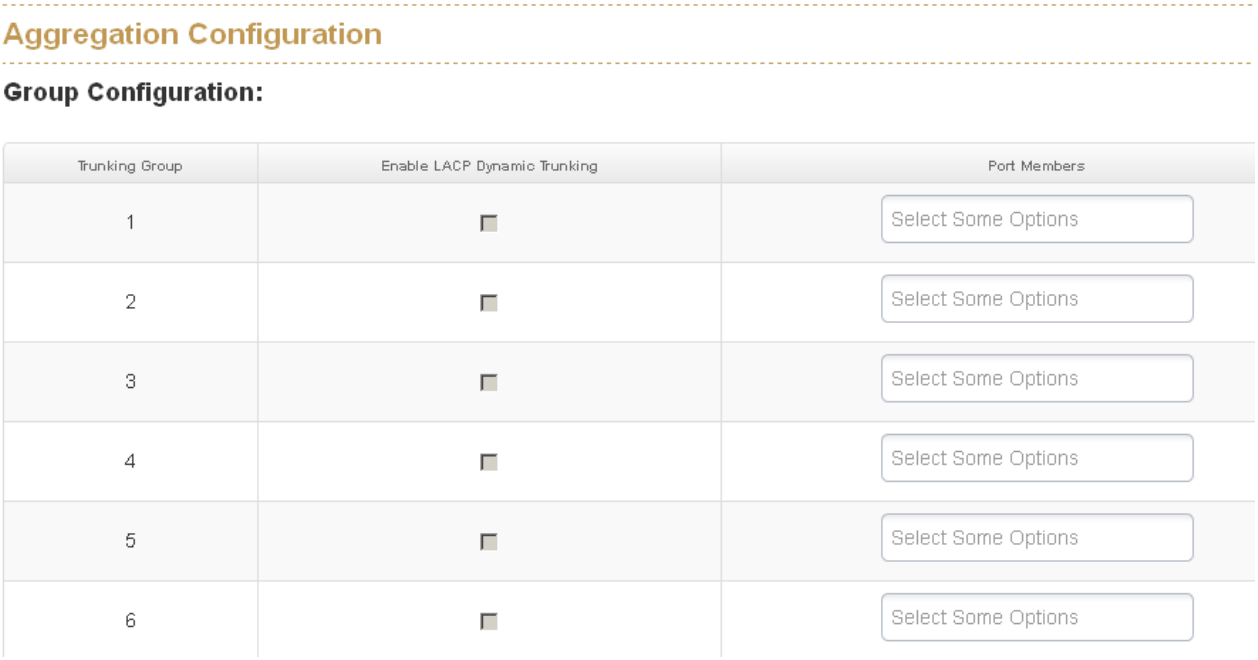
The switch port number of the logical STP port.

Role

The current STP port role of the port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort Disabled.

State

The current STP port state of the port. The port state can be one of the following values: Discarding Learning Forwarding.



6.15 Aggregation

6.15.1. Aggregation Configuration

Group Configuration

Trunking Group

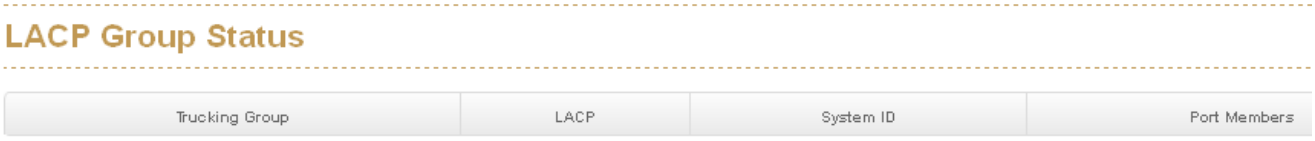
Number of trunking group

Enable LACP Dynamic Trunking:

Enable Trunking function

Port Members

Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.



6.15.2 LACP Port Status

Trunking Group

Number of trunking group

LACP

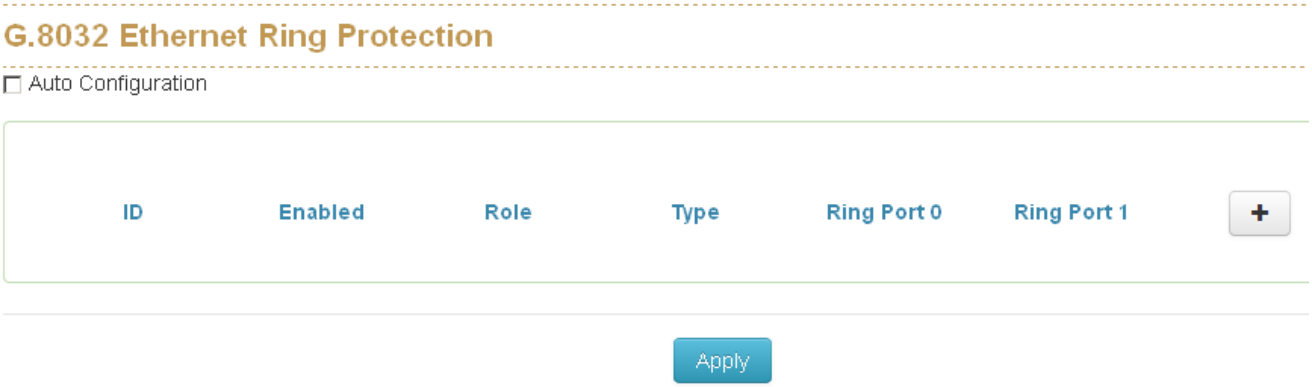
'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.

System ID

The ID of each Trunking group

Port Members

Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.



6.16 PTP

Enable on:

Select which port you want to enable PTP function.

Domain:

Set the PTP domain

Priority1:

Specify the **priority1** value to override the default criteria (clock quality, clock class, etc.) for best master clock selection. Lower values take precedence.The range for both is from 0 to 255., The default is 255

Priority2:

Specify a **priority2** value to be used as a tie-breaker between two devices that are otherwise equally matched in the default criteria. For example, you can use priority2 value to give a specific switch priority over other identical switches. The range for both is from 0 to 255. The default is 255.

Announce Interval:

Specify the time for sending announce messages. The range is 0 to 4 seconds. The default is 1 (2 seconds).

Announce Interval Timeout:

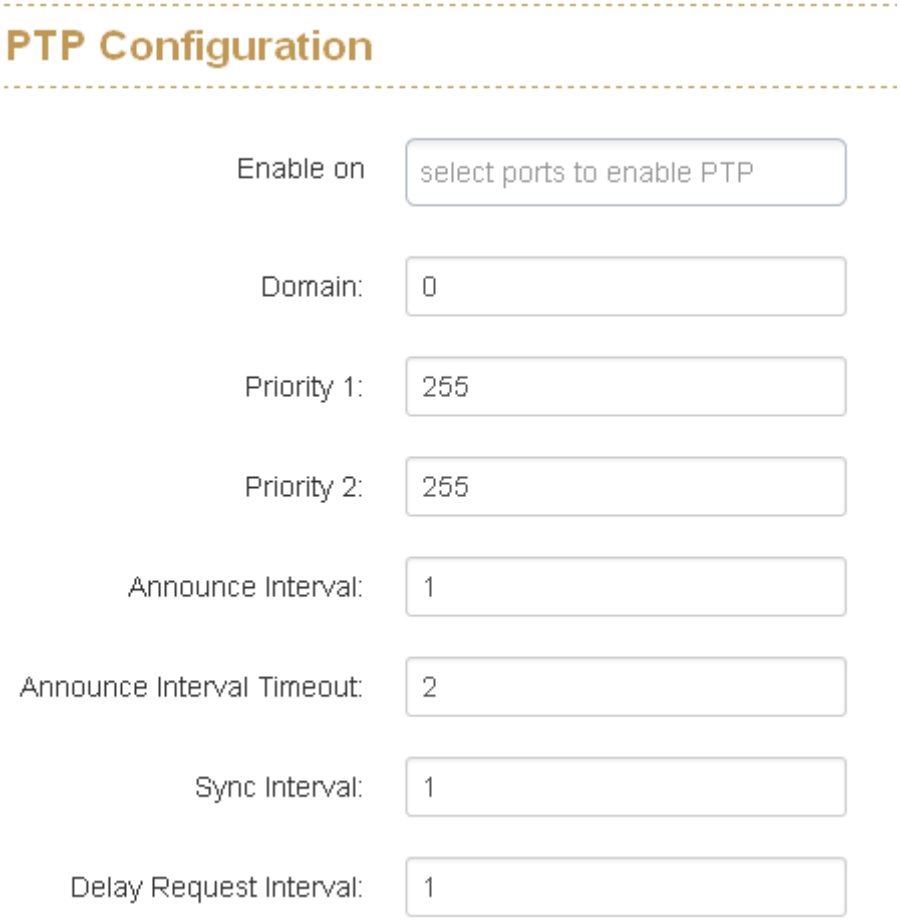
specify the time for announcing timeout messages. The range is 2 to 10 seconds. The default is 2 (4 seconds).

