CONNECTION TECHNOLOGY SYSTEMS

IPS-3120-PoE++
Managed Industrial PoE Gigabit Ethernet Switch

Network Management User’s Manual

Version 0.90

Trademarks

CTS is a registered trademark of Connection Technology Systems Inc. All other trademarks remain the property of their owners.

Copyright Statement

CTS has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Contents are subject to revision without prior notice. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from Connection Technology Systems Inc.

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 limitations are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. 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 your local distributors or an experienced radio/TV technician for help.

Changes or modifications to the equipment, which are not approved by the party responsible for compliance, could affect the user's authority to operate the equipment.

Shielded interface cables must be used in order to comply with emission limits.

Revision History

Manual Version	Firmware Version	Modification	Date
0.90	0.99.09	The initial version	20170727

Table of Content

1. HARDWARE OVERVIEW

Thank you for choosing the Managed Industrial PoE Gigabit Ethernet Switches. The Managed Industrial PoE Gigabit Ethernet Switches are designed to meet the massive needs for Gigabit Ethernet network deployments and aim at Industrial PoE applications that demand wide range of operating temperature. They are fully compliant with IEEE802.3, 802.3u, 802.3ab, 802.3z, 802.1p, 802.1q, 802.3x, 802.3af and 802.3at standards. The built-in management module allows users to configure this Managed Industrial PoE Gigabit Ethernet Switch and monitor the operation status locally or remotely through network.

With power redundancy, users can prevent network disconnection from unexpected power outage. By employing store and forward switching mechanism, the Switch provides low latency and faster data transmission. Moreover, it also supports more advanced-ethernet management functions, such as QoS and VLAN. Users can configure the required settings of the Switch and monitor its real-time operational status via Command Line Interface (CLI) and Web GUI.

1.1 Specification

Interface

IPS-3112-PoE++:

8 x 10/100/1000Mbps RJ-45, 60W PoE/PSE

4 x 100/1000Mbps SFP Slot

Console : 1 x RS-232 (RJ-45)

IPS-3108-EXP:

8 x 10/100/1000Mbps RJ-45, 30W PoE/PSE

Standards

IEEE802.3 10Base-T

IEEE802.3u 100Base-TX/FX

IEEE802.3ab 1000Base-T

IEEE802.3az EEE

IEEE802.3z 1000Base-X

IEEE802.1p Priority

IEEE802.1q Tag VLAN

IEEE802.3x Flow Control

IEEE802.1D/IEEE802.1w STP/RSTP

IEEE802.3af Power over Ethernet

IEEE802.3at Power over Ethernet Enhancements

IEEE802.1x Authentication Network Access Control

H/W Specification

Store and Forward Switching Mechanism
Auto Crossover for MDI/MDI-X in TP Port
Auto Negotiation in TP Port
Half/Full Duplex Mode Operation
Jumbo Frame up to : 10K Bytes
MAC Address Table : 8K
Non-Blocking Switching Fabric : 24Gbps
VLAN ID : 4K
1 Digital Output(Alarm Relay)
1 Digital Input

Switch Features

IEEE802.1q Tag Based VLAN
IGMP Snooping v1/v2
QoS Based on P-bit, DSCP
Strict Priority Queuing(SPQ)
Weighted Round Robin(WRR)
Port Trunking

Network Management

Telnet CLI
SNMP v1/v2c/v3
DHCP Client
FTP/HTTP/TFTP Firmware Upgrade
Dual Image
SNTP
SSHv2
Eventlog
Syslog

Cable Specifications

The following table contains various cable specifications for the Managed Switch. Please make sure to use the proper cable when connecting the Managed Industrial PoE Gigabit Ethernet Switches.

Cable Type	Description
10BASE-T	UTP Category 3, 4, 5 (100 meters max.) EIA/TIA- 568 150-ohm STP (100 meters max.)
100BASE-TX	UTP Cat. 5 (100 meters max.) EIA/TIA-568 150-ohm STP (100 meters max.)
1000BASE-T	UTP Cat. 5e (100 meters max.) UTP Cat. 5 (100 meters max.) EIA/TIA-568B 150-ohm STP (100 meters max.)
100BASE-FX	Multi-mode fiber module(2km) / Single-mode fiber module
1000BASE-SX	Multi-mode fiber module (550m)
1000BASE-LX	Single-mode fiber module (10km)
1000BASE-LH	Single-mode fiber module (30km/50km)
1000BASE-ZX	Single-mode fiber module (80km)
Mini-GBIC	SFP Transceiver for: 1000BASE-SX Multi-mode fiber module (550m) 1000BASE-LX Single-mode fiber module (10km) 1000BASE-LH Single-mode fiber module (30km/50km) 1000BASE-ZX Single-mode fiber module (80km)

1.2 Panel Layout

Front Panel

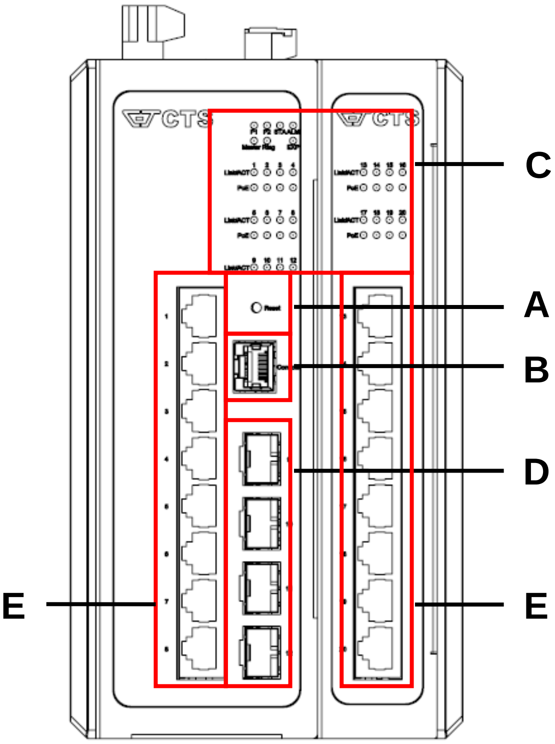


Figure 1. Front Panel

A. Reset Button:

- Insert a pin or paper clip to press the Reset Button for 5 seconds to restart the system.
- Insert a pin or paper clip to press the Reset Button for 10 seconds to reset the device back to defaults.

B. Console port (RJ-45 to RS-232)

C. LEDs (for more information, please refer to **chapter 3.1**)

D. 100/1000Mbps SFP port(s)

E. 10/100/1000Mbps RJ-45 port(s)

Rear Panel

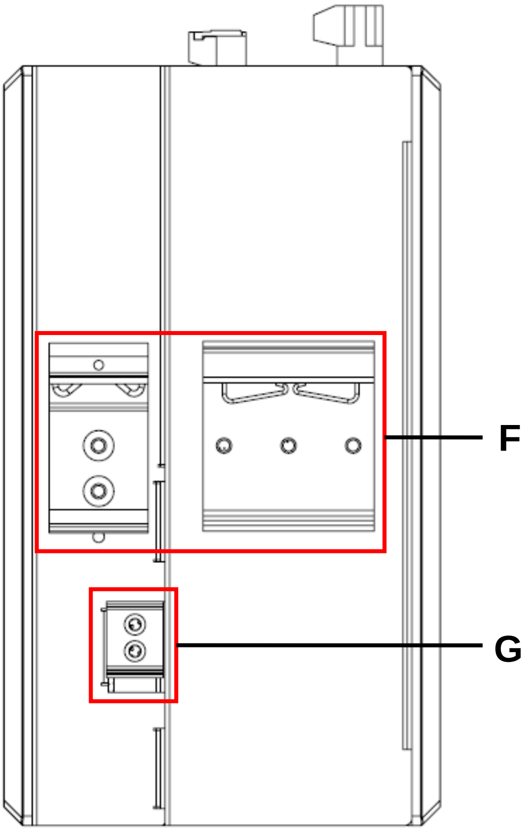


Figure 2. Rear Panel

Top Panel

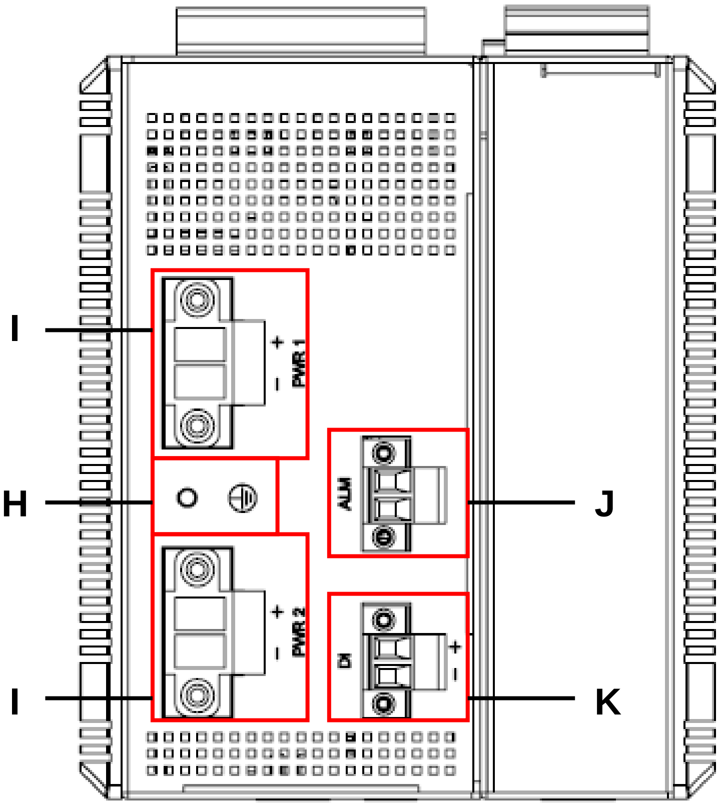


Figure 3. Top Panel

F. Din-Rail metal spring (for more information, please refer to **chapter 2.3.1**)
G. Slide Switch metal spring (for more information, please refer to **chapter 2.3.2**)
H. Ground screw (for more information, please refer to **chapter 2.3.3**)
I. Terminal blocks for power supply (for more information, please refer to **chapter 2.4**)
J. Terminal blocks for relay alarm output (for more information, please refer to **chapter 2.4**)
K. Terminal blocks for digital input (for more information, please refer to **chapter 2.4**)

2. INSTALLATION

To properly install the Managed Industrial PoE Gigabit Ethernet Switch, please follow the procedures listed below. Procedures covered in this chapter are described below in separate sections.

- Installation Requirements
- Unpacking the Managed Industrial PoE Gigabit Ethernet Switch
- Installing the Managed Industrial PoE Gigabit Ethernet Switch
- Powering on the Managed Industrial PoE Gigabit Ethernet Switch
- Connecting the Managed Industrial PoE Gigabit Ethernet Switch to the Network

2.1 Installation Requirements

ATTENTION

Be sure to power off before installing or wiring your Managed Industrial PoE Gigabit Ethernet Switch.

Be sure to calculate the maximum possible current in each power wire and common wire. If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

Be sure to read and follow important guidelines as below:

- Do not run signal or communications wiring and power wiring through the same wire conduit. Wires with different signal characteristics should be routed separately to avoid interference.
- It is recommended that wiring which shares similar electrical characteristics can be bundled together.
- Keep input wiring and output wiring separate and label the wiring to all devices in the system if necessary.

2.2 Checking the Package Contents

Unpack the package carefully and check the package contents. The standard package should contain the following items:

- 1 Managed Industrial PoE Gigabit Ethernet Switch

- Quick Installation Guide x 1 and User manual CD x 1

***Note:** If any of the above items is found missing or damaged, please contact your local sales representative for support or replacement.*

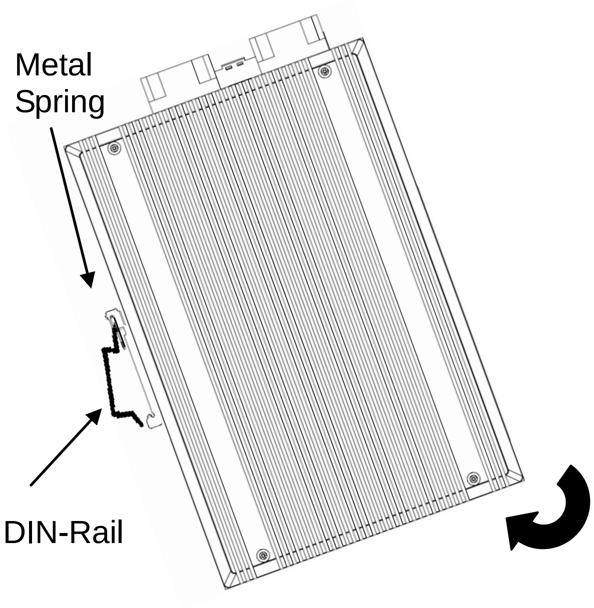
2.3 Installing the Managed Industrial PoE Gigabit Ethernet Switch

ATTENTION

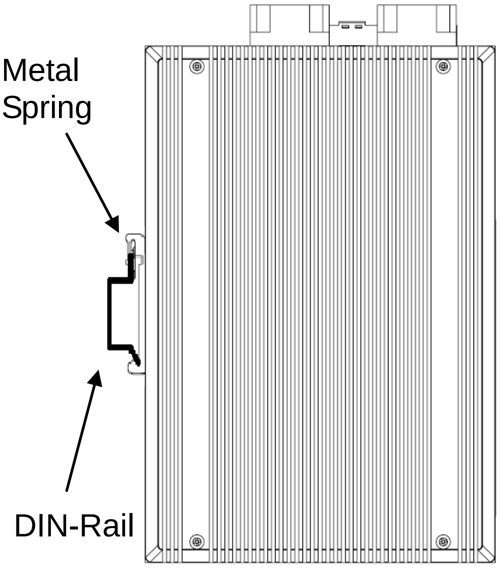
This product is intended to be mounted to a well-grounded mounting surface, such as a metal panel.

2.3.1 DIN-Rail Installation

STEP 1：Insert the top of the DIN-Rail into the slot just below the metal spring



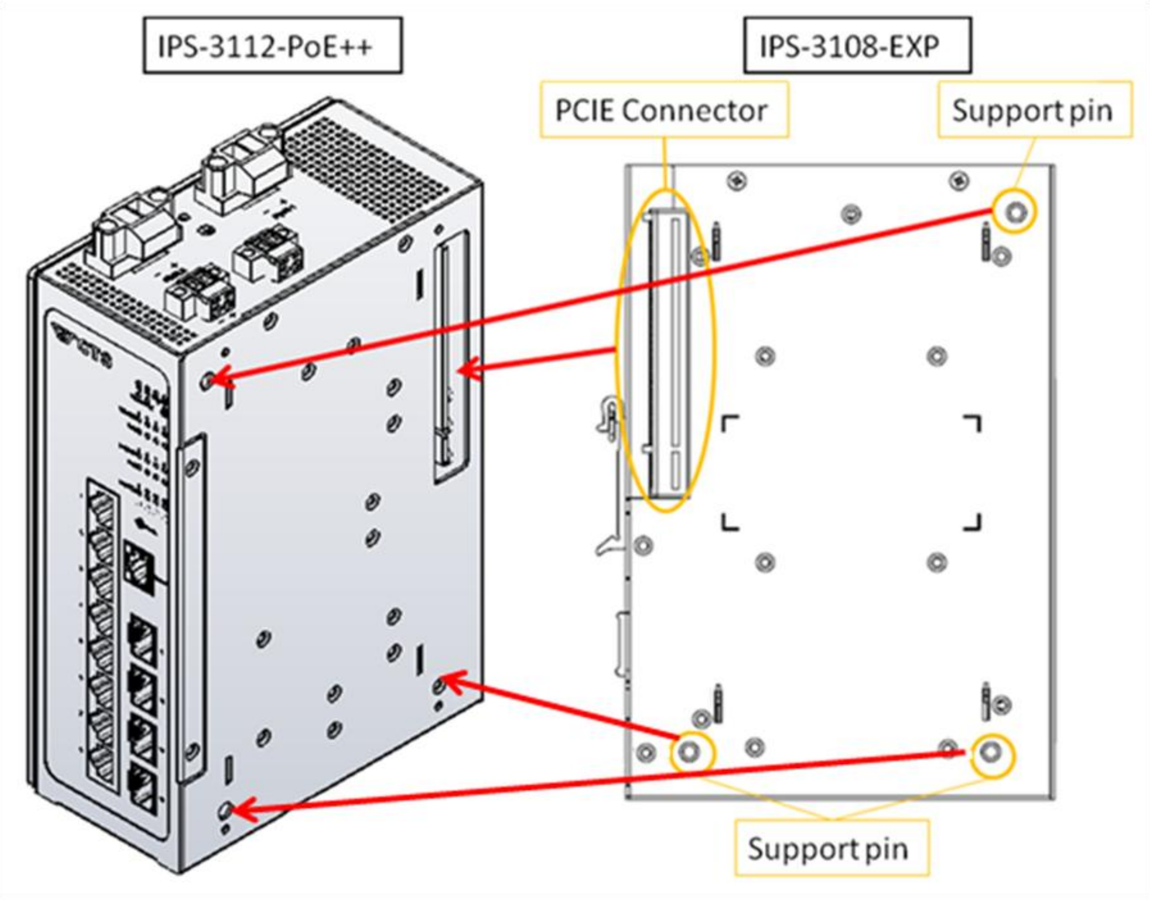
STEP 2：The DIN-Rail attachment unit will be snapped into place as shown