Sync Interval:

enter the time for sending synchronization messages. The range is -1 second to 1 second. The default is 1 second.

Delay Request Interval:

specify the time recommended to the member devices to send delay request messages when the port is in the master state. The range is -1 second to 6 seconds. The default is 1 (2 seconds).



6.17 G.8032 ERPS

6.17.1. G.8032 Ethernet Ring Protection Configuration

The G.8032 Ethernet Ring Protection Switch instances are configured here.

ID

The ID of the created Protection group

Enabled

Enable/Disable the G.8032 ERP.

Role

It can be either RPL owner or RPL Neighbor.

Type

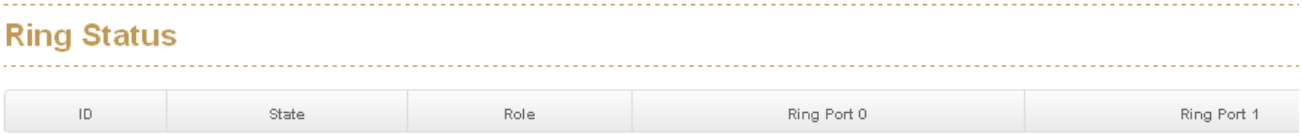
Type of Protecting ring. It can be either major ring or sub-ring.

Ring Port 0

This will create a Port 0 of the switch in the ring.

Ring Port 1

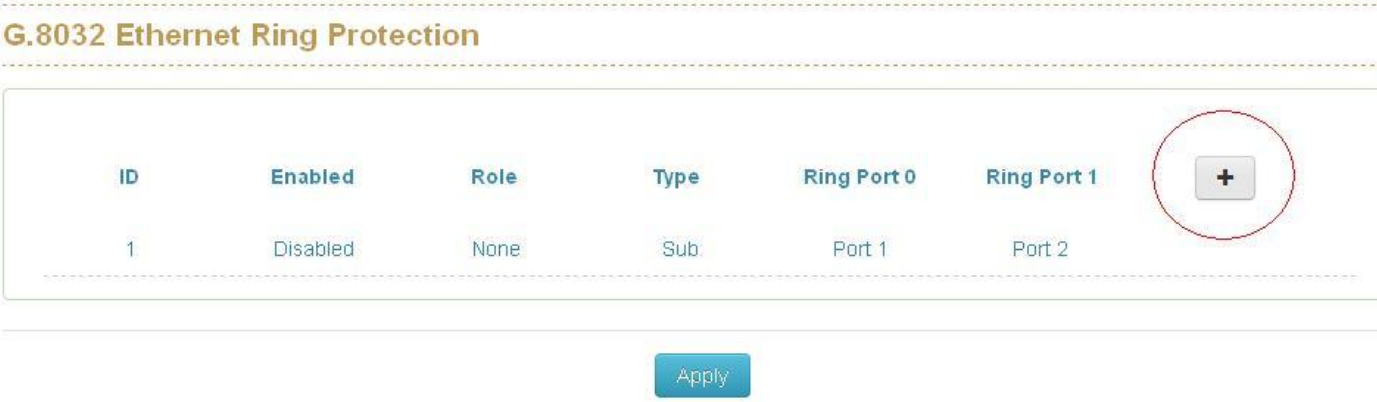
This will create "Ring Port 1" of the switch in the Ring.



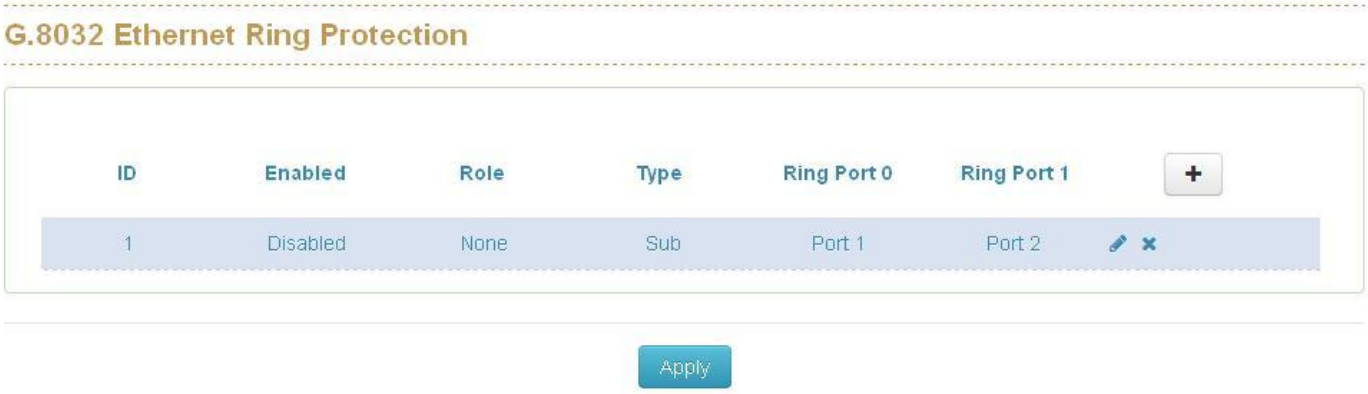
How to set G8032

6.16.1.1 Make sure you have disabled the MSTP protocol.

6.16.1.2 Press “+” icon to add one ring with G.8032 protocol.
PS: in this case, we will use the port9 and port10 of each switch to build a ring.



6.16.1.3 Enter edit mode



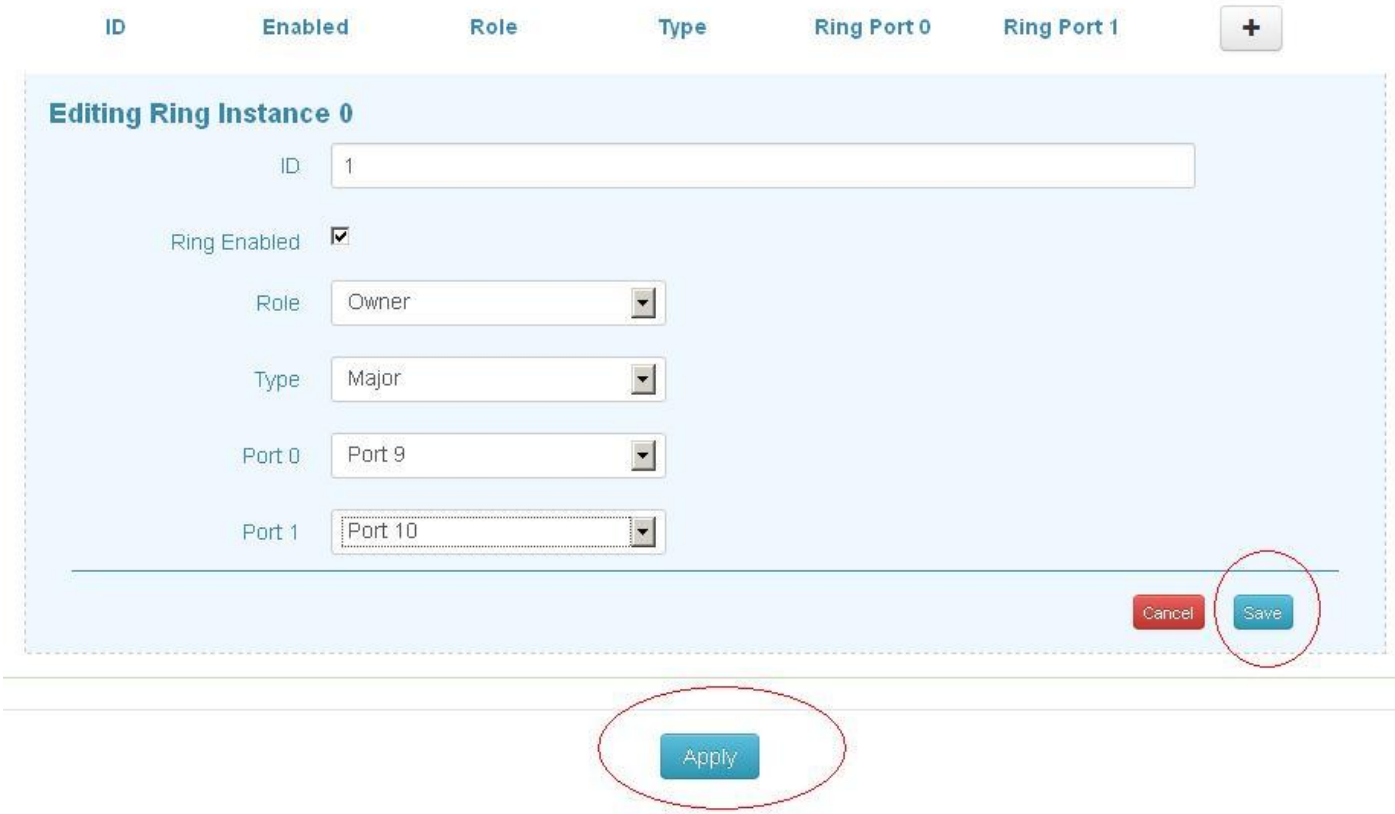
6.16.1.4 There are 3 switches in the ring of G.8032, one play the role of "owner", one for "neighbour" and one for "none" , remember 3 very import things during the setting procedure:

6.16.1.5 the port0 of "owner" switch must connect with the "neighbour" switch.

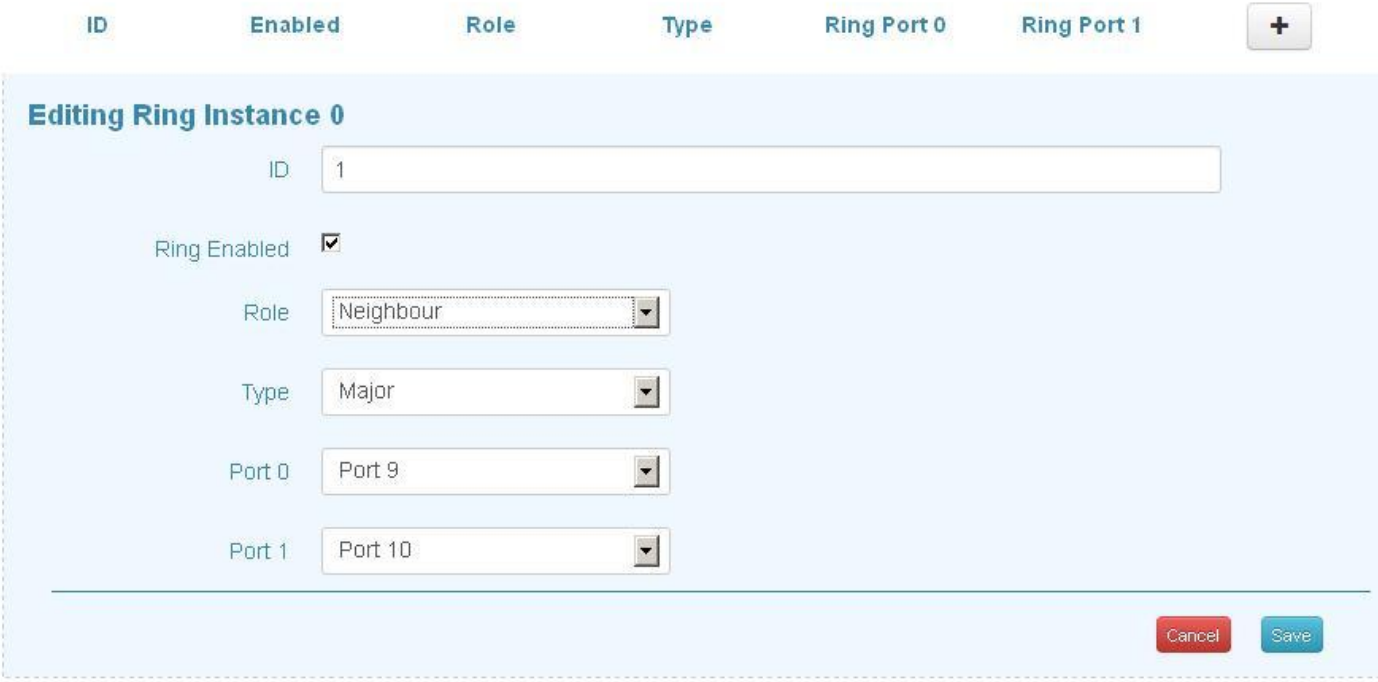
6.16.1.6 After enable the ring of G8032, the port0 of owner switch will be blocked at first.

For safe issue, we suggest the user to finished all setting G8032 then connect the physical connection if the user was not familiar the ring G8032 function.

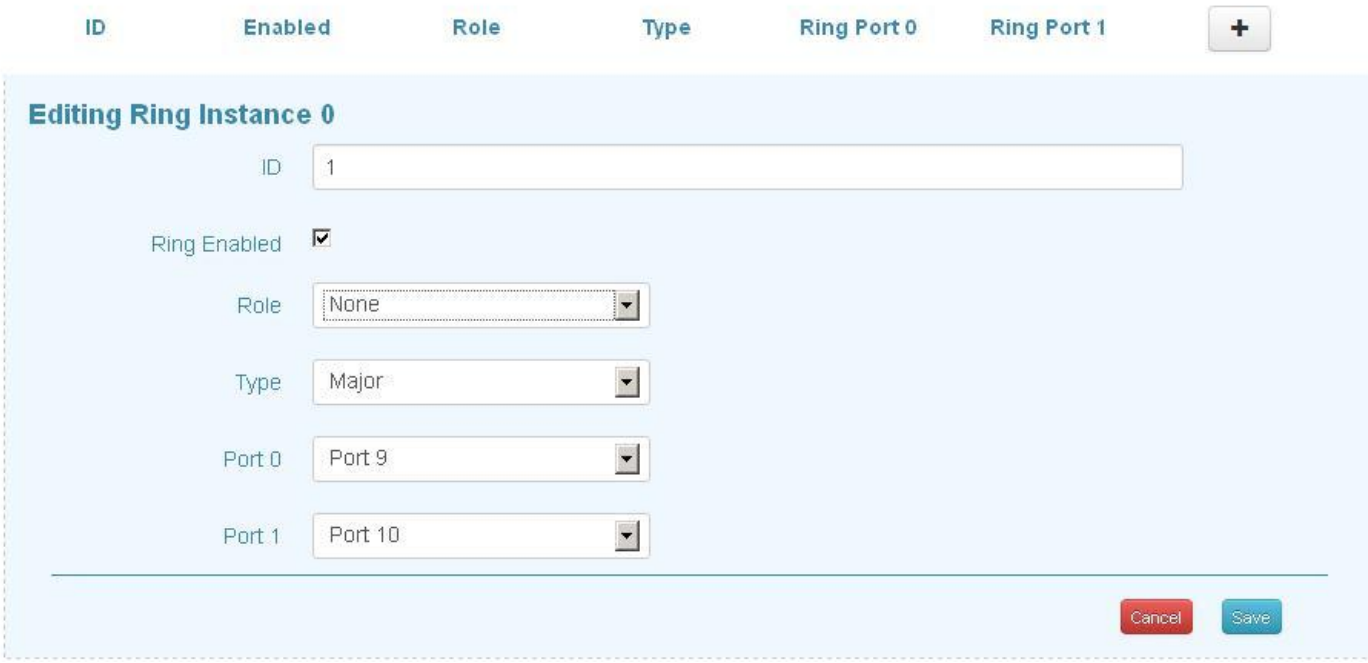
6.16.1.7 The setting of owner switch
(because we only have single ring, so we set the type as Major)



6.16.1.8 The setting of neighbour switch



6.16.1.9 The setting of none switch



6.16.2. Ring Status Help

ID

The ID of the created Protection group

State

ERPS state according to State Transition Tables in G.8032.