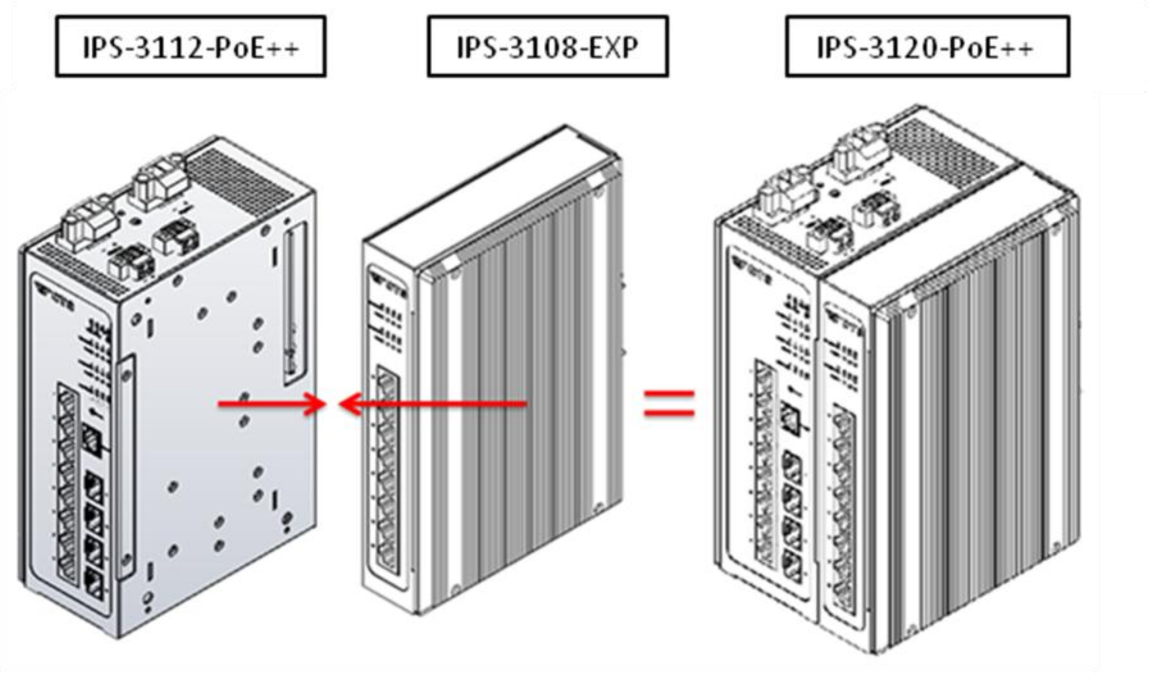


2.3.2 Assemble and Disassemble IPS-3120-PoE++ Expansion Module

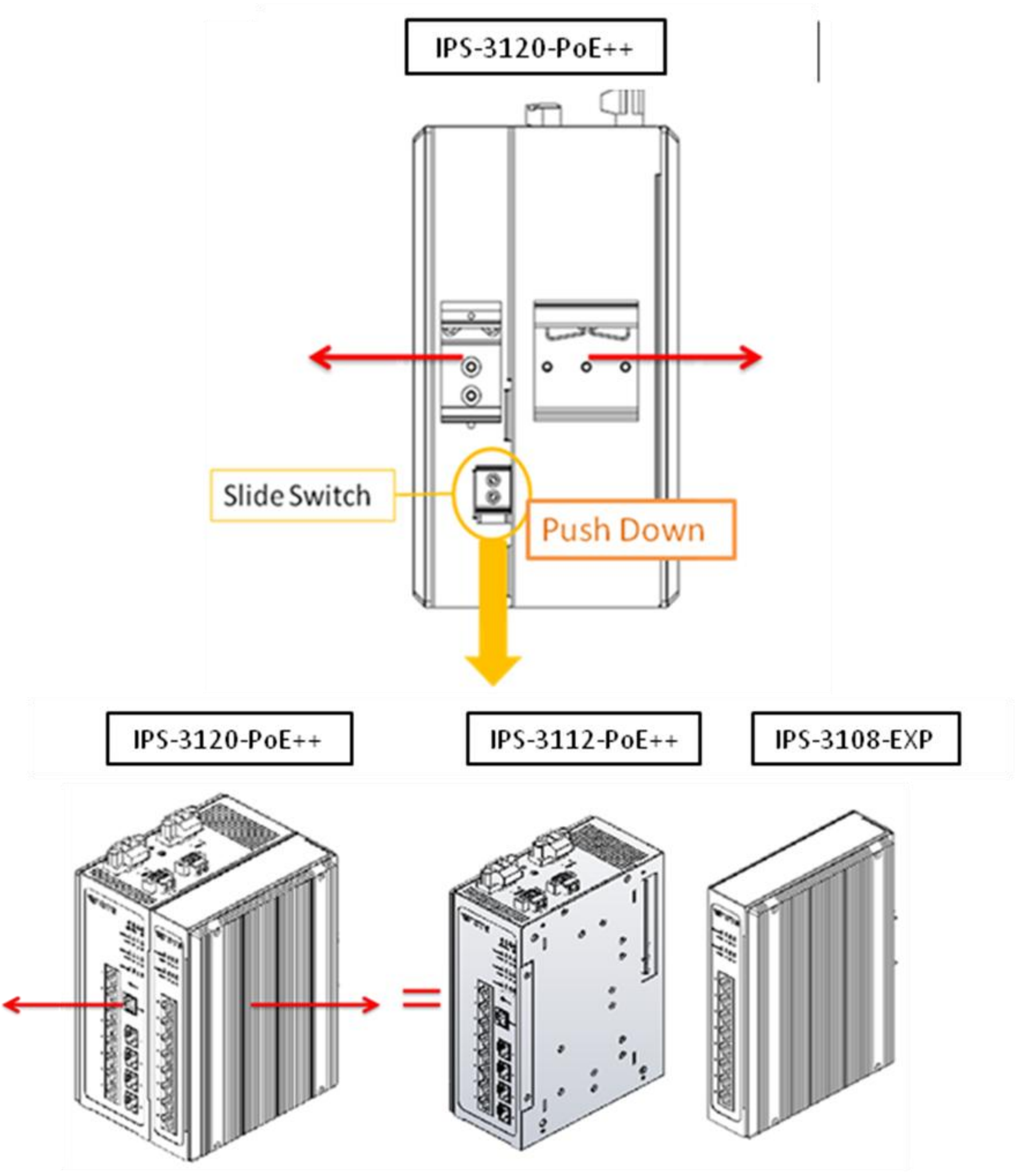
Combine two models into one model.
If you want to use both your IPS-3108-EXP and IPS-3112-PoE++ as a IPS-3120-PoE++ Expansion Module.
Dock IPS-3108-EXP into the IPS-3112-PoE++ as shown in the illustration below.

Assemble: 1 PCIE and 3 support pins on the IPS-3108-EXP aligned with the corresponding holes on the IPS-3112-PoE++, and then close together, when hears the click sound, that has been completed close, 2 machines will combine into IPS-3120-PoE++ Expansion Module.





Disassemble: There is a slide switch on the rear side of the IPS-3112-PoE++, push the slide switch down to the bottom, both hands hold IPS-3112-PoE++ and IPS-3108-EXP respectively, and separate it, then it restored to 2 devices.



2.3.3 Grounding the Managed Industrial PoE Gigabit Ethernet Switch

Grounding helps to limit the effects of noise due to electromagnetic interference (EMI). Be sure to install the ground connection from the ground screw to the grounding surface before connecting devices.

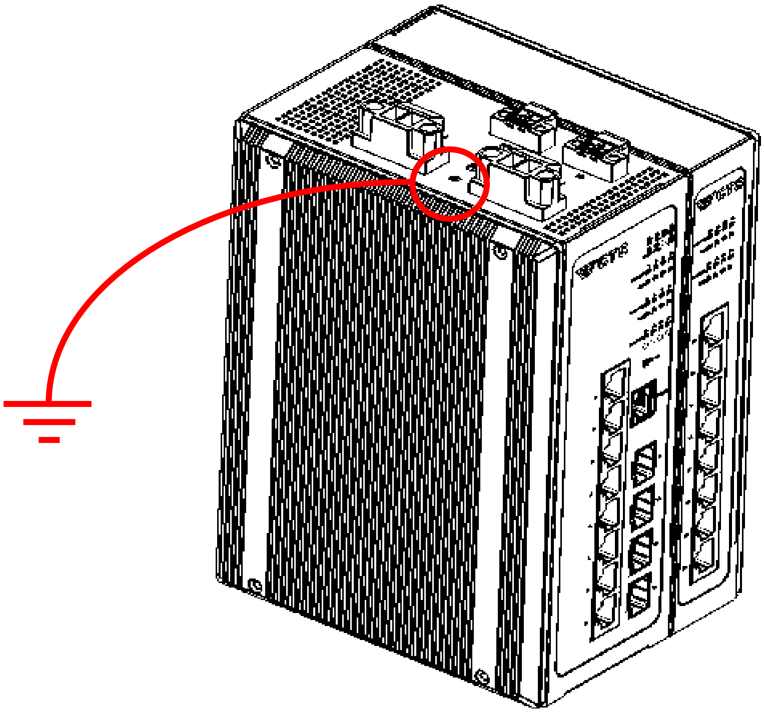


Figure 4. Grounding wiring

2.4 Powering the Managed Industrial PoE Gigabit Ethernet Switch

The Managed Industrial PoE Gigabit Ethernet Switch can be used with DC power 48-54 VDC with the terminal block. The terminal block is located on the upper panel of the Managed Industrial PoE Gigabit Ethernet Switch. Before powering the Managed Industrial PoE Gigabit Ethernet Switch, please make sure that network cables and power cables are securely connected.

ATTENTION

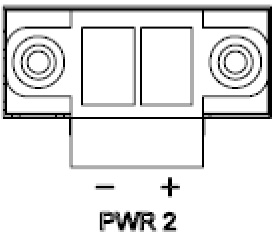
Before connecting the Managed Industrial PoE Gigabit Ethernet Switch to the DC power inputs, make sure the DC power source voltage is stable.

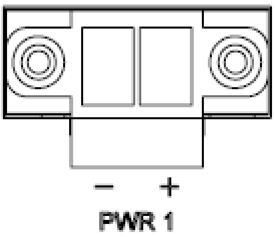
Wiring the terminal blocks

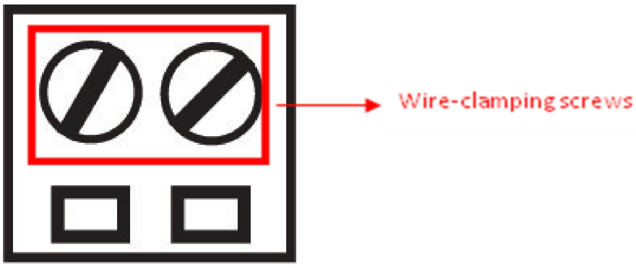
PWR1 and PWR2 (power input) are one pair of contacts on the terminal block. For power redundancy purpose, both the PWR1 and PWR2 need to be configured. The redundant power input will take over seamlessly when one power source is down to protect your device or network from the loss of power.

Power Input Configuration

Insert the positive and negative wires of 12 AWG at least we suggest into the “+” and “-” contacts on the terminal block. PWR1 and PWR2 allow that the power input range is 48~54VDC. Tighten the wire-clamping screws to fix wires of 12 AWG by using a flat-head screwdriver.

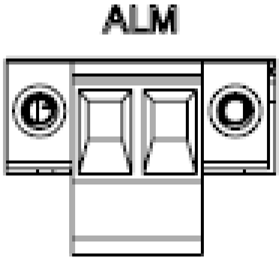






Relay Alarm Output Configuration

Relay alarm has 2 contacts on the terminal block used to connect alarm devices such as speakers or LEDs to alert users when the redundant power or a port link is disconnected. The default contact is normal open, the capacity of relay alarm is 1A/30VDC.

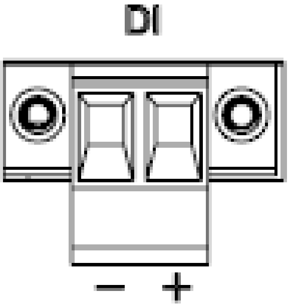


Tighten the wire-clamping screws to fix alarm-device wires by using a flat-head screwdriver as described above.

Digital Input (DI) is a pair of digital input connection on the terminal blocks used to detects if a voltage is above/below a specific threshold.

Digital Input Configuration

Insert the positive and negative wires into the "+" and "-" contact on the terminal blocks. Digital Input allows that the power input range +12~+54VDC for state "1" and -54~+3VDC for state "0". Digital Input also allows maximum input current 18mA.



Tighten the wire-clamping screws to fix the wires by using a flat-head screwdriver as described above.

Note: *If there is no power redundancy, the relay alarm is not available.*

2.5 Connecting the switch to Network

Connect to Network

This Managed Industrial PoE Gigabit Ethernet Switch has 4 uplink ports (SFP) and 8 downlink 10/100/1000Mbps RJ-45 ports for you to implement it in your Industrial PoE environment. All RJ-45 ports can be inserted by 10/100/1000Base-T cables, connecting to the end devices. The fiber port(s) can accept any kind of connector with proper SFP transceiver (mini-GBIC).

2.6 Installing and Removing SFP Modules

2.6.1 Installing SFP Modules

To connect the fiber transceiver and LC cable, use the following guidelines:

1. Position the SFP transceiver with the handle on top.
2. Locate the triangular marking in the slot and align it with the bottom of the transceiver.
3. Insert the SFP transceiver into the slot until it clicks into place.
4. Make sure the module is seated correctly before sliding the module into the slot. A click sounds when it is locked in place.

Note: *If you are attaching fiber optic cables to the transceiver, continue with the following step. Otherwise, repeat the previous steps to install the remaining SFP transceivers in the device.*

1. Remove the protective plug from the SFP transceiver.

Note: *Do not remove the dust plug from the transceiver if you are not installing the fiber optic cable at this time. The dust plug protects hardware from dust contamination.*

2. Insert the fiber cable into the transceiver. The connector snaps into place and locks.

3. Repeat the previous procedures to install any additional SFP transceivers in the switch. The fiber port is now set up.

2.6.2 Removing SFP Modules

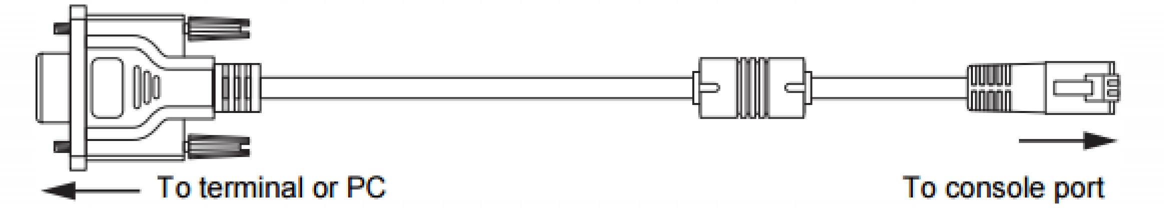
To disconnect an LC connector, use the following guidelines:

1. Press down and hold the locking clips on the upper side of the optic cable.
2. Pull the optic cable out to release it from the transceiver.

3. Hold the handle on the transceiver and pull the transceiver out of the slot.

2.7 Connecting the Switch to Console Port

The industrial switch supports a secondary means of management. By connecting the RJ45 to RS232 serial cable between a COM port on your PC (9-pin D-sub female) and the switch's RJ45 (RJ45) port, a wired connection for management can be established.



3. OPERATION

3.1 LED Definitions

LED	Definition	Color	Operation
P1	Power	Off	Device is powered down.
		Green	Device is powered on.
P2	Power	Off	Device is powered down.
		Green	Device is powered on.
STA	System Status	Orange	System is booting up.
		Green	System is working normally.
		Green Blinking	When upgrade procedure is completed, the Status LED indicator will blink 3 times in green.
		Orange Blinking	When the system is set back to default factory setting, the Status LED indicator will blink 3 times in orange.
			When the system is restarted, the Status LED indicator will blink once in orange.
			System is undergoing upgrading procedure.
ALM	Alarm	Off	Power supplies link up.
		Orange	One of power supplies links down.
Master	Role	Off	The role of switch is slave.
		Green	The role of switch is master.
Ring	Function	Off	Ring Detection is disabled.
		Green	Ring Detection is enabled.
EXP	Expansion Module	Off	Expansion module is not installed.
		Green	Expansion module is installed and runs in good operation.
		Orange	Expansion module is installed, yet runs in abnormal operation.
LINK/ACT 1~20	Port Status	Off	Port link is down
		Orange	Link is up and works at 10/100Mbps.
		Orange Blinking	Receiving and transmitting data.
		Green	Link is up and works at 1000Mbps.
		Green Blinking	Receiving and transmitting data.
PoE 1~8 13~20	Port Status	Off	PoE is disabled.
		Green	PoE is enabled and starts providing power.

4. MAINTENANCE

It is easy to use and maintain this Managed Industrial PoE Gigabit Ethernet Switch. The procedures are suggested when you want to identify faults, perform hardware replacement and firmware upgrading.

4.1 Fault Identification

Identifying faults can greatly reduce the time required to find the problem and solution. Users may perform local or remote checks to find the problems.

Hardware Check

Users can perform local checks by observing LED indicators status.

- When the whole system fails to function,
  - Check Power LED status
  - Check Power connection
  - Reset power

- When certain network link fails to function,
  - Locate the port of the switch
  - Check Port Link Status LED
  - Check cable connection between the port and the connected device
  - Reset power

Software Check

Users may check the Managed Industrial PoE Gigabit Ethernet Switch through SNMP manager remotely. For detailed procedures, please refer to the Network Management User's Manual.

4.2 Hardware Replacement Procedures

ATTENTION

The Managed Industrial PoE Gigabit Ethernet Switch contains no user-serviceable parts. DO NOT, UNDER ANY CIRCUMSTANCES, open and attempt to repair it.

Failure to observe this warning could result in personal injury or death from electrical shock.

Failure to observe the above warning will immediately void any Warranty.

5. Software Overview

Thank you for choosing the Managed Industrial PoE Gigabit Ethernet Switches. The Managed Industrial PoE Gigabit Ethernet Switches are designed to meet the massive needs for Gigabit Ethernet network deployments and aim at Industrial PoE applications that demand wide range of operating temperature. They are fully compliant with IEEE802.3, 802.3u, 802.3ab, 802.3z, 802.1p, 802.1q, 802.3x, 802.3af and 802.3at standards. The built-in management module allows users to configure this Managed Industrial PoE Gigabit Ethernet Switch and monitor the operation status locally or remotely through network.

Besides, redundant power supplies are offered on the Managed Industrial PoE Gigabit Ethernet Switches for users to create a reliable and stable network in the event of power failure. By employing store and forward switching mechanism, the Switch provides low latency and faster data transmission. Moreover, it also supports advanced functions such as VLAN and QoS. Users can configure the required settings of the Switch and monitor its real-time operational status via Command Line Interface (CLI).

5.1 Management Preparations

The Managed Industrial PoE Gigabit Ethernet Switch can be accessed through both Telnet connection and a web browser such as Internet Explorer, Google Chrome or Firefox, etc. Before you can access the Managed Industrial PoE Gigabit Ethernet Switch and configure it, you need to connect cables properly.

5.1.1 Connecting the Managed Industrial PoE Switch

It is extremely important that proper cables are used with correct pin arrangements when connecting the Managed Industrial PoE Gigabit Ethernet Switch to other devices such as switches, hubs, workstations, etc.

- **1000Base-X Fiber Port or 100/1000 Base-X Fiber Port**

  The 1000Base-X fiber port(s) are located at the front panel of the Managed Industrial PoE Gigabit Ethernet Switch. These port(s) are primarily used for uplink connection and can operate at 100/100Mbps or 1000Mbps Full or Half Duplex mode. Duplex SC or WDM Simplex SC types of connectors are available. Use proper multi-mode or single-mode optical fiber cable to connect these port(s) with the other Ethernet Fiber port.

  Before connecting to other switches, workstations or media converters, make sure both sides of the fiber transfer are with the same media type, for example 1000Base-X Single-mode to 1000Base-X Single-mode, 1000Base-X Multi-mode to 1000Base-X Multi-mode. Check that the fiber-optic cable type matches the fiber transfer model. To connect to 1000Base-SX transfer, use the multimode fiber cable (one side must be male duplex SC connector type). To connect to 1000Base-LX transfer, use the single-mode fiber cable (one side must be male duplex LC connector type).

- **10/100/1000Base-T RJ-45 Ports**

  8 10/100/1000Base-T RJ-45 ports are located on the front panel of the Managed Industrial PoE Gigabit Ethernet Switch. These RJ-45 ports allow users to connect their traditional copper-based Ethernet devices to network. All these ports support auto-negotiation and MDI/MDIX auto-crossover, i.e. the crossover or straight through CAT-5 cable may be used.

5.1.2 Assigning IP Addresses

IP addresses have the format n.n.n.n, for example 168.168.8.100.

IP addresses are made up of two parts:

- The first part (168.168.XXX.XXX in the example) indicates network address identifying the network where the device resides. Network addresses are assigned by three allocation organizations. Depending on your location, each allocation organization assigns a globally unique network number to each network that wishes to connect to the Internet.

- The second part (XXX.XXX.8.100 in the example) identifies the device within the network. Assigning unique device numbers is your responsibility. If you are unsure of the IP addresses allocated to you, consult the allocation organization from which your IP addresses were obtained.

Remember that an address can be assigned to only one device on a network. If you connect to the outside, you must change all the arbitrary IP addresses to comply with those you have been allocated by the allocation organization. If you do not do this, your outside communications will not be connected.

A subnet mask is a filtering system for IP addresses. It allows you to further subdivide your network. You must use the proper subnet mask for a proper operation of a network with subnets defined.

6. Command Line Interface (CLI)

This chapter guides you to use Command Line Interface (CLI) via Telnet connection, specifically in:

- Configuring the system
- Resetting the system
- Upgrading newly released firmware

6.1 Remote Console Management-Telnet

You can use Command Line Interface to manage the Managed Industrial PoE Gigabit Ethernet Switch via Telnet session. For first-time users, you must first assign a unique IP address to the Managed Industrial PoE Gigabit Ethernet Switch before you can manage it remotely. Use any one of the RJ-45 ports on the front panel as the temporary management console port to login to the device with the default username & password and then assign the IP address using IP command in Global Configuration Mode.

Follow steps described below to access the Managed Industrial PoE Gigabit Ethernet Switch through Telnet session:

Step 1. Use any one of the RJ-45 ports on the front panel as a temporary management console port to login to the Industrial PoE Managed Gigabit Ethernet Switch.

Step 2. Run Telnet client and connect to *192.168.0.1*. For first-time users, make sure the IP address of your PC or workstation is assigned to an IP address between 192.168.0.2 and 192.168.0.254 with subnet mask 255.255.255.0.

Step 3. When asked for a username, enter "***admin***". When asked for a password, *leave the password field blank* and press Enter (by default, no password is required.)

Step 4. If you enter CLI successfully, the prompt display *Switch*> (the model name of your device together with a greater than sign) will appear on the screen.

Step 5. Once you enter CLI successfully, you can set up the Switch's IP address, subnet mask and the default gateway using "IP" command in Global Configuration Mode. The telnet session will be terminated immediately once the IP address of the Switch has been changed.

Step 6. Use new IP address to login to the Managed Industrial PoE Gigabit Ethernet Switch via Telnet session again.

Limitation: Only one active Telnet session can access the Managed Industrial PoE Gigabit Ethernet Switch at a time.

6.2 Navigating CLI

After you successfully access to the Managed Industrial PoE Gigabit Ethernet Switch, you will be asked for a login username. Enter your authorized username and password, and then you will be directed to User Mode. In CLI management, User Mode only provides users with basic functions to operate the Managed Industrial PoE Gigabit Ethernet Switch. If you would like to configure advanced features of the Managed Industrial PoE Gigabit Ethernet Switch, such as VLAN and QoS, you must enter Configuration Mode. The following table provides an overview of modes available in this Managed Industrial PoE Gigabit Ethernet Switch.

Command Mode	Access Method	Prompt Displayed	Exit Method
User Mode	Login username & password	IPS-3112-PoE++>	logout
Privileged Mode	From User Mode, enter the *enable* command	IPS-3112-PoE++#	disable, exit, logout
Configuration Mode	From Privileged Mode, enter the *config* or *configure* command	IPS-3112-PoE++(config)#	exit

NOTE: *By default, the model name will be used for the prompt display. For convenience, the prompt display "Switch" will be used throughout this user's manual.*

6.2.1 General Commands

This section introduces you some general commands that you can use in all modes, including "help", "exit", "history" and "logout".

Entering the command…	To do this…	Available Modes
help	Obtain a list of available commands in the current mode.	User Mode Privileged Mode Configuration Mode
exit	Return to the previous mode or login screen.	User Mode Privileged Mode Configuration Mode
history	List all commands that have been used.	User Mode Privileged Mode Configuration Mode
logout	Logout from the CLI or terminate Telnet session.	User Mode Privileged Mode

6.2.2 Quick Keys

In CLI, there are several quick keys that you can use to perform several functions. The following table summarizes the most frequently used quick keys in CLI.

Keys	Purpose
tab	Enter an unfinished command and press “Tab” key to complete the command.
?	Press “?” key in each mode to get available commands.

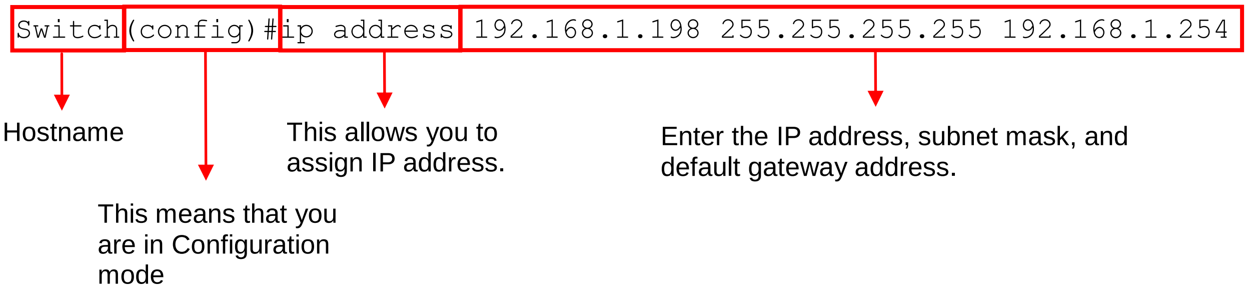
Unfinished command followed by ?	Enter an unfinished command or keyword and press “?” key to complete the command and get command syntax help.
	
	Examples:
	`Switch#h?`
	`help        Show available commands`
	`history     Show history commands`

Up arrow	Use Up arrow key to scroll through the previous entered commands, beginning with the most recent key-in commands.
Down arrow	Use Down arrow key to scroll through the previous entered commands, beginning with the commands that are entered first.

6.2.3 Command Format

While in CLI, you will see several symbols often. As mentioned above, you might already know what “>”, “#” and (config)# represent. However, to perform what the device is intended to do, you have to enter a string of complete command correctly. For example, if you want to assign IP address for the Managed Industrial PoE Gigabit Ethernet Switch, you need to enter the following command with the required parameter and IP, subnet mask and default gateway:

IP command syntax: `Switch(config)#ip address [A.B.C.D] [255.X.X.X] [A.B.C.D]`



```
Switch(config)#ip address 192.168.1.198 255.255.255.255 192.168.1.254
```

Hostname
This allows you to assign IP address.
Enter the IP address, subnet mask, and default gateway address.
This means that you are in Configuration mode

The following table lists common symbols and syntax that you will see frequently in this User's Manual for your reference:

Symbols	Brief Description
>	Currently, the device is in User Mode.
#	Currently, the device is in Privileged Mode.
(config)#	Currently, the device is in Configuration Mode.
Syntax	**Brief Description**
[ ]	Brackets mean that this field is required information.
[A.B.C.D]	Brackets represent that this is a required field. Enter an IP address or gateway address.
[255.X.X.X]	Brackets represent that this is a required field. Enter the subnet mask.
[port-based | 802.1p | dscp | vid]	There are four options that you can choose. Specify one of them.
[1-8191]	Specify a value between 1 and 8191.

[0-7] 802.1p_list
[0-63] dscp_list
	Specify one value, more than one values or a range of values.
	Example 1: specifying one value
	`Switch(config)#qos 802.1p-map 1 0`
	`Switch(config)#qos dscp-map 10 3`
	Example 2: specifying more than one values (separated by commas)
	`Switch(config)#qos 802.1p-map 1,3 0`
	`Switch(config)#qos dscp-map 10,13,15 3`
	Example 3: specifying a range of values (separating by a hyphen)
	`Switch(config)#qos 802.1p-map 1-3 0`
	`Switch(config)#qos dscp-map 10-15 3`

6.2.4 Login Username & Password

Default Login

After you enter Telnet session, a login prompt will appear to request a valid and authorized username and password combination. For first-time users, enter the default login username "**admin**" and "**press Enter key**" in password field (no password is required for default setting). When system prompt shows "Switch>", it means that the user has successfully entered User mode.

For security reasons, it is strongly recommended that you add a new login username and password using User command in Configuration mode. When you create your own login username and password, you can delete the default username (admin) to prevent unauthorized accesses.

Forgot Your Login Username & Password?

If you forgot your login username and password, you can use the "reset button" to set all configurations back to factory defaults. Once you have performed system setting to defaults, you can login with default username and password. Please note that if you use this method to gain access to the Managed Industrial PoE Gigabit Ethernet Switch, all configurations saved in Flash will be lost. It is strongly recommended that a copy of configurations is backed up in your local hard-drive or file server from time to time so that previously-configured settings can be restored to the Managed Industrial PoE Gigabit Ethernet Switch for use after you gain access again to the device.

6.3 User Mode

In User mode, only a limited set of commands is provided. Please note that in Use mode, you have no authority to configure advanced settings. You need to enter Privileged mode or Configuration mode to set up advanced functions of a switch feature. For a list of commands available in User mode, enter the question mark (?) or "help" command after the system prompt displays "Switch>".

Command	Description
exit	Quit User mode and close the terminal connection.
help	Display a list of available commands in User mode.
history	Display the command history.
logout	Logout from the Managed Industrial PoE Gigabit Ethernet Switch.
enable	Enter Privileged mode.

6.4 Privileged Mode

The only place where you can enter Privileged (Enable) mode is User mode. When you successfully enter Enable mode, the prompt will be changed to Switch# (the model name of your device together with a pound sign). Enter the question mark (?) or help command to view a list of commands available for use.

Command	Description
copy-cfg	Restore or backup configuration file.
disable	Exit Enable mode and return to User mode
exit	Exit Enable mode and return to User mode.
firmware	Upgrade Firmware via FTP or TFTP server.
help	Display a list of available commands in Enable mode.
history	Show commands that have been used.
logout	Logout from the Managed Industrial PoE Gigabit Ethernet Switch.
reload	Restart the Managed Industrial PoE Gigabit Ethernet Switch.
traceroute	Set up traceroute command
write	Save the current configurations to Flash.
configure	Enter Global Configuration mode
show	Display the system information.

6.4.1 Copy-cfg Command

Use the “copy-cfg” command to restore the Managed Industrial PoE Gigabit Ethernet Switch back to the defaults or to the defaults without changing IP configurations, backup a configuration file to FTP or TFTP server, or restore a configuration file via FTP or TFTP server.