Role

It can be either RPL owner or RPL Neighbour.

Ring Port 0

true : ring port 0 is blocking

false : ring port 0 is not blocking

Ring Port 1

true : ring port 0 is blocking

false : ring port 0 is not blocking

6.178Maintenance

6.18.1 **Save Configuration**

Save setting of switch

6.18.2 Config backup/restore

Settings Backup

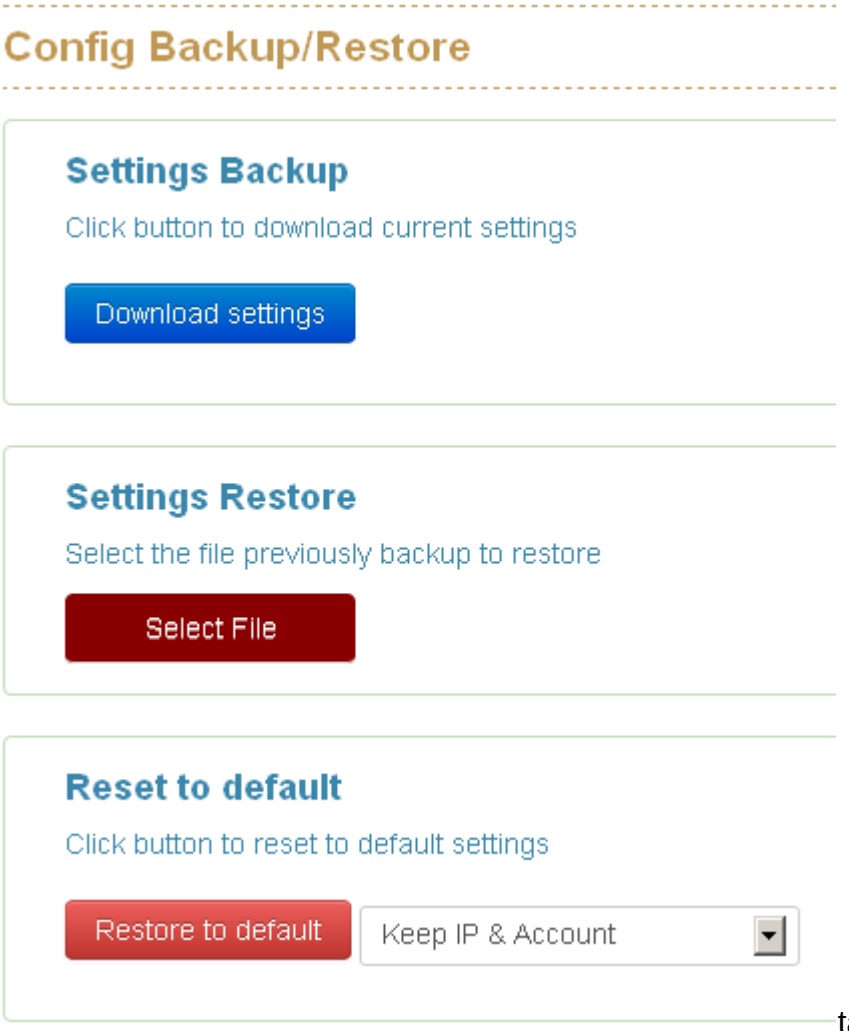
You can download the backup configuration of the switch.

Settings Restore

You can copy the backup configuration of the switch to the startup configuration on this page. The new startup configuration is not available immediately, which means that restart the switch is necessary.

Reset to default

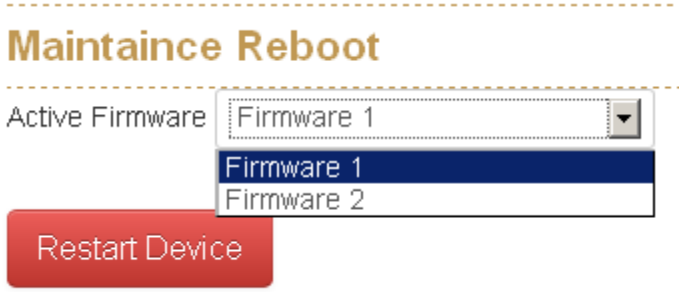
You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no res



tart is necessary.

6.18.3 Restart device

Reboot the switch with selected firmware.



6.18.4 Firmware Upgrade

Update the switch with the firmware file which on your desktop.

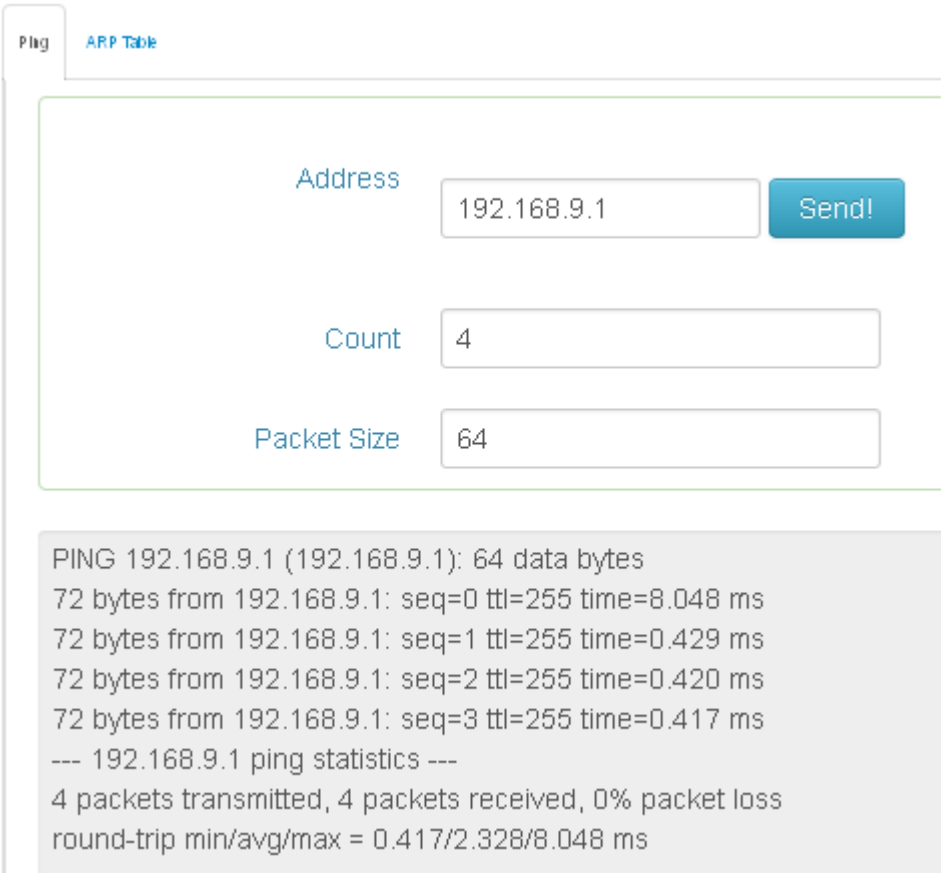
6.18.5 **Diagnostics**

PING

Address: Set the IP address which you want to ping

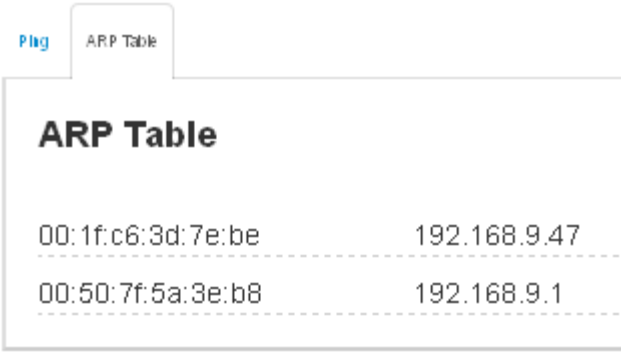
Count: Set the times of Ping

Packet Size: set the size of Ping packet.