1. To restore a configuration file via FTP or TFTP server:

Command	Parameter	Description
Switch# copy-cfg from ftp [A.B.C.D] [file name] [user_name] [password]	[A.B.C.D]	Enter the IP address of your FTP server.
	[file_name]	Enter the configuration file name that you want to restore.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
Switch# copy-cfg from tftp [A.B.C.D] [file_name]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file_name]	Enter the configuration file name that you want to restore.
Example		
Switch# copy-cfg from ftp 192.168.1.198 HS_0600_file.conf misadmin1 abcxyz		
Switch# copy-cfg from tftp 192.168.1.198 HS_0600_file.conf		

2. **To restore the Managed Industrial PoE Gigabit Ethernet Switch back to default settings:**

Command / Example
Switch# copy-cfg from default

NOTE: *There are two ways to set the Managed Industrial PoE Gigabit Ethernet Switch back to the factory default settings. Users can use the "copy-cfg from default" command in CLI or simply press the "Reset Button" located on the front panel to restore the device back to the initial state.*

3. **To restore the Managed Industrial PoE Ethernet Switch back to default settings except the network setting:**

Command / Example
Switch# copy-cfg from default keep-ip

4. **To backup a configuration file to FTP or TFTP server:**

Command	Parameter	Description
Switch# copy-cfg to ftp [A.B.C.D] [file_name] [user_name] [password]	[A.B.C.D]	Enter the IP address of your FTP server.
	[file_name]	Enter the configuration file name that you want to backup.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
Switch# copy-cfg to tftp [A.B.C.D] [file_name]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file_name]	Enter the configuration file name that you want to backup.
Example		
Switch# copy-cfg to ftp 192.168.1.198 HS_0600_file.conf misadmin1 abcxyz		
Switch# copy-cfg to tftp 192.168.1.198 HS_0600_file.conf		

6.4.2 Firmware Command

To upgrade the firmware via FTP or TFTP server, use the "firmware" command.

Command	Parameter	Description
Switch# firmware upgrade ftp [A.B.C.D] [file_name] [user_name] [password]	[A.B.C.D]	Enter the IP address of your FTP server.
	[file_name]	Enter the firmware file name that you want to upgrade.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.

Switch# firmware upgrade tftp [A.B.C.D] [file_name]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file_name]	Enter the firmware file name that you want to upgrade.
Example		
Switch# firmware upgrade ftp 192.168.1.198 HS_0600_file.bin edgeswitch10 abcxyz		
Switch# firmware upgrade tftp 192.168.1.198 HS_0600_file.bin		

6.4.3 Reload Command

To restart the Managed Industrial PoE Gigabit Ethernet Switch by image 1 or 2, use the “reload” command.

Command / Example
Switch# reload image-1
Switch# reload image-2

6.4.4 Traceroute Command

Traceroute is used to trace the path between the local host and the remote host. Enter the **traceroute** command in User mode. In this command, you can add an optional max hops value for the number of hops that packets are sent and received.

Command	Parameter	Description
Switch> traceroute [A.B.C.D] [-h (1-100)hops]	[A.B.C.D]	Enter the IP address that you would like to ping.
	[-h (1-100)hops]	Specify max hops between the local host and the remote host
Example		
Switch> traceroute 8.8.8.8 Switch> traceroute 8.8.8.8 –h 30		

6.4.5 Write Command

To save running configurations to startup configurations, use the “write” command. All unsaved configurations will be lost when you restart the Managed Industrial PoE Gigabit Ethernet Switch.

Command / Example
Switch# write

6.4.6 Configure Command

You can enter Configuration mode only from Privileged mode. You can type in “configure” or “config” to enter Configuration mode. The display prompt will change from “Switch#” to “Switch(config)#” once you successfully enter Configuration mode.

Command / Example
Switch# config Switch(config)#
Switch# configure Switch(config)#

6.5 Global Configuration Mode

When you enter “configure” or “config” and press “Enter” in Privileged mode, you will be directed to Global Configuration mode where you can set up advanced switching functions, such as QoS and VLAN. Any command entered will be applied to the running-configuration and device’s operation. From this level, you can also enter different sub-configuration modes to set up specific configurations for VLAN, QoS or interfaces.

Command	Description
dot1x	IEEE 802.1X global configuration commands
exit	Exit from Global Configuration mode.
help	Display a list of available commands.
history	Show commands that have been used.
ip	Global IP configuration commands
mac	Global MAC configuration commands
management	Manage the interface configuration.
ntp	Set up required configurations for Network Time Protocol.
qos	Set up the priority of packets within the Managed Industrial PoE Switch.
snmp-server	Create a new SNMP community and trap destination and specify the trap types.
switch	Switch Global configuration commands
switch-info	Switch information configuration commands
syslog	Set up required configurations for Syslog server.
ring-detection	Set up Ring Detection commands.
time-range	Set up a specific period of time for an event.
user	User Account management
vlan	Set up VLAN mode and VLAN configuration.
no	Negate a command or set it back to its default setting.
interface	Select one or a range of interfaces to configure.

show	Display the system information.

6.5.1 Entering Interface Numbers

In Configuration mode, you can configure a command that is only applied to designated interfaces. For example, you can set up each interface's VLAN assignment, speed, or duplex mode. For configuring, you must first enter the interface number. There are four ways to enter your interface numbers to signify the combination of different interfaces that apply to a command or commands.

Commands	Description
Switch(config)# interface 1 Switch(config-if-1)#	Enter a single interface. Only interface 1 will apply to commands entered.
Switch(config)# interface 1,3,5 Switch(config-if-1,3,5)#	Enter three discontinuous interfaces, separating by a comma. Interface 1, 3, 5 will apply to commands entered.
Switch(config)# interface 1-3 Switch(config-if-1-3)#	Enter three continuous interfaces. Use a hyphen to signify a range of interface numbers. In this example, interface 1, 2, and 3 will apply to commands entered.
Switch(config)# interface 1,3-5 Switch(config-if-1,3-5)#	Enter a single interface number together with a range of interface numbers. Use both commas and hyphens to signify the combination of different interface numbers. In this example, interface 1, 3, 4, 5 will apply to commands entered.

The "interface" command can be used together with "QoS", "VLAN" and "Security" commands. For detailed usages, please refer to QoS, VLAN and Security sections below.

6.5.2 No Command

Most commands that you enter in Configuration mode can be negated by "no" command following the same or original command. The purpose of "no" command is to disable a function, remove a command, or configure the setting back to the default value. In each sub-section below, the use of no command to fulfill different purposes will be introduced.

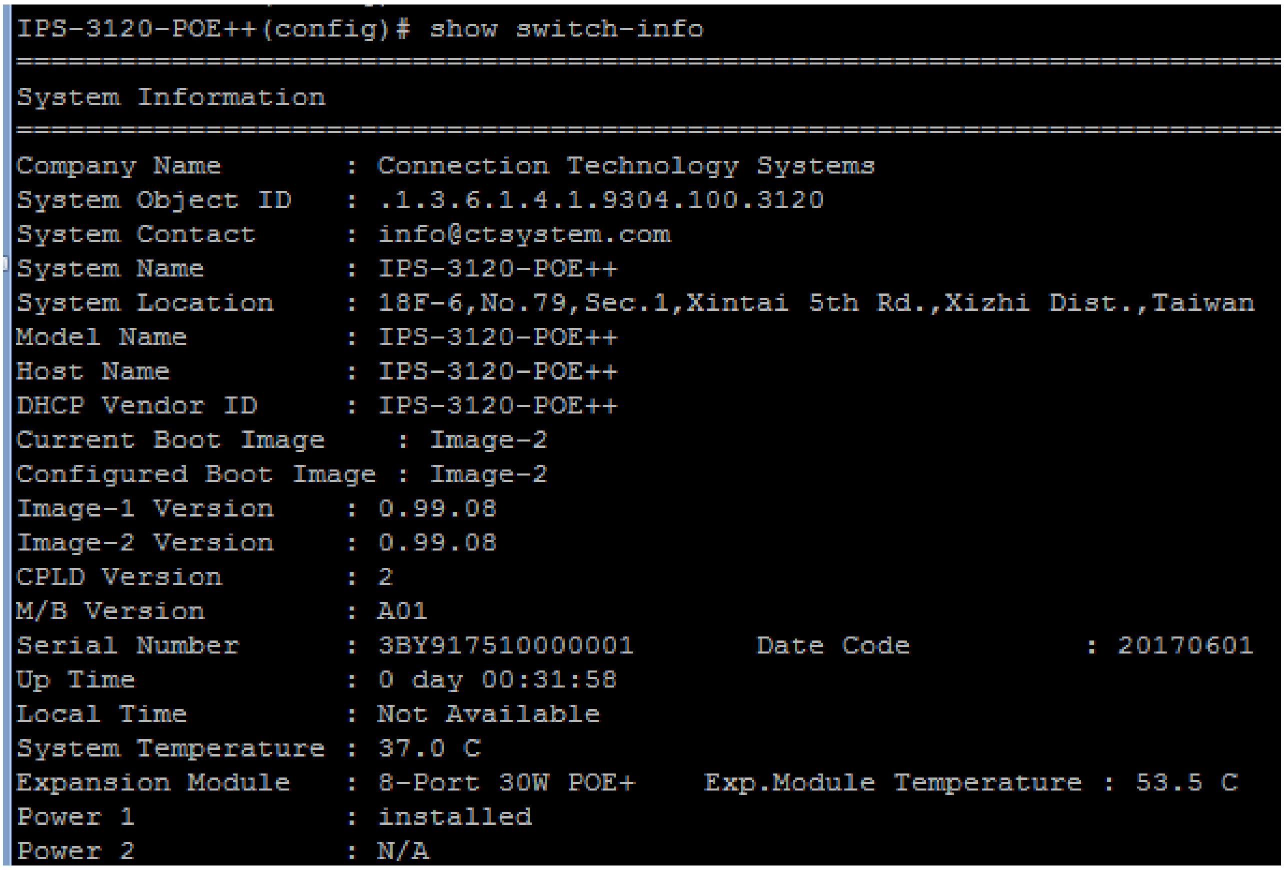
6.5.3 Show Command

The "show" command is very important for network administrators to get information about the device, receive outputs to verify a command's configurations, or troubleshoot a network configuration error. The show command can be used in Privileged or Configuration mode. Different uses of the show command are described as below:

Commands	Description
Switch(config)# show default-config	Show system default configuration.
Switch(config)# show dot1x	Show IEEE 802.1x information.
Switch(config)# show ethernet	Show Ethernet Information.
Switch(config)# show interface	Show interface information.
Switch(config)# show ip	Show IP information.
Switch(config)# show log	Show log information.
Switch(config)# show mac	Show MAC information.
Switch(config)# show management	Show management information.
Switch(config)# show ntp	Show NTP information.
Switch(config)# show poe	Show POE information.
Switch(config)# show qos	Show QoS information.
Switch(config)# show running-config	Show running configuration.
Switch(config)# show sfp	Show SFP information.
Switch(config)# show snmp-server	Show SNMP server information.
Switch(config)# show start-up-config	Show system start up configuration.
Switch(config)# show switch	Show switch configuration.
Switch(config)# show switch-info	Show switch information.
Switch(config)# show syslog	Show syslog configuration.
Switch(config)# show ring-detection	Show ring detection configuration.
Switch(config)# show time-range	Show time range information.
Switch(config)# show user	Show user account configuration.
Switch(config)# show vlan	Show VLAN information.

1. Displaying system information

Enter the “show switch-info” command in Privileged or Configuration mode, and then the following similar screen page will appear.



```
IPS-3120-POE++(config)# show switch-info
==========================================================================
System Information
==========================================================================
Company Name        : Connection Technology Systems
System Object ID    : .1.3.6.1.4.1.9304.100.3120
System Contact      : info@ctsystem.com
System Name         : IPS-3120-POE++
System Location     : 18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan
Model Name          : IPS-3120-POE++
Host Name           : IPS-3120-POE++
DHCP Vendor ID      : IPS-3120-POE++
Current Boot Image     : Image-2
Configured Boot Image : Image-2
Image-1 Version     : 0.99.08
Image-2 Version     : 0.99.08
CPLD Version        : 2
M/B Version         : A01
Serial Number       : 3BY917510000001       Date Code          : 20170601
Up Time             : 0 day 00:31:58
Local Time          : Not Available
System Temperature : 37.0 C
Expansion Module    : 8-Port 30W POE+    Exp.Module Temperature : 53.5 C
Power 1             : installed
Power 2             : N/A
```

Company Name: Display a company name for this Managed Industrial PoE Gigabit Ethernet Switch. Use the “switch-info company-name [company-name]” command to edit this field.

System Object ID: Display the predefined System OID.

System Contact: Display the contact information for this Managed Industrial PoE Gigabit Ethernet Switch. Use the “switch-info sys-contact [sys-contact]” command to edit this field.

System Name: Display a descriptive system name for this Managed Industrial PoE Gigabit Ethernet Switch. Use the “switch-info sys-name [sys-name]” command to edit this field.

System Location: Display a brief location description for this Manage Industrial PoE Gigabit Ethernet Switch. Use the “switch-info sys-location [sys-location]” command to edit this field.

Model Name: Display the model name of the device.

Host Name: Display the host name of the device.

DHCP Vendor ID: Display the DHCP Vendor ID of the device.

Current Boot Image: Display the image in use.

Configured Boot Image: Display the image which would be used after rebooting.

Image-1 Version: Display the firmware version used in image-1.

Image-2 Version: Display the firmware version used in image-2.

M/B Version: Display the main board version.

1000M Port Number: Display the number of ports transmitting at the speed of 1000Mbps

100M Port Number: Display the number of ports transmitting at the speed of 100Mbps

WAN Fiber Type: Display the information about the slide-in fiber type.

WAN Fiber Vendor: Display the vendor of the slide-in fiber.

WAN Fiber PN: Display the PN of the slide-in fiber.

Fiber 2 Type*: Display the information about the slide-in fiber type.

Fiber 2 Vendor*: Display the vendor of the slide-in fiber.

Fiber 2 PN*: Displays the PN of the slide-in fiber.

Serial Number: Display the serial number of this Managed Industrial PoE Gigabit Ethernet Switch.

Date Code: Displays the Managed Industrial PoE Gigabit Ethernet Switch Firmware date code.

Uptime: Display the time the device has been up.

Local Time: Display the time of the location where the switch is.

CPU Temperature: Display the current temperature of the CPU.

PHY1 Temperature: A PHY connects a link layer device to a physical medium such as an copper cable optical fiber. View-only field that shows the PHY 1's temperature.

PHY2 Temperature: View-only field that shows the PHY 2's temperature.

PHY3 Temperature: View-only field that shows the PHY 3's temperature.

SWITCH Temperature: Display the current temperature of the device.

POWER Temperature: Display the current temperature of the power in use.

Power 1: Display the status of power A.

Power 2: Display the status of power B.

***Fiber 2 information for 2-fiber model only**

2. Displaying or verifying currently-configured settings

Please refer to “interface command”, “ip command”, “mac command”, “qos command”, “user command”, and “vlan command” sections.

3. Displaying the interface information or statistics

Please refer to “show interface command” and “show sfp information command” sections.

4. Showing default, running and startup configurations

Please refer to “show default-config command”, “show running-config command” and “show start-up-config command” sections.

6.5.4 Channel-group Command

1. Configuring a static link aggregation group (LAG)

Command	Parameter	Description
Switch(config)# channel-group trunking [group_name]	[group_name]	Specify a name for the link aggregation group.
Switch(config)# interface [port_list] Switch(config-if-PORT-PORT)# channel-group trunking [group_name]	[port_list] [group_name]	Use the “interface” command and enter several discontinuous port numbers to assign the selected ports to the specified link aggregation group.
No command		
Switch(config)# no channel-group trunking [group_name]	[group_name]	Delete a link aggregation group.
Switch(config)# interface [port_list] Switch(config-if-PORT-PORT)# no channel-group trunking	[port_list]	Remove the selected ports from a link aggregation group.
Show command		
Switch(config)# show channel-group trunking		Show or verify link aggregation settings including aggregated port numbers and load-balancing status.
Switch(config)# show channel-group trunking [group_name]	[group_name]	Show or verify a specific link aggregation group’s settings including port numbers and load-balancing status.
Example		
Switch(config)# channel-group trunking corenetwork		Create a link aggregation group called “corenetwork”.
Switch(config)# interface 1,2,3 Switch(config-if-1-3)#channel-group trunking corenetwork		Assign port 1, 2 and 3 to the link aggregation group “corenetwork”.