ARP Table

You can find the MAC addrees of each IP you have ping via this switch in here.



Troubles shooting

- Verify that is using the right power cord/adapter (DC 24-48V), please don't use the power adapter with DC output higher than 48V, or it may damage this device.
- Select the proper UTP/STP cable to construct the user network. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections that depend on the connector type the switch equipped: 100Ω Category 3, 4 or 5 cable for 10Mbps connections, 100Ω Category 5 cable for 100Mbps connections, or 100Ω Category 5e/above cable for 1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).
- **Diagnosing LED Indicators:** To assist in identifying problems, the switch can be easily monitored through panel indicators, which describe common problems the user may encounter and where the user can find possible solutions.
- If the power indicator does not light on when the power cord is plugged in, you may have a problem with power cord. Then check for loose power connections, power losses or surges at power outlet. If you still cannot resolve the problem, contact the local dealer for assistance.
- If the LED indicators are normal and the connected cables are correct but the packets still cannot be transmitted. Please check the user system's Ethernet devices' configuration or status.

Appendix A—RJ-45 Pin Assignment

RJ-45 Pin Assignments

The UTP/STP ports will automatically sense for Fast Ethernet (10Base-T/100Base-TX connections), or Gigabit Ethernet (10Base-T/100Base-TX/1000Base-T connections). Auto MDI/MDIX means that the switch can connect to another switch or workstation without changing straight through or crossover cabling. See the figures below for straight through and crossover cable schematic.

- **10 /100BASE-TX Pin outs**

With10/100BASE-TX cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data.

- **RJ-45 Pin Assignments**

Pin Number	Assignment
1	Tx+
2	Tx-
3	Rx+
6	Rx-

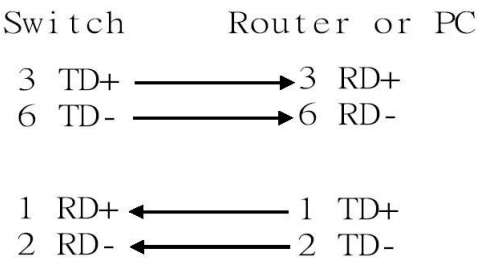
[NOTE] "+" and "-" signs represent the polarity of the wires that make up each wire pair.

The table below shows the 10/100BASE-TX MDI and MDI-X port pin outs.

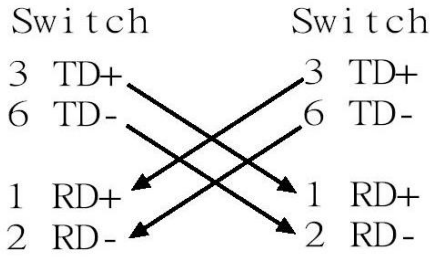
Pin Number	MDI-X Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)

■ 10/100Base-TX Cable Schematic

The following two figures show the 10/100Base-TX cable schematic.



Straight-through cable schematic

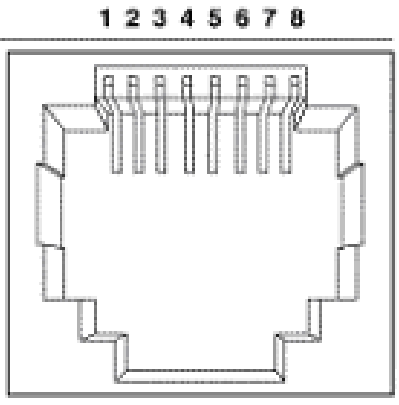


Cross over cable schematic

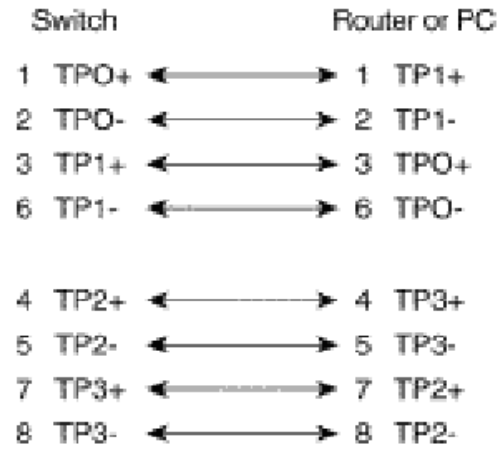
■ 10/100/1000Base-TX Pin outs

The following figure shows the 10/100/1000 Ethernet RJ-45 pin outs.

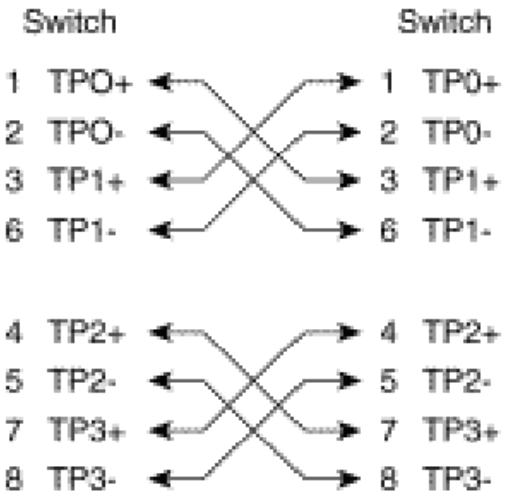
Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



■ 10/100/1000Base-TX Cable Schematic



Straight through cables schematic



Cross over cables schematic

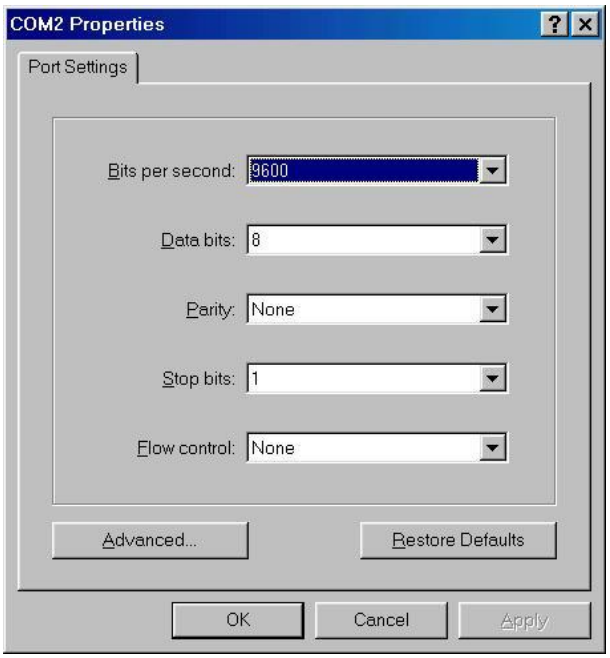
Appendix B—Command Line mode

Except the web acess mode, the Lantech switch also support Telnet access and console access mode, to compare the web access mode, both the Telnet and console only support command line user interface, all these commands will show as below:

1. Access via console port

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

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



The settings of communication parameters

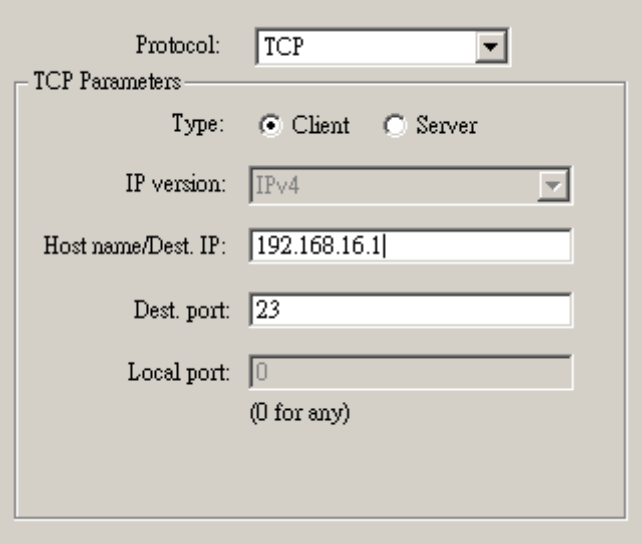
Having finished the parameter settings, click '**OK**'. When the blank screen shows up, press Enter key to have the login prompt appears. First you need to key in "cli" to enter the command line mode then Key in '**admin**' (default value) for both User name and

Password (use **Enter** key to switch), then press Enter and the Main Menu of console management appears. Please see below figure for login screen.

Notice: if you forgot the password, you can access the switch via console port and input lantech/lantech to restore the password to default.

2. Access via Telnet

Use Telnet utility to access switch IP and make sure the socket was set as 23, all the commands under Telnet mode were the same as the Console mode.



3. Commands

3.1 **System**

Command: system

Parameter: N/A

Description: Enter the system mode

Example:

```
>system
Available Commands:
System Configuration
System Contact [<conta
System Name [<name>]
System Location [<loca
System Description [<
System DHCPClient [ena
System DHCPServer [ena
System DHCPStatus
System NetStatus
System NetSettingIPv4
System NetSettingIPv6
System Reboot
System RestoreDefault
System Log
System Save
System Ping [<IpAddr>]
System Arp
System Memory
System ConfigAccess [e
System Upgrade [URL]
SYSTEM>_
```

3.1.1 Command: system> configuration

Parameter: N/A

Description: show the information of switch

Example:

```
SYSTEM>configuration
SYSTEM>
SystemName : IES-5408DSFP
SystemDescription : 4 1000 SFP +
SystemLocation : 13
SystemContact :
SystemTimeZoneOffset : 0
OID : 1.3.6.1.4.1.37072.302.2.3
MacAddr : 00:11:22:33:44:81
SystemDate : Fri Jun 21 2013 15:
SystemUptime : 77141
SoftwarekernelVersion : 39c48cd6
SoftwareVersion : V3.27
```

3.1.2 Command: system > Contact

Parameter: N/A

Description: display or fix the contact information

Example: if I want to change the contact windows to jacky@lantechcom.tw

```
SYSTEM>contact jacky@lantechcom.tw
SYSTEM>
SystemContact : jacky@lantechcom.tw
```

3.1.3 Command: system > name

Parameter: N/A

Description: display or fix the system name

Example:

```
SYSTEM>name
SYSTEM>
SystemName : IES-5408DSFP
SYSTEM>name IGS-5400-2P
SYSTEM>
SystemName : IGS-5400-2P
```

3.1.4 Command: system > location

Parameter: N/A

Description: display or fix the location

Example:

```
SYSTEM>location
SYSTEM>
SystemLocation : 13
SYSTEM>location Taiwan
SYSTEM>
SystemLocation : Taiwan
```

3.1.5 Command: system > description

Parameter: N/A

Description: display or fix the system description

Example:

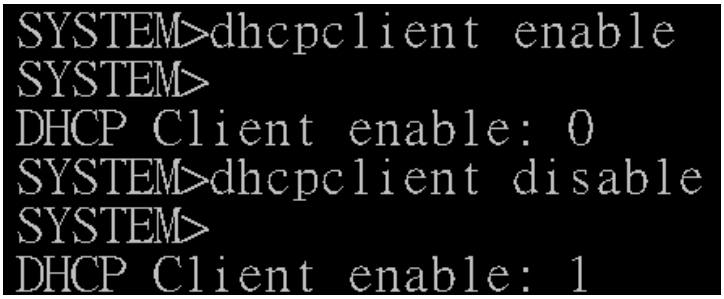
```
SYSTEM>
SystemDescription : switch
SYSTEM>description industrial
SYSTEM>
SystemDescription : industrial
```

3.1.6 Command: system > DHCPclient

Parameter: enable/disable

Description: enable or disable DHCP client

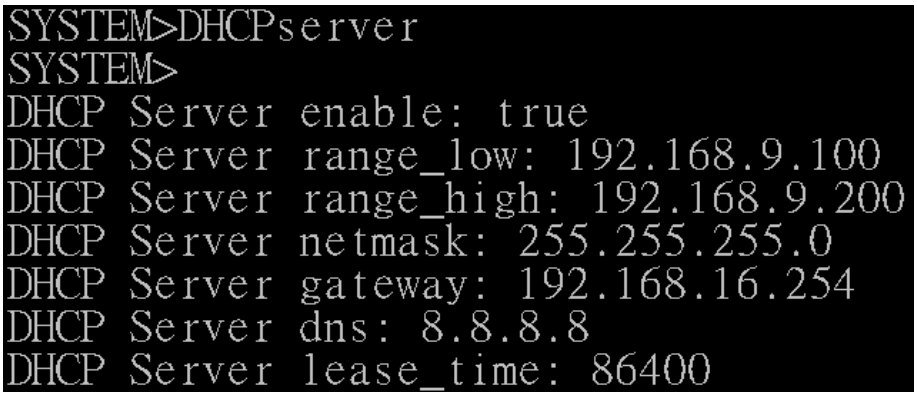
Example:



3.1.7 Command: system > DHCP server

Parameter: [enable|disable]→ enable or disable DHCP server
[<range_low>]/[<range_high>]→ set the IP range
[<netmask>]→ set submask
[<gateway>]→ set gateway
[<dns>]→ set DNS server
[<lease_time>]→ set the lease time of released IP

Example:



3.1.8 Command system > DHCPstatus

Parameter: N/A

Description: show the information of DHCP client

Example:

```
SYSTEM>DHCPstatus
SYSTEM>
MacAddress              IpAddress
---------------------   ---------------------------
    00:1f:c6:3d:7e:25                  192.168.9.101
```

3.1.9 Command: system > netstatus

Parameter: N/A

Description: show the status about IP address

Example:

```
SYSTEM>netstatus
SYSTEM>
IpAddr : 192.168.16.1
Netmask : 255.255.255.0
GatewayIp :
DnsIp : 168.95.1.1
```

3.1.10 Command: system > netsettingIPv4

Parameter: [<IpAddr>]→ set IP address
[<netmask>]→ set netmask
[<gatewayip>]→ set gateway
[<dnsip>]→ set DNS server

Description: set the IP detail of switch

Example:

```
SYSTEM>netsettingIPv4
SYSTEM>
IpAddr : 192.168.16.1
Netmask : 255.255.255.0
GatewayIp : 192.168.9.1
DnsIp : 168.95.1.1
```

3.1.11 Command: system > netsettingIPv6

Parameter: N/A

Description: set the IP address of IPv6

Example:

```
SYSTEM>netsettingIPv6
SYSTEM>
IpAddrv6 : 2001:0db8:0:f101::3
```

3.1.12 Command: system > reboot

Parameter: N/A

Description: reboot the switch

Example:

```
SYSTEM>reboot
SYSTEM>System Reboot after 1 sec

Broadcast message from root (Fri Jun 21 17

The system is going down for reboot NOW!
```

3.1.13 Command: system > restoredefault

Parameter: keep_none → restore all setting

keep_all → restore all but keep original IP address and account

keep_ip → restore all but keep original IP address

keep_account → restore all but keep original account

Description: restore the setting of switch to factory default

Example:

```
SYSTEM>restoredefault ?
Invalid parameter:?
Syntax:System RestoreDefault [keep_none | keep_all | keep_ip | keep_account]
```