2. Use “Interface” command to configure link aggregation groups dynamically (LACP).

Channel-group & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# channel-group lacp		Enable LACP on the selected interfaces. The Managed Switch supports dynamic Link Aggregation Control Protocol (LACP) which is specified in IEEE 802.3ad. Static trunks have to be manually configured at both ends of the link. In other words, LACP configured ports can automatically negotiate a trunked link with LACP configured ports on other devices. You can configure any number of ports on the Managed Switch as LACP, as long as they are not already configured as part of a static trunk. If ports on other devices are also configured as LACP, the Managed Switch and the other devices will negotiate a trunk link between them. If an LACP trunk consists of more than four ports, all other ports will be placed in a standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.
Switch(config-if-PORT-PORT)# channel-group lacp key [0-255]	[0-255]	Specify a key to the selected interfaces. Ports in an aggregated link group must have the same LACP port Key. In order to allow a port to join an aggregated group, the port Key must be set to the same value. The range of key value is between 0 and 255. When key value is set to 0, the port Key is automatically set by the Managed Switch.
Switch(config-if-PORT-PORT)# channel-group lacp type [active]	[active]	Specify the selected interfaces to active LACP role. **“Active” Port Role:** Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so that

		the group may be changed dynamically as required. In order to utilize the ability to change an aggregated port group, that is, to add or remove ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP. **"Passive" Port Role:** LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports.
No command		
Switch(config-if-PORT-PORT)# no channel-group lacp		Disable LACP on the selected interfaces.
Switch(config-if-PORT-PORT)# no channel-group lacp key		Reset the key value of the selected interfaces to the factory default.
Switch(config-if-PORT-PORT)# no channel-group lacp role		Reset the LACP type of the selected interfaces to the factory default (passive mode).
Show command		
Switch(config)# show channel-group lacp		Show or verify each interface's LACP settings including current mode, key value and LACP type.
Switch(config)# show channel-group lacp [port_list]	[port_list]	Show or verify the selected interfaces' LACP settings.
Switch(config)# show channel-group lacp status		Show or verify each interface's current LACP status.
Switch(config)# show channel-group lacp status [port_list]	[port_list]	Show or verify the selected interfaces' current LACP status.
Switch(config)# show channel-group lacp statistics		Show or verify each interface's current LACP traffic statistics.
Switch(config)# show channel-group lacp statistics [port_list]	[port_list]	Show or verify the selected interfaces' current LACP statistics.
Switch(config)# show channel-group lacp statistics clear		Clear all LACP statistics.
Channel-group & interface command example		
Switch(config)# interface 1-3		Enter port 1 to port 3's interface mode.
Switch(config-if-1-3)# channel-group lacp		Enable LACP on the selected interfaces.
Switch(config-if-1-3)# channel-group lacp key 10		Set a key value "10" to the selected interfaces.
Switch(config-if-1-3)# channel-group lacp role		Set the selected interfaces to active

active	LACP type.

6.5.5 Dot1X Command

Command	Parameter	Description
Switch(config)# dot1x		Enable dot1x function. When enabled, the Managed Switch acts as a proxy between the 802.1X-enabled client and the authentication server. In other words, the Managed Switch requests identifying information from the client, verifies that information with the authentication server, and relays the response to the client.
Switch(config)# dot1x radius-assigned vlan		Globally enable to allow the Radius server to use the following tunnel attributes for port's VLAN assignment after successful authentication: Tunnel-Type=VLAN(13), Tunnel-Medium-Type=802, Tunnel-Private-Group-ID=VLANID.
Switch(config)# dot1x reauthentication		Enable re-authentication function.
Switch(config)# dot1x reauth-period [0-3600]	[0-3600]	Specify a period of authentication time that a client authenticates with the authentication server. The allowable value is between 0 and 3600 seconds.
Switch(config)# dot1x secret [shared_secret]	[shared_secret]	Specify a shared secret of up to 30 characters. This is the identification word or number assigned to each RADIUS authentication server with which the client shares a secret.
Switch(config)# dot1x server [A.B.C.D]	[A.B.C.D]	Specify the RADIUS Authentication server IP address.
No command		
Switch(config)# no dot1x		Disable IEEE 802.1x function.
Switch(config)# no dot1x reauth-period		Reset the re-authentication period value back to the default setting (60 seconds).
Switch(config)# no dot1x reauthentication		Disable re-authentication function.
Switch(config)# no dot1x secret		Remove the original shared secret.

Switch(config)# no dot1x server		Remove the specified server IP address.
Switch(config)# no dot1x timeout		Reset the timeout value back to the default setting (10 seconds).
Show command		
Switch(config)# show dot1x		Show or verify 802.1x settings.
Switch(config)# show dot1x interface		Show or verify each interface’s 802.1x settings including port status and authentication status.
Switch(config)# show dot1x interface [port_list]	[port_list]	Show or verify the selected interfaces’ 802.1x settings including port status and authentication status.
Switch(config)# show dot1x statistics		Show or verify 802.1x statistics.
Switch(config)# show dot1x statistics [port_list]	[port_list]	Show or verify the selected interfaces’ statistics.
Switch(config)# show dot1x status		Show or verify 802.1x status.
Switch(config)# show dot1x status [port_list]	[port_list]	Show or verify the selected interfaces’ 802.1x status.
Dot1x command example		
Switch(config)# dot1x		Enable IEEE 802.1x function.
Switch(config)# dot1x reauth-period 3600		Set the reauthentication period to 3600 seconds.
Switch(config)# dot1x reauthentication		Enable re-authentication function.
Switch(config)# dot1x secret agagabcxyz		Set the shared secret to “agagabcxyz”
Switch(config)# dot1x server 192.168.1.10		Set the 802.1x server IP address to 192.168.1.10.
Switch(config)# dot1x timeout 120		Set the timeout value to 120 seconds.

Use “Interface” command to configure a group of ports’ IEEE 802.1x settings.

Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# dot1x mab		MAC-Authentication Bypass (MAB) is commonly used for devices, such as VoIP phones and Ethernet printers, that do not support the 802.1x protocol. This method allows such devices to be authenticated using the same database infrastructure as that

		used in 802.1x. 1. The device connects to a switch port. 2. The switch learns the device MAC address upon receiving the first frame from the device (the device usually sends out a DHCP request message when first connected). 3. The switch sends an EAP Request message to the device, attempting to start 802.1X authentication. 4. The switch times out while waiting for the EAP reply, because the device does not support 802.1x. 5. The switch sends an authentication message to the authentication server, using the device MAC address as the username and password. 6. The switch authenticates or rejects the device according to the reply from the authentication server. Enable to activate MAB function.
Switch(config-if-PORT-PORT)# dot1x max-req [1-10]	[1-10]	Specify the maximum times the request should be sent. The connected client will be authenticated using MAB if the switch has tried the specified times and receive no EAP reply from the device.
Switch(config-if-PORT-PORT)# dot1x port-control [auto | authorized | unauthorized]		Specify the selected ports to "auto" or "unauthorized". **"auto":** This requires 802.1X-aware clients to be authorized by the authentication server. Accesses from clients that are not dot1x aware will be denied. **"authorized":** This forces the Managed Switch to grant access to all clients, either 802.1X-aware or 802.1x-unaware. No authentication exchange is required. By default, all ports are set to "authorized".

		“unauthorized”: This forces the Managed Switch to deny access to all clients, neither 802.1X-aware nor 802.1X-unaware.
Switch(config)# dot1x radius-assigned vlan		Globally enable to allow the Radius server to use the following tunnel attributes for port’s VLAN assignment after successful authentication: Tunnel-Type=VLAN(13), Tunnel-Medium-Type=802, Tunnel-Private-Group-ID=VLANID.
Switch(config-if-PORT-PORT)# dot1x reauthenticate		Re-authenticate the selected interfaces immediately.
Switch(config-if-PORT-PORT)# dot1x reauthentication		Enable periodic Reauthentication.
Switch(config-if-PORT-PORT)# dot1x timeout [1-255]	[1-255]	Specify the time value in seconds. The Managed Switch will wait for a period of time for the response from the authentication server to an authentication request before it times out. The allowable value is between 1 and 255 seconds.
No command		
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# no dot1x port-control		Reset the selected interfaces’ 802.1x state to the factory default (authorized state).
Show command		
Switch(config)# show dot1x		Show or verify 802.1x settings.
Switch(config)# show dot1x interface		Show or verify each interface’s 802.1x settings including port status and authentication status.
Switch(config)# show dot1x interface [port_list]	[port_list]	Show or verify the selected interfaces’ 802.1x settings including port status and authentication status.
Switch(config)# show dot1x statistics		Show or verify 802.1x statistics.
Switch(config)# show dot1x statistics [port_list]	[port_list]	Show or verify the selected interfaces’ statistics.

Switch(config)# show dot1x status		Show or verify 802.1x status.
Switch(config)# show dot1x status [port_list]	[port_list]	Show or verify the selected interfaces' 802.1x status.
Dot1x & interface command example		
Switch(config)# interface 1-3		Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-1-3)# dot1x port-control auto		Set the selected ports to "auto" state.
Switch(config-if-1-3)# dot1x reauthenticate		Re-authenticate the selected interfaces immediately.

6.5.6 IP Command

1. To set up or remove the IP address of the Managed Industrial PoE Switch:

IP command	Parameter	Description
Switch(config)# ip address [A.B.C.D] [255.X.X.X] [A.B.C.D]	[A.B.C.D]	Enter the desired IP address for the Managed Industrial PoE Ethernet Switch.
	[255.X.X.X]	Enter subnet mask of your IP address.
	[A.B.C.D]	Enter the default gateway address.
No command		
Switch(config)# no ip address		Remove the configured IP settings and set back to defaults.
Show command		
Switch(config)# show ip address		Show the current IP configurations or verify the configured IP settings.
IP command example		
Switch(config)# ip address 192.168.1.198 255.255.255.0 192.168.1.254		Set up the Switch's IP to 192.168.1.198, subnet mask to 255.255.255.0, and default gateway to 192.168.1.254.

2. To enable the Managed Industrial PoE Switch to automatically get IP address from the DHCP server:

Command / Example	Description
Switch(config)# ip address dhcp	Enable DHCP mode.
No command	
Switch(config)# no ip address dhcp	Disable DHCP mode.
Show command	
Switch(config)# show ip address	Show the current IP configurations or verify the configured IP settings.

3. Enable or disable IGMP/MLD snooping globally.

IGMP, Internet Group Management Protocol, is a communication protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It can be used for online streaming video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 packets IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch it analyses all the IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the multicast list for that group. And, when the switch hears an IGMP Leave, it removes the host's port from the table entry.

IGMP snooping can very effectively reduce multicast traffic from streaming and other bandwidth intensive IP applications. A switch using IGMP snooping will only forward multicast traffic to the hosts interested in that traffic. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also reduces the workload at the end hosts since their network cards (or operating system) will not have to receive and filter all the multicast traffic generated in the network.

Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4.

Command / Example	Parameter	Description
Switch(config)# ip igmp snooping		When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic. This is for IGMPv1,v2 and MLDv1 only.
Switch(config)# ip igmp snooping version-3		When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic. This is for IGMPv3 and MLDv2 only.
Switch(config)# ip igmp snooping flooding		Set forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic will flood when enabled. However, the traffic will forward to router-ports only when disabled.
Switch(config)# ip igmp snooping immediate-leave		Enable immediate leave function.
Switch(config)# ip igmp snooping max-response-time [1-255] (1/10secs)	[1-255] (1/10secs)	Specify the maximum response time. This determines the maximum amount of time allowed before sending an IGMP/MLD

		response report.
Switch(config)# ip igmp snooping mcast-router [port_list]	[port_list]	Specify multicast router ports.
Switch(config)# ip igmp snooping query-interval [1-6000] secs	[1-6000]	Specify Query time interval. This is used to set the time interval between transmitting IGMP/MLD queries.
Switch(config)# ip igmp snooping vlan [1-4094]	[1-4094]	Specify a VLAN ID. This enables IGMP/MLD Snooping on a specified VLAN.
Switch(config)# ip igmp snooping vlan [1-4094] query	[1-4094]	Enable a querier on the specified VLAN.
No command		
Switch(config)# no ip igmp snooping		Disable IGMP/MLD Snooping function.
Switch(config)# no ip igmp snooping flooding		Disable flooding function. Traffic will forward to router-ports only when disabled.
Switch(config)# no ip igmp snooping immediate-leave		Disable immediate leave function.
Switch(config)# no ip igmp snooping max-response-time		Reset maximum response time back to the factory default.
Switch(config)# no ip igmp snooping mcast-router [port_list]	[port_list]	Remove the selected ports from the router port list.
Switch(config)# no ip igmp snooping query-interval		Reset Query interval value back to the factory default.
Switch(config)# no ip igmp snooping vlan [1-4094]	[1-4094]	Disable IGMP/MLD Snooping on the specified VLAN.
Switch(config)# no ip igmp snooping vlan [1-4094] query	[1-4094]	Disable a querier on the specified VLAN.
Show command		
Switch(config)#show ip igmp snooping		Show current IGMP/MLD snooping status including immediate leave function.
Switch(config)#show ip igmp snooping groups		Show IGMP/MLD group table.
Switch(config)#show ip igmp snooping status		Show IGMP/MLD Snooping status.

Configure IGMP Filtering policies.

IGMP Filtering command	Parameter	Description
Switch(config)# ip igmp filter		Enable IGMP Filtering function.
Switch(config)# ip igmp profile [profile_name]	[profile_name]	Specify a name for this profile.
Switch(config-profile-ID)# segment [1-400]	[1-400]	Specify an existing segment ID.
Switch(config)# ip igmp segment [1-400]	[1-400]	Specify a segment ID.

Switch(config-segment-ID)# name [segment_name]	[segment_name]	Specify a name for this segment.
Switch(config-segment-ID)# range [E.F.G.H] [E.F.G.H]	[E.F.G.H] [E.F.G.H]	Specify a multicast IP range.
No command		
Switch(config)# no ip igmp filter		Disable IGMP Filtering function.
Switch(config)# no ip igmp segment [1-400]	[1-400]	Delete the specified segment. Only the segment that does not belong to any profiles can be deleted.
Switch(config)# no ip igmp profile [profile_name]	[profile_name]	Delete the specified profile.
Show command		
Switch(config)# show ip igmp filter		Show IGMP Filtering setting.
Switch(config)# show ip igmp filter interface [port_list]	[port_list]	Show the specified ports' IGMP Filtering status.
Switch(config)#show ip igmp profile		Show IP multicast profile information.
Switch(config)#show ip igmp profile [profile_name]	[profile_name]	Show the specified profile's setting.
Switch(config)#show ip igmp segment		Show IP multicast segment information.
Switch(config)#show ip igmp segment [1-400]	[1-400]	Show the specified segment's setting.
Switch(config-segment-ID)# show		Show the selected segment's setting.
Switch(config-profile-ID)# show		Show the selected profile's setting.
IGMP Filtering command example		
Switch(config)# ip igmp filter		Enable IGMP Filtering function.
Switch(config)# ip igmp segment 50		Create a segment "50".
Switch(config-segment-50)# name Silver		Specify a name "Silver" for this segment 50.
Switch(config-segment-50)# range 224.10.0.2 229.10.0.1		Specify a multicast IP range 224.10.0.2 to 229.10.0.1.
Switch(config)# ip igmp profile Silverprofile		Specify a name "Silverprofile" for this profile.
Switch(config-profile-Silverprofile)# segment 50		Silverprofile includes segment 50.

Use "Interface" command to configure a group of ports' IGMP Filtering function.

IGMP & Interface Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# ip igmp filter		Enable IGMP Filter on the selected ports.