3.1.14 Command: system > log

Parameter: N/A

Description: display the event log

Example:

```
Fri, 21 Jun 2013 03:40:27 GMT  linkchg
Fri, 21 Jun 2013 05:37:26 GMT  linkchg
Fri, 21 Jun 2013 05:37:40 GMT     boot
Fri, 21 Jun 2013 06:04:23 GMT     auth
Fri, 21 Jun 2013 06:15:20 GMT     auth
```

3.1.15 Command: system > save

Parameter: N/A

Description: save the fixed setting

Example:

```
SYSTEM>save
SYSTEM>
System save success!!
```

3.1.16 Command: system > ping

Parameter; N/A

Description: ping the IP address

Example:

```
SYSTEM>ping 192.168.16.1
SYSTEM>host 192.168.16.1 is alive
```

3.1.17 Command: system > arp

Parameter: N/A

Description: resolve the IP address to MAC address

Example:

```
SYSTEM>arp
SYSTEM>
IpAddress              MacAddress
--------------------   ----------------------------
      192.168.16.66              00:1f:c6:3d:7e:25
```

3.1.18 Command: system > memory

Parameter: N/A

Description: display the status of used switch memory

Example:

```
SYSTEM>memory
SYSTEM>
Type             Size(kb)
-----------      ----------------
   MemTotal                239540
    MemFree                173664
```

3.1.19 Command: system > configaccess

Parameter: [export|import] → export or import the setting of switch
[URL] → set the destination which save/load the setting file, support both the TFTP and FTP protocol.

Description: export or import the setting of switch

Example:

```
SYSTEM>configaccess export ftp://192.168.16.66
```

3.1.20 Command: system > upgrade

Parameter: [URL] → set the source of firmware file, support TFTP and FTP and HTTP protocol.

Description: update switch firmware

Example:

```
SYSTEM>upgrade tftp:192.168.16.1

Please wait for upgrade
```

3.2 LLDP

Command: LLDP

Parameter: N/A

Description: Enter the LLDP mode

Example:

```
>lldp
Available Commands:
LLDP Configuration [<port_list>]
LLDP Enabled [enable|disable]
LLDP Mode [<port_list>] [enabledRx
LLDP Interval [<interval>]
LLDP Timetolive [<ttl>]
LLDP Info [<port_list>]
LLDP Statistics [clear]
LLDP>_
```

3.2.1 Command: LLDP > configuration

Parameter: N/A

Description: display the LLDP information

Example:

```
LLDP>configuration
LLDP>
Interval: 10
Port    Mode
----    ------------
   1      enabledRxTx
   2      enabledRxTx
   3      enabledRxTx
   4      enabledRxTx
   5      enabledRxTx
   6      enabledRxTx
   7      enabledRxTx
   8      enabledRxTx
   9      enabledRxTx
  10      enabledRxTx
  11      enabledRxTx
  12      enabledRxTx
```

3.2.2 Command: LLDP > enabled

Parameter: N/A

Description: enable LLDP protocol

Example:

```
LLDP>enabled
LLDP>
Enabled: true
```

3.2.3 Command: LLDP > mode

Parameter: [<port_list>]→display LLDP information of the dedicated port

[enabledRxTx]→ enable Tx and Rx of LLDP function with dedicated port

[enabledTxOnly]→ enable Tx only of LLDP function with dedicated port

[enabledRxOnly]→ enable Rx only of LLDP function with dedicated port

[disabled]→ disable LLDP function with dedicated

Description: enable LLDP function of each port

Example:

```
LLDP>mode
LLDP>
Port     Mode
----     ------------
   1        enabledRxTx
   2        enabledRxTx
   3        enabledRxTx
   4        enabledRxTx
   5        enabledRxTx
   6        enabledRxTx
   7        enabledRxTx
```

3.2.4 Command: LLDP > interval

Parameter: N/A

Description: set the interval time of LLDP

Example:

```
LLDP>interval 10
LLDP>
Interval: 10
```

3.2.5 Command: LLDP > timetolive

Parameter: N/A

Description: display the alive time of LLDP information.

Example:

```
LLDP>timetolive
LLDP>
Time to live : 15
```

3.2.6 Command: LLDP > info

Parameter: N/A

Description: display the LLDP information of neighbor port

Example:

```
LLDP>info
LLDP>
Localport       ChassisID              PortID  PortDescription SystemNa
---------       -------------------    ------  --------------- -------
```

3.2.7 Command: LLDP > statistics

Parameter: N/A

Description: display the detail information of LLDP settings

Example:

```
LLDP>statistics
LLDP>
Total LLDP traffic statistics
Total entries added : 0
Total entries deleted : 0
Total entries aged : 0
Total frames out : 6127
Total frames in : 0
Total frames received in error : 0
Total frames discarded : 0
Total TLVs discarded : 0
Total TLVs unrecognized : 0
Localport        FramesIn         FramesOu
---------        --------         --------
        1               0               55
        2               0               55
        3               0               55
        4               0               55
```

3.3 Port

Command: port

Parameter: N/A

Description: Enter the port mode

Example:

```
>port
Available Commands:
Port Configuration [<port_list>]
Port Status [<port_list>]
Port Enabled [<port_list>] [enable|disable]
Port Description [<port_list>] [string]
Port Speed [<port_list>] [10hdx|10fdx|100hdx
Port FlowControl [<port_list>] [enable|disab
Port IngressRate [<port_list>] [<rate> kbps]
Port EgressRate [<port_list>] [<rate> kbps]
Port Statistics [clear]
```

3.3.1 Command: port > configuration

Parameter: N/A

Description: display the setting of each port

Example:

```
PORT>configuration
PORT>
Port    enabled Description     Speed Conf      Flow Control Co
----    ------- -----------     ----------      --------------
   1       true      Port 1          auto                   tr
   2       true      Port 2          auto                   tr
   3       true      Port 3          auto                   tr
   4       true      Port 4          auto                   tr
   5       true      Port 5          auto                   tr
   6       true      Port 6          auto                   tr
   7       true      Port 7          auto                   tr
```

3.3.2 Command: port > status

Parameter: N/A

Description: display the connection status of each port

Example:

```
PORT>status
PORT>
Port    Group ID        Type    Link    State   Speed
----    --------        ------  ----    -----   -----
   1           -1       100TX   down    enable    N/A
   2           -1       100TX   down    enable    N/A
   3           -1       100TX   down    enable    N/A
   4           -1       100TX     up    enable    100
   5           -1       100TX   down    enable    N/A
   6           -1       100TX   down    enable    N/A
   7           -1       100TX   down    enable    N/A
   8           -1       100TX   down    enable    N/A
   9           -1        DSFP   down    enable    N/A
```

3.3.3 Command: port > enabled

Parameter: [<port_list>]→ choose which port you want to enable or diasble
[enable|disable]→ enable/disable

Description: enable or disable switch port

Example:

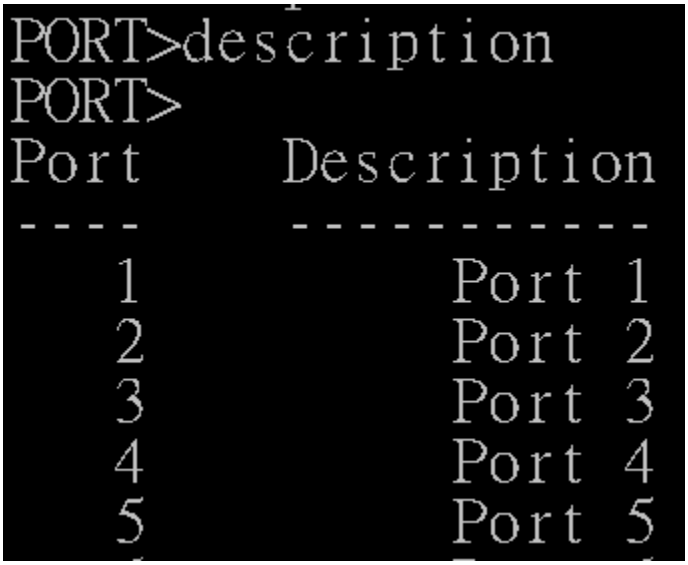
```
PORT>enable
PORT>
Port    Enabled
----    -------
   1       true
   2       true
   3       true
   4       true
   5       true
   6       true
   7       true
```