Switch(config-if-PORT-PORT)# ip igmp filter profile [profile_name]…	[profile_name] …	Assign the selected ports to a profile.
Switch(config-if-PORT-PORT)# ip igmp max-groups [1-512]	[1-512]	Specify the maximum number of multicast streams.
Switch(config-if-PORT-PORT)# ip igmp static-multicast-ip [E.F.G.H] vlan [1-4094]	[E.F.G.H]	Create a static multicast IP to VLAN entry. Specify static multicast IP address.
	[1-4094]	Specify a VLAN ID
Switch(config-if-PORT-PORT)# ip sourceguard [dhcp | fixed-ip]	[dhcp | fixed-ip]	Specify authorized access information for the selected ports. **dhcp:** DHCP server assigns IP address. **fixed IP:** Only Static IP (Create Static IP table first). **unlimited:** Non-Limited (Allows both static IP and DHCP-assigned IP). This is the default setting.
Switch(config-if-PORT-PORT)# ip sourceguard static-ip [A.B.C.D | A:B:C:D:E:F:G:H] vlan [1-4094]	[A.B.C.D | A:B:C:D:E:F:G:H]	Add a static IP address to static IP address table. Specify an IP address.
	[255.X.X.X]	Specify subnet mask for the specified IP address.
	[1-4094]	Specify a VLAN ID.
No command		
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# no ip igmp filter		Disable IGMP Filter on the selected interfaces.
Switch(config-if-PORT-PORT)# no ip igmp filter profile [profile_name]	[profile_name]	Remove the selected ports from the specified profile.
Switch(config-if-PORT-PORT)# no ip igmp max-groups		Set the maximum number of multicast streams back to the factory default (512 channels).
Switch(config-if-PORT-PORT)# no ip igmp static-multicast-ip [E.F.G.H] vlan [1-4094]	[E.F.G.H]	Remove this static multicast IP to VLAN entry. Specify static multicast IP address.
	[1-4094]	Specify a VLAN ID.
Switch(config-if-PORT-PORT)# no ip sourceguard		Set the accepted IP source to the factory default (unlimited).
Switch(config-if- PORT-PORT)#	[A.B.C.D |	Specify an IP address that you want

no ip sourceguard static-ip [A.B.C.D | A:B:C:D:E:F:G:H] vlan [1-4094]	A:B:C:D:E:F:G:H]	to remove from IP source binding table.
	[255.X.X.X]	Specify the subnet mask for this IP address.
	[1-4094]	Specify a VLAN ID.
Show command		
Switch(config)# show ip igmp filter		Show IGMP Filtering setting.
Switch(config)# show ip igmp filter interface [port_list]	[port_list]	Show the specified ports' IGMP Filtering status.
Switch(config)# show ip igmp profile		Show IP multicast profile information.
Switch(config)# show ip igmp profile [profile_name]	[profile_name]	Show the specified profile's setting.
Switch(config)# show ip igmp segment		Show IP multicast segment information.
Switch(config)# show ip igmp segment [1-400]	[1-400]	Show the specified segment's setting.
Switch(config)# show ip igmp static-multicast-ip		Show static multicast IP table.
Switch(config-segment-ID)# show		Show the selected segment's setting.
Switch(config-profile-ID)# show		Show the selected profile's setting.
Switch(config)# show ip sourceguard interface		Show each interface's IP sourceguard type.
Switch(config)# show ip sourceguard static-ip		Show the IP source binding table for sourceguard function.
IGMP & Interface example		
Switch(config)# interface1-3		Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-1-3)# ip igmp filter		Enable IGMP Filter on port 1 to port 3.
Switch(config-if-1-3)# ip igmp filter profile Silverprofile		Assign the selected ports to the specified profile "Silverprofile".
Switch(config-if-1-3)# ip igmp max-groups 400		Set the maximum number of multicast streams to 400.
Switch(config-if-1-3)# ip igmp static-multicast-ip 224.10.0.5 vlan 50		Create a static multicast IP to VLAN entry.

6.5.7 MAC Command

Set up the MAC address table aging time. Entries in the MAC address table containing source MAC addresses and their associated ports will be deleted if they are not accessed within the configured aging time.

MAC Command	Parameter	Description
Switch(config)# mac address-table aging-time [0-900]	[0-900]	Enter the aging time for the MAC address table. The available number is from 0 to 900. The default setting is “300” seconds.
No command		
Switch(config)# no mac address-table aging-time		Set the MAC address table aging time to the default value (300 seconds).
Show command		
Switch(config)# show mac aging-time		Show the current MAC address table aging time.
Switch(config)# show mac address-table		Show the MAC addresses learned by the Managed Industrial PoE Switch
Switch(config)# show mac address-table interface [port]	[port]	Show the MAC addresses learned by the selected ports.
Switch(config)# show mac address-table top		Show the first page of the MAC address table.
MAC command example		
Switch(config)# mac address-table aging-time 600		Set the MAC address table aging time to 600 seconds.

6.5.8 Management Command

Management command	Parameter	Description
Switch(config)# management console timeout [5-300]	[5-300]	Under RS-232 interface, specify the session aging time within the range: 5-300 seconds. The default setting is “300” seconds.
Switch(config)# management [ssh | telnet | web]	[ssh | telnet |web]	Select the system service type: SSH, telnet or web.
Switch(config)# management telnet port [1-65535]	[1-65535]	Specify the telnet port number. The default setting is “23”
No command		
Switch(config)# no management [ssh | telnet | web]	[ssh | telnet | web]	Set the system service type to Disabled.
Switch(config)# no management telnet port		Disable the configured telnet port.
Show command		
Switch(config)# show management		Show the current system service type.
Management command example		
Switch(config)# management ssh		Enable SSH system service type.

6.5.9 NTP Command

Set up required configurations for Network Time Protocol.

Command	Parameter	Description
Switch(config)# ntp		Enable the Managed Industrial PoE Ethernet Switch to synchronize the time with a time server.
Switch(config)# ntp daylight-saving [recurring | date]	[recurring | date]	Enable the day light saving.
Switch(config)# ntp offset [Mm,w,d,hh:mm-Mm,w,d,hh:mm]	[Mm,w,d,hh:mm-Mm,w,d,hh:mm]	Configure the offset of the daylight saving in the recurring mode. **Mm=1-12, w=1-5, d=0-6(0=Sun, 6=Sat) hh=0-23, mm=0-59, Days=1-365**
Switch(config)# ntp offset [Days,hh:mm-Days,hh:mm]	[Days,hh:mm-Days,hh:mm]	Configure the offset of the daylight saving in the date mode. **Mm=1-12, w=1-5, d=0-6(0=Sun, 6=Sat) hh=0-23, mm=0-59, Days=1-365**
Switch(config)# ntp server1 [A.B.C.D]	[A.B.C.D]	Specify the primary time server IP address.
Switch(config)# ntp server2 [A.B.C.D]	[A.B.C.D]	Specify the secondary time server IP address.
Switch(config)# ntp syn-interval [1-8]	[1-8]	Specify the time interval to synchronize the NTP time server. The meanings of the value: **1:1hr, 2:2hrs, 3:3hrs, 4:4hrs, 5:6hrs, 6:8hrs, 7:12hrs, 8:24hrs**
Switch(config)# ntp time-zone [0-135]	[0-135]	Specify the time zone where the Managed Industrial PoE Switch belongs. Use a command to view the complete code list of 135 time zones. For example, “Switch(config)# ntp time-zone ?”
No command		
Switch(config)# no ntp		Disable the Managed Industrial PoE Switch to synchronize the time with a time server.
Switch(config)# no ntp daylight-saving		Disable the daylight saving function.
Switch(config)# no ntp offset		Set the offset back to the default setting.
Switch(config)# no ntp server1		Delete the primary time server IP address.
Switch(config)# no ntp server2		Delete the secondary time server IP address.
Switch(config)# no ntp syn-interval		Set the synchronization interval back to the default setting.
Switch(config)# no ntp time-zone		Set the time-zone setting back to the default setting.
Show command		

Switch(config)# show ntp	Show or verify the current time server settings.
NTP command example	
Switch(config)# ntp	Enable the Managed Industrial PoE Switch to synchronize the time with a time server.
Switch(config)# ntp server1 192.180.0.12	Set the primary time server IP address to 192.180.0.12.
Switch(config)# ntp server2 192.180.0.13	Set the secondary time server IP address to 192.180.0.13.
Switch(config)# ntp syn-interval 8	Set the synchronization interval to 24 hrs.
Switch(config)# ntp time-zone 4	Set the time zone to GMT-8:00 Vancouver.

6.5.10 QoS Command

1. To specify the desired QoS mode:

QoS command	Parameter	Description
Switch(config)# qos [802.1p | dscp]	[802.1p | dscp]	Specify the QoS mode. **802.1p:** Use the *“qos 802.1p-map [0-7] [0-7]”* command to assign a priority bit to a queue. **dscp:** Use the “*qos dscp-map [0-63] dscp_list [0-7]”* to assign several DSCP bit values to a queue.
No command		
Switch(config)# no qos		Disable the QoS function.
Show command		
Switch(config)# show qos		Show or verify the QoS configurations.
QoS command example		
Switch(config)# qos 802.1p		Enable QoS function and use 802.1p mode.
Switch(config)# qos dscp		Enable QoS function and use DSCP mode.

2. To set up the 802.1p priority bit and queue mapping:

802.1p-map command	Parameter	Description
Switch(config)# qos 802.1p-map [0-7] 802.1p_list [0-7]	[0-7] 802.1p_list	Specify the corresponding 802.1p bits to a queue.

	[0-7]	Specify a queue to the specified 802.1p bits.
No command		
Switch(config)# no qos 802.1p-map [0-7] 802.1p_list	[0-7] 802.1p_list	Set the queue of the specific 802.1p bits back to the default.
Show command		
Switch(config)# show qos		Show or verify QoS configurations.
802.1p-map example		
Switch(config)# qos 802.1p-map 5 3		Specify the 802.1p bit 5 to the priority queue 3.
Switch(config)# qos 802.1p-map 5-7 3		Specify the 802.1p bit 5, 6 and 7 to the priority queue 3.

3. To set up the DSCP and queue mapping:

DSCP-map command	Parameter	Description
Switch(config)# qos dscp-map [0-63] dscp_list [0-7]	[0-63] dscp_list	Specify the corresponding DSCP values to a queue.
	[0-7]	Specify the queue to the specified DSCP values.
No command		
Switch(config)# no qos dscp-map [0-63] dscp_list		Set the queue of the specific DSCP values back to the default.
Show command		
Switch(config)# show qos		Show or verify QoS configurations.
DSCP-map example		
Switch(config)# qos dscp-map 30 3		Specify the DSCP value 30 to the priority queue 3.
Switch(config)# qos dscp-map 40,50 3		Specify the DSCP value 40 and 50 to the priority queue 3.

4. To set up the management priority:

Management-priority command	Parameter	Description
Switch(config)# qos management-priority [0-7]	[0-7]	Specify the management traffic 802.1p bit.
No command		
Switch(config)# no qos management-priority		Set management traffic priority back to the default value which is 0.
Management-priority example		
Switch(config)# qos management-priority 4		Set the management traffic priority to 4.

NOTE: *To check the setting of management traffic priority, please refer to 6.5.18 VLAN Command.*

5. To set up the QoS queuing mode:

Queuing-mode command	Parameter	Description
Switch(config)# qos queuing-mode [weight]	[weight]	By default, “strict” queuing mode is used. If you want to use “weight” queuing mode, you need to use the “qos queuing-mode wieght” command. **Strict mode:** Traffic assigned to queue 7 will be transmitted first, and the traffic assigned to queue 6 will not be transmitted until queue 7’s traffic is all transmitted, and so forth. **Weight mode**: All queues have fair opportunity of dispatching. Each queue has the specific amount of bandwidth according to its assigned weight.
No command		
Switch(config)# no qos queuing-mode		Set the queuing mode to the strict mode.
Show command		
Switch(config)# show qos		Show or verify QoS configurations.
Queuing-mode example		
Switch(config)# qos queuing-mode weight		Change the queuing mode from Strict to Weight.

6. To set up queuing weights of the weight mode:

Queue-weighted command	Parameter	Description
Switch(config)# qos queue-weighted [1:2:3:4:5:6:7:8]	[_:_:_:_:_:_:_:_] (1-32)	By default, the weights are “1:2:3:4:5:6:7:8”. Specify a value from 1 to 32 to each queue. The total amount of the weights cannot be more than 128.
No command		
Switch(config)# no qos queue-weighted		Set the queuing weights back to the default.
Show command		
Switch(config)# show qos		Show or verify QoS configurations.
Queue-weighted example		
Switch(config)# qos queue-weighted 1:2:4:6:8:10:12:14		Specify the queue weights as 1:2:4:6:8:10:12:14.

6.5.11 SNMP Server Command

1. Create a SNMP community and set up detailed configurations for this community.

Snmp-server command	Parameter	Description
Switch(config)# snmp-server community [community]	[community]	Specify a SNMP community name up to 20 alphanumeric characters.
Switch(config-community-NAME)# active		Enable this SNMP community account.
Switch(config-community-NAME)# description [Description]	[Description]	Enter the description up to 35 alphanumerical characters for this SNMP community.
Switch(config-community-NAME)# level [admin | rw | ro]	[admin | rw | ro]	Specify the access privilege for this SNMP account. By default, when you create a community, the access privilege for this account is set to “read only”. **Admin:** Full access right, including maintaining user account, system information, loading factory settings, etc.. **rw:** Read & Write access privilege. Partial access right, unable to modify system information, user account, load factory settings and upgrade firmware. **Ro:** Read Only access privilege.
No command		
Switch(config)# no snmp-server community [community]	[community]	Delete the specified community.
Switch(config-community-NAME)# no active		Disable this SNMP community account.
Switch(config-community-NAME)# no description		Remove the entered SNMP community descriptions.
Switch(config-community-NAME)# no level		Remove the configured level. This will set this community’s level to read only.
Show command		
Switch(config)# show snmp-server community [community]	[community]	Show the specified SNMP server account’s settings.
Switch(config)# show snmp-server community		Show SNMP community account’s information in Global Configuration Mode.
Switch(config-community-NAME)# show		View or verify the configured SNMP community account’s information.
Exit command		
Switch(config-community-NAME)# exit		Return to Global Configuration Mode.
Snmp-server example		
Switch(config)# snmp-server community mycomm		Create a new community “mycomm” and edit the details of this community account.
Switch(config-community-mycomm)# active		Activate the SNMP community “mycomm”.
Switch(config-community-mycomm)# description rddeptcomm		Add a description for “mycomm” community.

Switch(config-community-mycomm)# level admin	Set “mycomm” community level to admin.

2. Set up a SNMP trap destination.

Trap-dest command	Parameter	Description
Switch(config)# snmp-server trap-destination [1-3]	[1-3]	Create a trap destination account.
Switch(config-trap-ACCOUNT)# active		Enable this SNMP trap destination account.
Switch(config-trap-ACCOUNT)# community [community]	[community]	Enter the community name of network management system.
Switch(config-trap-ACCOUNT)# destination [A.B.C.D]	[A.B.C.D]	Enter the SNMP server IP address.
No command		
Switch(config)# no snmp-server trap-destination [1-3]	[1-3]	Delete the specified trap destination account.
Switch(config-trap-ACCOUNT)# no active		Disable this SNMP trap destination account.
Switch(config-trap-ACCOUNT)# no community		Delete the configured community name.
Switch(config-trap-ACCOUNT)# no description		Delete the configured trap destination description.
Show command		
Switch(config)# show snmp-server trap-destination [1-3]	[1-3]	Show the specified trap destination information.
Switch(config)# show snmp-server trap-destination		Show SNMP trap destination information in Global Configuration mode.
Switch(config-trap-ACCOUNT)# show		View this trap destination account’s information.
Exit command		
Switch(config- trap-ACCOUNT)# exit		Return to Global Configuration Mode.
Trap-destination example		
Switch(config)# snmp-server trap-destination 1		Create a trap destination account.
Switch(config-trap-1)# active		Activate the trap destination account.
Switch(config-trap-1)# community mycomm		Refer this trap destination account to the community “mycomm”.
Switch(config-trap-1)# description redepttrapdest		Add a description for this trap destination account.
Switch(config-trap-1)# destination 172.168.1.254		Set trap destination IP address to 192.168.1.254.

3. Set up SNMP trap types that will be sent.

Trap-type command	Parameter	Description
Switch(config)# snmp-server trap-type [all |auth-fail | cold-start | port-link | power-down | warm-start]	[all |auth-fail | cold-start | port-link | power-down | warm-start]	Specify the trap type that will be sent when a certain situation occurs. **all:** A trap will be sent when authentication fails, the device cold /warm starts, port link is up or down, power is down. **auth-fail:** A trap will be sent when any unauthorized user attempts to login. **cold-start:** A trap will be sent when the device boots up. **port-link:** A trap will be sent when the link is up or down. **power-down:** A trap will be sent when the device's power is down. **warm-start:** A trap will be sent when the device restarts.
No command		
Switch(config)# no snmp-server trap-type auth-fail		Authentication failure trap will not be sent.
Show command		
Switch(config)# show snmp-server trap-type		Show the current enable/disable status of each type of trap.
Trap-type example		
Switch(config)# snmp-server trap-type all		All types of SNMP traps will be sent.

6.5.12 Spanning-tree Command

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

Multiple active paths between network nodes cause a bridge loop. Bridge loops create several problems. First, the MAC address table used by the switch or bridge can fail, since the same MAC addresses (and hence the same network hosts) are seen on multiple ports. Second, a broadcast storm occurs. This is caused by broadcast packets being forwarded in an endless loop between switches. A broadcast storm can consume all available CPU resources and bandwidth.

Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manually enabling/disabling these backup links.

To provide faster spanning tree convergence after a topology change, an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP), introduced by IEEE with document 802.1w. RSTP is a refinement of STP; therefore, it shares most of its basic operation characteristics. This essentially creates a cascading effect away from the root bridge where each designated bridge proposes to its neighbors to determine if it can make a rapid transition. This is one of the major elements which allow RSTP to achieve faster convergence times than STP.