3.3.4 Command: port > description

Parameter: N/A

Description: display the description of each port

Example:

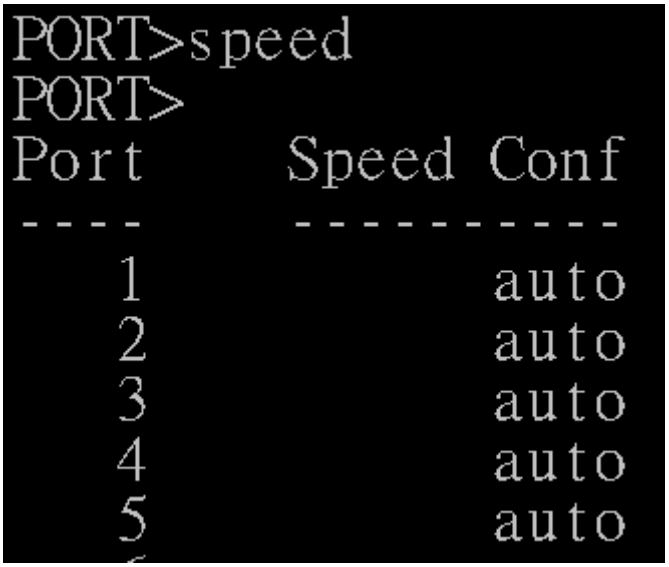


3.3.5 Command: port > speed

Parameter: N/A

Description: display the speed of each port

Example:

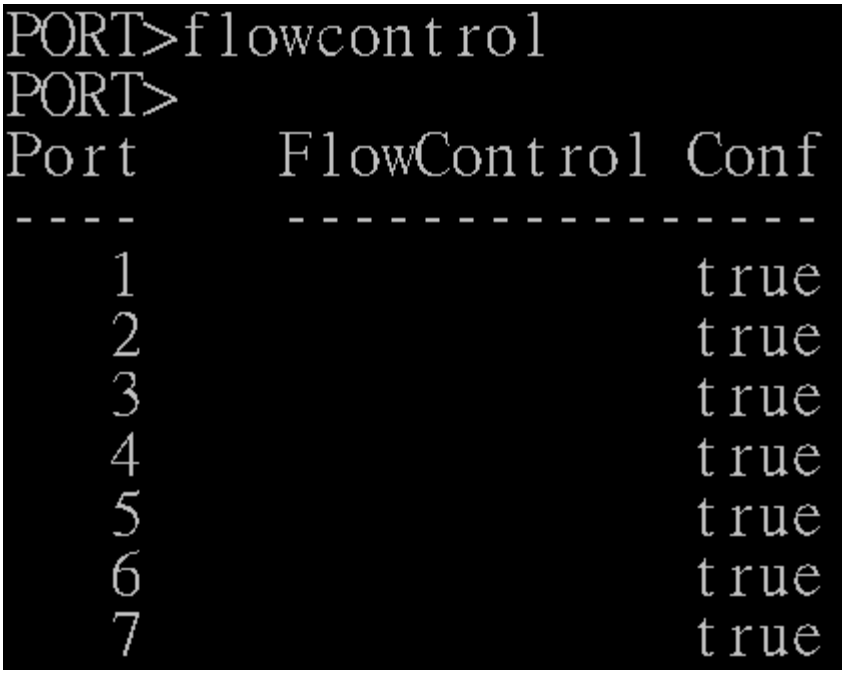


3.3.6 Command: port > flowcontrol

Parameter: [<port_list>]→ choose which port you want to enable or diasble
[enable|disable]→ enable/disable

Description: enable or disable flow control function of each port

Example:



3.3.7 Command: port > Ingressrate

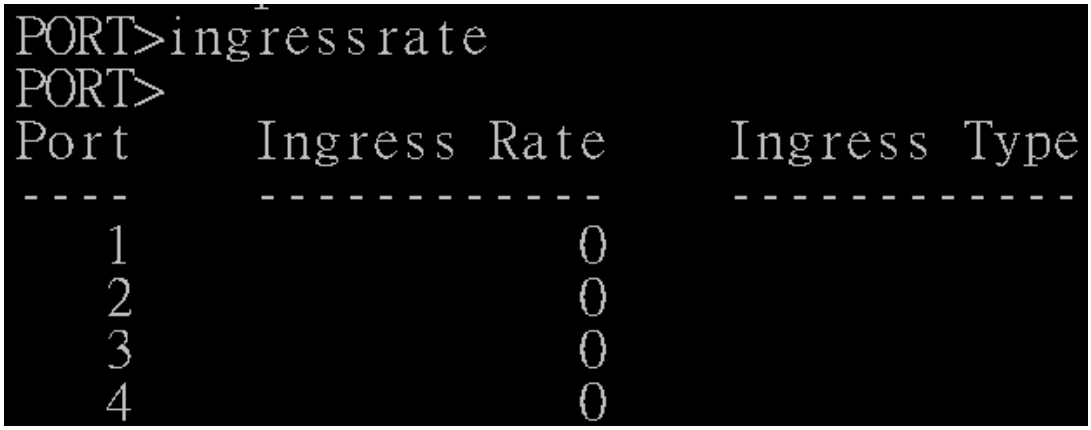
Parameter: [<port_list>]→ choose which port you want to set the ingress rate

[<rate> kbps]→set the ingress rate of these packet as below

- broadcast
- multicast
- unicast
- broad_uni
- broad_multi
- multi_uni
- uni_broad_multi

Description: set the ingress rate of the dedicated port with specified packet

Example:

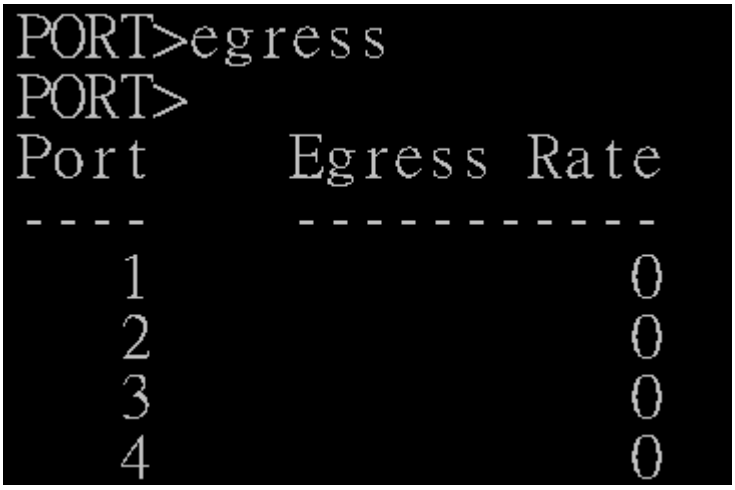


3.3.8 Command: port > egressrate

Parameter: [<port_list>]→ choose which port you want to set the ingress rate
[<rate> kbps]→set the ingress rate

Description: set the egress rate of the dedicated port

Example:



3.3.9 Command: port > statistics

Parameter: N/A

Description: display the detail information of port statistics

Example:


PORT>statistics
PORT>
ports :
Txgoodbyte :
Txgoodpkts :
Txmcpkts :
Txbrdcpkts :
Txerr :
Txucpkts :
Txmultiplepkts :
Txdeferredpkts :
Rxgoodbyte :
Rxbadbyte :
Rxgoodpkts :
Rxbadpkts :
Rxbrdcpkts :
Rxmcpkts :
Rxmacerror :
Rxbadfc :
Rxucpkts :
Rxunrecogcntr :
Rxgoodfc :
64byte :