Spanning-tree command	Parameter	Description
Switch(config)# spanning-tree aggregated-port		Enable Spanning Tree Protocl function on aggregated ports.
Switch(config)# spanning-tree aggregated-port cost [0-200000000]	[0-200000000]	Specify aggregated ports' path cost.
Switch(config)# spanning-tree aggregated-port priority [0-15]	[0-15]	Specify aggregated ports' priority. **0=0, 1=16, 2=32, 3=48, 4=64, 5=80 6=96, 7=112, 8=128, 9=144, 10=160 11=176, 12=192, 13=208, 14=224, 15=240**
Switch(config)# spanning-tree aggregated-port edge		Enable aggregated ports to shift to forwarding state when the link is up. If you know a port is directly connected to an end device (that doesn't support RSTP) then set it as an edge port to ensure maximum performance. This will tell the switch to immediately start forwarding traffic on the port and not bother trying to establish a RSTP connection. Otherwise, turn it off.
Switch(config)# spanning-tree aggregated-port p2p [forced_true | forced_false | auto]	[forced_true | forced_false | auto]	Set the aggregated ports to non-point to point ports (forced_false) or allow the Managed Switch to detect point to point status automatically (auto). By default, aggregated ports are set to point to point ports (forced_true).
Switch(config)# spanning-tree delay-time [4-30]	[4-30]	Specify the Forward Delay value in seconds. The allowable value is between 4 and 30 seconds.
Switch(config)# spanning-tree hello-time [1-10]	[1-10]	Specify the Hello Time value in seconds. The allowable value is between 4 and 30 seconds.
Switch(config)# spanning-tree max-age [6-200]	[6-200]	Specify the Maximum Age value in seconds. The allowable value is between 6 and 200.

Switch(config)# spanning-tree priority [0-15]	[0-15]	Specify a priority value on a per switch basis. The allowable value is between 0 and 15. **0=0, 1=4096, 2=8192, 3=12288, 4=16384** **5=20480, 6=24576, 7=28672, 8=32768** **9=36864, 10=40960, 11=45056,12=49152** **13=53248, 14=57344, 15=61440**
Switch(config)# spanning-tree version [compatible | normal]	[compatible | normal]	Set up RSTP version. **“compatible”** means that the Managed Switch is compatible with STP. **“normal”** means that the Managed Switch uses RSTP.
No command		
Switch(config)# no spanning-tree aggregated-port		Disable STP on aggregated ports.
Switch(config)# no spanning-tree aggregated-port cost		Reset aggregated ports’ cost to the factory default.
Switch(config)# no spanning-tree aggregated-port priority		Reset aggregated ports’ priority to the factory default.
Switch(config)# no spanning-tree aggregated-port edge		Disable aggregated ports’ edge ports status.
Switch(config)# no spanning-tree aggregated-port p2p		Reset aggregated ports to point to point ports (forced_true).
Switch(config)# no spanning-tree delay-time		Reset the Forward Delay time back to the factory default.
Switch(config)# no spanning-tree hello-time		Reset the Hello Time back to the factory default.
Switch(config)# no spanning-tree max-age		Reset the Maximum Age back to the factory default.
Show command		
Switch(config)# show spanning-tree		Show or verify STP settings on the per switch basis.
Switch(config)# show spanning-tree aggregated-port		Show or verify STP settings on aggregated ports.
Switch(config)# show spanning-tree interface		Show each interface’s STP information including port state, path cost, priority, edge port state, and p2p port state.
Switch(config)# show spanning-tree interface [port_list]	[port_list]	Show the selected interfaces’ STP information including port state, path cost, priority, edge port state, and p2p port state.
Switch(config)# show spanning-tree statistics		Show each interface and each link aggregation group’s statistics information

		including the total RSTP packets received, RSTP packets transmitted, STP packets received, STP packets transmitted, TCN (Topology Change Notification) packets received, TCN packets transmited, illegal packets received, and unknown packets received.
Switch(config)# show spanning-tree statistics [port_list | llag]	[port_list | llag]	Show the selected interfaces or link aggregation groups' statistics information including the total RSTP packets received, RSTP packets transmitted, STP packets received, STP packets transmitted, TCN (Topology Change Notification) packets received, TCN packets transmited, illegal packets received, and unknown packets received.
Switch(config)# show spanning-tree status		Show current RSTP port status.
Switch(config)# show spanning-tree status [port_list | llag]	[port_list | llag]	Show the selected interfaces or link aggregation groups' statistics information
Switch(config)# show spanning-tree overview		Show the current STP state.

Spanning-tree command example	Description
Switch(config)# spanning-tree aggregated-port	Enable Spanning Tree on aggregated ports.
Switch(config)# spanning-tree aggregated-port cost 100	Set the aggregated ports' cost to 100.
Switch(config)# spanning-tree aggregated-port priority 0	Set the aggregated ports' priority to 0
Switch(config)# spanning-tree aggregated-port edge	Set the aggregated ports to edge ports.
Switch(config)# spanning-tree aggregated-port p2p forced_true	Set the aggregated ports to P2P ports.
Switch(config)# spanning-tree delay-time 20	Set the Forward Delay time value to 10 seconds.
Switch(config)# spanning-tree hello-time 2	Set the Hello Time value to 2 seconds.
Switch(config)# spanning-tree max-age 15	Set the Maximum Age value to 15 seconds.

Use "Interface" command to configure a group of ports' Spanning Tree settings.

Spanning tree & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For

		example:1,3 or 2-4
Switch(config-if-PORT-PORT)# spanning-tree		Enable spanning-tree protocol on the selected interfaces.
Switch(config-if-PORT-PORT)# spanning-tree cost [1-200000000]	[1-200000000]	Specify cost value on the selected interfaces.
Switch(config-if-PORT-PORT)# spanning-tree priority [0-15]	[0-15]	Specify priority value on the selected interfaces. **0=0, 1=4096, 2=8192, 3=12288, 4=16384** **5=20480, 6=24576, 7=28672, 8=32768** **9=36864, 10=40960, 11=45056,12=49152** **13=53248, 14=57344, 15=61440**
Switch(config-if-PORT-PORT)# spanning-tree edge		Set the selected interfaces to edge ports.
Switch(config-if-PORT-PORT)# spanning-tree p2p [forced_fasle | auto]	[forced_fasle | auto]	Set the aggregated ports to non-point to point ports (forced_false) or allow the Managed Switch to detect point to point status automatically (auto). By default, aggregated ports are set to point to point ports (forced_true).
No command		
Switch(config-if-PORT-PORT)# no spanning-tree		Disable spanning-tree protocol on the selected interfaces.
Switch(config-if-PORT-PORT)# no spanning-tree cost		Set the cost value back to the factory default.
Switch(config-if-PORT-PORT)# no spanning-tree priority		Set the priority value back to the factory default.
Switch(config-if-PORT-PORT)# no spanning-tree edge		Set the selected interfaces to non-edge ports.
Switch(config-if-PORT-PORT)# no spanning-tree p2p		Set the selected interface to point to point ports.
Show command		
Switch(config)# show spanning-tree		Show or verify STP settings on the per switch basis.
Switch(config)# show spanning-tree aggregated-port		Show or verify STP settings on aggregated ports.
Switch(config)# show spanning-tree interface		Show each interface’s STP information including port state, path cost, priority, edge port state, and p2p port state.
Switch(config)# show spanning-tree interface [port_list]	[port_list]	Show the selected interfaces’ STP information including port state, path cost, priority, edge port state, and p2p port state.

Switch(config)# show spanning-tree statistics		Show each interface and each link aggregation group’s statistics information including the total RSTP packets received, RSTP packets transmitted, STP packets received, STP packets transmitted, TCN (Topology Change Notification) packets received, TCN packets transmited, illegal packets received, and unknown packets received.
Switch(config)# show spanning-tree statistics [port_list | llag]	[port_list | llag]	Show the selected interfaces or link aggregation groups’ statistics information including the total RSTP packets received, RSTP packets transmitted, STP packets received, STP packets transmitted, TCN (Topology Change Notification) packets received, TCN packets transmited, illegal packets received, and unknown packets received.
Switch(config)# show spanning-tree status		Show current RSTP port status.
Switch(config)# show spanning-tree status [port_list | llag]	[port_list | llag]	Show the selected interfaces or link aggregation groups’ statistics information
Switch(config)# show spanning-tree overview		Show the current STP state.
Spanning-tree & interface command example		**Description**
Switch(config)# interface 1-3		Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-1-3)# spanning-tree cost 100		Set the selected interfaces’ cost to 100.
Switch(config-if-1-3)# spanning-tree priority 0		Set the selected interfaces’ priority to 0
Switch(config-if-1-3)# spanning-tree edge		Set the selected ports to edge ports.
Switch(config-if-1-3)# spanning-tree p2p forced_false		Set the selected ports to non-P2P ports.

6.5.13 Switch-info Command

To set up the Managed Industrial PoE Switch’s basic information including company name, hostname, system name, etc., use “switch-info” command.

Switch-info Command	Parameter	Description

Switch(config)# switch-info company-name [company_name]	[company_name]	Enter a company name up to 55 alphanumeric characters for this Switch.
Switch(config)# switch-info dhcp-vendor-id [dhcp_vendor_id]	[dhcp_vendor_id]	Enter the user-defined DHCP vendor ID up to 55 alphanumeric characters. Please make sure you have an exact DHCP Vendor ID with the value specified in “vendor-classes” in your dhcp.conf file. For detailed information, please see Appendix A.
Switch(config)# switch-info system-contact [system_contact]	[system_contact]	Enter the contact information up to 55 alphanumeric characters for this Managed Industrial PoE Switch.
Switch(config)# switch-info system-location [system_location]	[system_location]	Enter a brief description of the Managed Industrial PoE Switch location up to 55 alphanumeric characters. The location is for reference only, for example, “13th Floor”.
Switch(config)# switch-info system-name [system_name]	[system_name]	Enter a unique name up to 55 alphanumeric characters for this Managed Industrial PoE Switch. Use a descriptive name to identify the Managed Industrial PoE Switch in relation to your network, for example, “Backbone 1”. This name is mainly used for reference only.
Switch(config)# switch-info host-name [host_name]	[host_name]	Enter a new hostname up to 15 alphanumeric characters for this Managed Industrial PoE Switch. By default, the hostname prompt shows the model name of this Managed Industrial PoE Switch. You can change the factory-assigned hostname prompt to the one that is easy for you to identify within the network configuration and maintenance.
No command		
Switch(config)# no switch-info company-name		Set the company name to the factory default.
Switch(config)# no switch-info dhcp-vendor-id		Set the DHCP vendor ID to the factory default.
Switch(config)# no switch-info system-contact		Set the system contact information to the factory default.
Switch(config)# no switch-info system-location		Set the system location to the factory default.
Switch(config)# no switch-info system-name		Set the system name to the factory default.
Switch(config)# no switch-info host-name		Set the hostname to the factory default.
Show command		
Switch(config)# show switch-info		Show the switch information including company name, system contact, system

	location, system name, model name, firmware version, fiber type, etc.
Switch-info example	
Switch(config)# switch-info company-name telecomxyz	Set the company name to “telecomxyz”.
Switch(config)# switch-info system-contact info@company.com	Set the system contact information to “info@compnay.com”.
Switch(config)# switch-info system-location 13thfloor	Set the system location to “13thfloor”.
Switch(config)# switch-info system-name backbone1	Set the system name to “backbone1”.

6.5.14 Ring Detection Command

Ring Detection used in ring topology is a helpful way of network recovery, preventing from disconnection resulting from any unexpected link down.

Ring Detection command	Parameter	Description
Switch(config)# ring-detection		Enable ring detection.
Switch(config)# ring-detection role [master]	[master]	Assign Ring role as master.
Switch(config)# ring-detection port [port_list]	[port_list]	Specify Ring port.
No command		
Switch(config)# no ring-detection role		Undo the Ring role.
Switch(config)# no ring-detection port		Disable Ring Detection on ports specified.
Show command		
Switch(config)#show ring-detection		Show Ring Detection information and Ring Detection configuration.
Switch(config)#show ring-detection state		Show Ring Detection status.

6.5.15 Syslog Command

Syslog command	Parameter	Description
Switch(config)# syslog		Enable the syslog server.
Switch(config)# syslog server1/server2/server3 [A.B.C.D]	[A.B.C.D]	Configure the IP address of the syslog server1/server2/server3.
No command		
Switch(config)# no syslog		Disable the syslog server.

Show command	
Switch(config)#show syslog	Show the syslog information.
Syslog example	
Switch(config)# syslog Switch(config)# syslog server1 192.168.0.222	Enable syslog and assign the server1 IP address 192.168.0.222.

6.5.16 Time Range Command

This command defines a time interval to be activated on a daily or weekly basis. This is convenient to assign when a function should automatically take effect. Before using the function, make sure that gateway is set under either IPv4 mode in **IP Command** (Section 2.5.6) and time server is configured in **NTP Command** (Section 2.5.10). Time Range related function scheduling will only take effect when Switch system time is sync with NTP time server.

Command	Parameter	Description
Switch(config)# poe time-range [time_range_name]	[time_range_name]	Specify a name to the time interval, and access its edit mode. To return to previous level, enter “exit”. It receives 32 characters at most. 10 time ranges can be set at most. Time interval can be classified into three types: Absolute, Periodic and Periodic List. **Absolute:** An absolute interval to enable a function. **Periodic:** An interval to enable a function on a weekly basis. The periodic interval only takes effect within specified absolute interval. **Periodic List:** An interval to enable a function on a daily basis. The periodic list interval only takes effect within specified absolute interval.
Switch(config –time-range-name)# absolute start [hh:mm dd MMM yyyy]	[hh:mm dd MMM yyyy]	Specify an absolute start time to a time interval. Where: hh(hour) 0-23 mm(minute) 0-59 dd(date) 1-31 MMM(month) jan,feb,mar,apr,may,jun,jul,aug,sep,oct,nov,dec yyyy(year) 2000-2097

		No start time assigned refers to start immediately. One absolute start point can be set at most.
Switch(config –time-range-name)# absolute end [hh:mm dd MMM yyyy]	[hh:mm dd MMM yyyy]	Specify an absolute end time to a time interval. Where: hh(hour) 0-23 mm(minute) 0-59 dd(date) 1-31 MMM(month) jan,feb,mar,apr,may,jun,jul,aug,sep,oct,nov,dec yyyy(year) 2000-2097 No end time assigned refers to run an function continuously. One absolute end point can be set at most.
Switch(config –time-range-name)# periodic [hh:mm dd] to [hh:mm dd]	[hh:mm dd] to [hh:mm dd]	Specify weekly recurring time interval. Two set of periodic intervals can be set at most.
Switch(config –time-range-name)# periodic list [hh:mm] to [hh:mm] [days]	[hh:mm] to [hh:mm] [days]	Specify a list of days in a week for periodic run. Where: hh(hour) 0-23 mm(minute) 0-59 days(7 days) including Sunday(sun), Monday(mon), Tuesday(tue), Wednesday(wed), Thursday(thu), Friday(fri), Saturday(sat) Cross-day setting is feasible. In other words, the second occurrence of time can be set on the following day, e.g. “22:00-2:00”. Two set of periodic list intervals can be set at most.
No Command		
Switch(config)# no time-range [time_range_name]	Remove a specified time-range name.	
Switch(config –time-range-name)# no absolute start	Remove absolute start time. Under a time range name, user may add one absolute start time and one absolute end time at most. Users may also add two optional time ranges at most using Periodic and Periodic List time range. For example, Users may set: 1. Two Periodic in time range, or	

	2. One Periodic and one Periodic List in time range, or 3. Two Periodic List in time range.
Switch(config –time-range-name)# no absolute end	Remove absolute start time. Under a time range name, user may add one absolute start time and one absolute end time at most. Users may also add two optional time ranges at most using Periodic and Periodic List time range. For example, Users may set: **1.** Two Periodic in time range, or **2.** One Periodic and one Periodic List in time range, or **3.** Two Periodic List in time range.
Switch(config –time-range-name)# no periodic [hh:mm] [day] [hh:mm] [day]	Remove periodic weekly time interval. (sun, mon, tue, wed, thu, fri, sat)
Switch(config –time-range-name)# no periodic list [hh:mm] to [hh:mm] [days]	Remove periodic list interval.
Show Command	
Switch(config)# show time-range	Display the time-range configuration
Switch(config)# show time-range [time_range_name]	Display the specified time-range configuration
Example Command	
Switch(config –time-range-name)# absolute start 8:00 10 jan 2015	Set effective time range start from 8:00, January 10th, 2015 sharp.
Switch(config –time-range-name)# absolute end 18:00 10 dec 2015	Set an effective time range that stops at 18:00, December 10th, 2015 sharp.
Switch(config –time-range-name)# periodic 10:00 mon to 20:00 wed	Set an effective time range that start from 10:00, Monday to 20:00 Wednesday.
Switch(config –time-range-name)# periodic list 09:00 to 18:00 mon tue wed thu fri	Set an effective time range that start from 09:00 to 18:00 every weekday.
Switch(config –time-range-name)# periodic list 20:00 to 04:00 tue wed thu fri sat	Set an effective time range that start from 20:00, Tuesday to 04:00 Saturday.
Switch(config –time-range-name)# periodic list 08:00 to 10:00 wed thu	Set an effective time range that start from 08:00 to 10:00 every Wednesday and Thursday.

6.5.17 User Command

1. Create a new login account.

User command	Parameter	Description
Switch(config)# user name [user_name]	[user_name]	Create a new user account. The authorized user login name is up to 20 alphanumeric characters. The maximum of the user accounts that can be created is 10.
Switch(config-user-USERNAME)# active		Activate this user account.
Switch(config-user-USERNAME)# description [description]	[description]	Enter the brief description for this user account.
Switch(config-user-USERNAME)# level [admin | rw | ro]	[admin | rw | ro]	Specify the user account level. By default, when you create a user account, the access privilege is set to "admin". **admin:** Full access right, including maintaining user account, system information, loading factory settings, etc. **rw:** Read & Write access privilege. Partial access right which is unable to modify system information, user account, load factory settings and upgrade firmware. **Ro:** Read Only access privilege.
Switch(config-user-USERNAME)# password [password]	[password]	Enter the password for this user account up to 20 alphanumeric characters.
No command		
Switch(config)# no user name [user_name]	[user_name]	Delete the specified user account.
Switch(config-user-USERNAME)# no description		Remove the configured description.
Switch(config-user-USERNAME)# no level		Remove the configured level. The account level will be set to the default setting.
Switch(config-user-USERNAME)# no password		Remove the configured password.
Show command		
Switch(config)# show user name [user_name]	[user_name]	Show the specified account's information.
Switch(config)# show user name		List all user accounts.
Switch(config-user-USERNAME)# show		Show or verify the newly-created user account's information.
User command example		
Switch(config)# user name miseric		Create a new login account "miseric".
Switch(config-user-USERNAME)# description misengineer		Add a description to this new account "miseric".

Switch(config-user-USERNAME)# level rw	Set this new account's access privilege to "read & write".
Switch(config-user-USERNAME)# password mis2256i	Set up a password for this new account "miseric"

2. Configure RADIUS server settings.

User command	Parameter	Description
Switch(config)# user radius		Enable RADIUS authentication.
Switch(config)# user radius radius-port [1025-65535]	[1025-65535]	Specify the RADIUS server port number. The default value is "1812"
Switch(config)# user radius retry-time [0-2]	[0-2]	Specify the number of times that the Switch will try to reconnect if the RADIUS server is not reachable. The default value is "0".
Switch(config)# user radius secret [secret]	[secret]	Specify a secret up to 30 alphanumeric characters for the RADIUS server. This secret key is used to validate the communication between the RADIUS server and Switch.
Switch(config)# user radius server1 [A.B.C.D]	[A.B.C.D]	Specify the primary RADIUS server IP address.
Switch(config)# user radius server2 [A.B.C.D]	[A.B.C.D]	Specify the secondary RADIUS server IP address.
No command		
Switch(config)# no user radius		Disable RADIUS authentication.
Switch(config)# no user radius radius-port		Set the radius port back to the factory default.
Switch(config)# no user radius retry-time		Set the retry time back to the factory default.
Switch(config)# no user radius secret		Remove the configured secret.
Switch(config)# no user radius server1		Delete the primary RADIUS server IP address.
Switch(config)# no user radius server2		Delete the secondary RADIUS server IP address.
Show command		
Switch(config)#show user radius		Show current RADIUS settings.
User command example		
Switch(config)# user radius		Enable RADIUS authentication.
Switch(config)# user radius radius-port 1812		Set the RADIUS server port number to 1812.
Switch(config)# user radius retry-time 2		Set the retry time to 2. The Switch will try to reconnect twice if the RADIUS server is not reachable.
Switch(config)# user radius secret abcxyzabc		Set up a secret abcxyzabc for validating the communication.

Switch(config)# user radius server1 192.180.3.1	Set the primary RADIUS server IP address to 192.180.3.1.
Switch(config)# user radius server2 192.180.3.2	Set the secondary RADIUS server IP address to 192.180.3.2.

6.5.18 VLAN Command

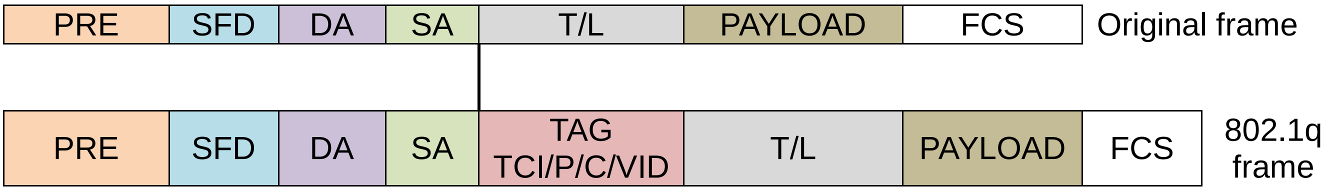
A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the Switch on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. A station can be ‘moved’ to another VLAN and thus communicates with its members and shares its resources, simply by changing the port settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

802.1Q VLAN Concept

Port-Based VLAN is simple to implement and use, but it cannot be deployed cross switches VLAN. The 802.1Q protocol was developed in order to provide the solution to this problem. By tagging VLAN membership information to Ethernet frames, the IEEE 802.1Q can help network administrators break large switched networks into smaller segments so that broadcast and multicast traffic will not occupy too much available bandwidth as well as provide a higher level security between segments of internal networks.

Introduction of 802.1Q frame format



PRE Preamble	62 bits	Used to synchronize traffic
SFD Start Frame Delimiter	2 bits	Marks the beginning of the header

DA Destination Address	6 bytes	The MAC address of the destination
SA Source Address	6 bytes	The MAC address of the source
TCI Tag Control Info	2 bytes	Set to 0x8100 for 802.1p and Q tags
P Priority	3 bits	Indicates 802.1p priority level 0-7
C Canonical Indicator	1 bit	Indicates if the MAC addresses are in the canonical format – Ethernet is set to “0”.
VID VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L Type/Length Field	2 bytes	Ethernet II “type” or 802.3 “length”
Payload	< or = 1500 bytes	User data
FCS Frame Check Sequence	4 bytes	Cyclical Redundancy Check

Important VLAN Concepts for 802.1Q VLAN Configuration

There are two key concepts as follows:

- **Access-VLAN** specifies the VLAN ID to the switch port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a time. When the port is configured as **Access Mode**, the port is called an **Access Port**, and the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies a set of VLAN IDs to a given port to receive and send **tagged** packets which have the same VLAN ID. A port can be assigned to multiple Trunk-VLANs at a time. When the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, and the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

A port can be configured to the 802.1q VLAN modes as below:

- **Access Mode:**

  Access Links (the link to/from access ports) are the most common type of links on any VLAN switch. All network hosts (such as PCs) connect to the switch's Access Links in order to gain access to the local network. We configure only one Access-VLAN per port, that is, there’s only one VLAN ID (VID) which the network hosts will be allowed to access.

  It is important to note at this point that any network host connected to an Access Port is totally unaware of the VLAN assigned to the port. The network host simply assumes it is part of a single broadcast domain, just as it happens with any normal switch. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode:**

  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. This type of ports is usually found in connections between switches. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple switches.

- **Trunk Native Mode:**

A Trunk-native port can carry untagged packets and the 802.1Q tagged packets simultaneously. Untagged packets can pass the Trunk-Native port, but the untagged packets will be tagged a value of the assigned Port VLAN ID (PVID) in the internal device. Tagged packets with the value of the assigned VLAN IDs (VIDs) can pass through the interface as well. In addition, these packets will keep their original VLAN ID in the internal device.

Example: PortX configuration

Configuration	Result

Trunk-VLAN = 10, 11, 12
Access-VLAN = 20
Mode = Access
	PortX is an **Access Port.**
	PortX's **VID** is ignored.
	PortX's **PVID** is 20.
	PortX sends **Untagged** packets (PortX takes away VLAN tag if the PVID is 20).
	PortX receives **Untagged** packets only.

Trunk-VLAN = 10, 11, 12
Access-VLAN = 20
Mode = Trunk
	PortX is a **Trunk Port.**
	PortX's **VID** is 10, 11 and 12.
	PortX's **PVID** is ignored.
	PortX sends and receives **Tagged** packets whose VID is 10, 11 or 12.

Trunk-VLAN = 10, 11, 12
Access-VLAN = 20
Mode = Trunk-native
	PortX is a **Trunk-native Port.**
	PortX's **VID** is 10, 11 and 12.
	PortX's **PVID** is 20.
	PortX sends and receives **Tagged** packets whose VID is 10, 11 or 12.
	PortX receives **Untagged** packets and add PVID 20

1. **To use the "Interface" command to configure a group of ports' 802.1q VLAN settings:**

VLAN & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example: 1,3 or 2-4
Switch(config-if-PORT-PORT)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID). The default VID is "1".
Switch(config-if-PORT-PORT)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID). The default VID is "1".
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode access		Set the selected ports to Access mode (untagged).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk		Set the selected ports to Trunk mode (tagged).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk native		Set the selected ports to Trunk-Native mode. (Tagged and untagged)

		Note: When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.
Switch(config-if-PORT-PORT)# vlan port-based [name]	[name]	Set the selected ports to a specified port-based VLAN. **Note:** Before adding a port to a VLAN group, it's necessary to create a port-based VLAN group first by the "vlan port-based [name]" command.
No command		
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan access-vlan		Set the selected ports' PVID to the default setting.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan mode		Set the VLAN mode of the selected port(s) to Access mode.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan mode trunk native		Set the VLAN mode of the selected port(s) to Trunk mode.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected port(s) from the specified trunk VLAN group.
Switch(config-if-PORT-PORT)# no vlan port-based [name]	[name]	Remove the selected port(s) from the specified port-based VLAN group.
VLAN & interface command example		
Switch(config)# interface 1-3		Enter port 1 to port 3's interface mode.
Switch(config-if-1-3)# vlan dot1q-vlan access-vlan 10		Set port 1 to port 3's Access-VLAN ID (PVID) to 10.
Switch(config-if-1-3)# vlan dot1q-vlan mode access		Set the selected ports to Access mode (untagged).
Switch(config-if-1-3)# vlan dot1q-vlan mode trunk native		Set the selected ports to Trunk-Native mode (tagged and untagged).
Switch(config-if-1-3)# vlan port-based mktpbvlan		Set the selected ports to the specified port-based VLAN group "mktpbvlan".

2. To modify a 802.1q VLAN and a management VLAN rule or create a port-based VLAN group:

Port-based VLAN can effectively segment one network into several broadcast domains. Broadcast, multicast and unknown packets will be limited within the VLAN. Port-Based VLAN is uncomplicated, fairly rigid in implementation, and useful for network administrators who want to quickly and easily set up VLAN so as to isolate the effect of broadcast packets on their network.

VLAN dot1q command	Parameter	Description

Switch(config)# vlan dot1q-vlan		Enable 802.1q VLAN.
Switch(config)# vlan dot1q-vlan [1-4094]	[1-4094]	Modify a specified 802.1q VLAN. **Note:** A 802.1q VLAN needs to be created under the “interface” command. Here, you can only modify it instead of creating a new VLAN ID.
Switch(config-vlan-ID)# name [vlan_name]	[vlan_name]	Specify a descriptive name for this VLAN ID, up to 15 characters.
Switch(config)# vlan management-vlan [1-4094] management-port [port_list] mode [access | trunk | trunk-native]	[1-4094]	Specify the management VLAN ID.
	[port_list]	Specify the management port.
	[access | trunk | trunk-native]	Assign the management port to Trunk, Trunk-Native or Access mode. **“trunk” mode:** The selected ports send and receive tagged packets. **“access” mode:** The selected ports send and receive untagged packets. **“trunk-native” mode:** The selected ports send and receive tagged and untagged packets
Switch(config)# vlan port-based		Enable port-based VLAN.
Switch(config)# vlan port-based [name]	[name]	Specify a name for this port-based VLAN, up to 15 characters.
Switch(config)# vlan port-based [name] include-cpu		Include CPU into this port-based VLAN.
No command		
Switch(config)# no vlan dot1q-vlan		Disable 802.1q VLAN
Switch(config-vlan-ID)# no name		Remove the descriptive name of the specified VLAN ID.
Switch(config)# no vlan port-based		Disable port-based VLAN.
Switch(config)# no vlan port-based [name]	[name]	Delete the specified port-based VLAN.
Switch(config)# no vlan port-based [name] include-cpu		Exclude CPU from this port-based VLAN
Show command		
Switch(config)# show vlan dot1q-vlan tag-vlan		Show IEEE 802.1q Tag VLAN table

Switch(config)# show vlan dot1q-vlan trunk-vlan		Show Configure Trunk VLAN table
Switch(config-vlan-ID)# show		Show the membership status of this VLAN ID
Switch(config)# show vlan interface		Show all ports' VLAN assignment and VLAN mode.
Switch(config)# show vlan interface [port_list]	[port_list]	Show the selected ports' VLAN assignment and VLAN mode.
Switch(config)# show vlan port-based		Show the port-based VLAN table.
Exit command		
Switch(config-vlan-ID)# exit		Return to Global configuration mode.
Port-based VLAN example		
Switch(config)# vlan port-based MKT_Office		Create a port-based VLAN "MKT_Office".
Switch(config)# vlan management-vlan 1 management-port 1-3 mode access		Set VLAN 1 to management VLAN (untagged) and port 1~3 to management ports.

6.5.19 interface command

Use this command to set up various port configurations of discontinuous or a range of ports.

1. To enter interface numbers:

Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several port numbers separated by commas or a range of port numbers with a hyphen. For example: 1,3 or 2-4

Note: *You need to enter interface numbers first before issuing 2-9 commands below.*

2. To enable the port auto-negotiation:

Command	Parameter	Description
Switch(config-if-PORT-PORT)# auto-negotiation		Set the selected interfaces to the auto-negotiation. When the auto-negotiation is enabled, the speed configuration will be ignored.
No command		
Switch(config-if-PORT-PORT)# no auto-negotiation		Set the auto-negotiation setting to the default setting.

3. To set up port-trunking:

Command	Parameter	Description
Switch(config-if-PORT-PORT)# channel-group trunking [group_name]	[group_name]	Specify the selected port(s) to the trunking group. **Note 1:** At least 2 ports, not more than 8 ports can be aggregated. **Note 2:** A port-trunking group needs to be created before assigning ports to it (see 2.5.4 “channel-group”)
No command		
Switch(config-if-PORT-PORT)# channel-group trunking		Remove the ports from the port-trunking group.

4. **To set up the port description:**

Command	Parameter	Description
Switch(config-if-PORT-PORT)# description [description]	[description]	Type the description of the port(s), up to 35 characters.
No command		
Switch(config-if-PORT-PORT)# no description		Remove the entered description of the selected port(s).

5. **To configure the media type:**

Command	Parameter	Description
Switch(config-if-PORT-PORT)# media-type [fiber | copper | Auto-Media]	[fiber | copper | Auto-Media]	Configure the media type of the port(s). **Note:** Only port 9 and 10 which are combo ports can be configured.
No command		
Switch(config-if-PORT-PORT)# no media-type		Set the media type of the port(s) back to the default which is Auto-Media.

6. **To configure the Dot1x setting:**

Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# dot1x port-control [auto | unauthorized]		Specify the selected ports to “auto” or “unauthorized”. **“auto”:** This requires 802.1X-aware clients to be authorized by the

		authentication server. Accesses from clients that are not dot1x aware will be denied. **"unauthorized":** This forces the Managed Switch to deny access to all clients, neither 802.1X-aware nor 802.1X-unaware.
Switch(config-if-PORT-PORT)# dot1x reauthenticate		Re-authenticate the selected interfaces.
No command		
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# no dot1x port-control		Reset the selected interfaces' 802.1x state to the factory default (authorized state).
Show command		
Switch(config)# show dot1x		Show or verify 802.1x settings.
Switch(config)# show dot1x interface		Show or verify each interface's 802.1x settings including port status and authentication status.
Switch(config)# show dot1x interface [port_list]	[port_list]	Show or verify the selected interfaces' 802.1x settings including port status and authentication status.
Switch(config)# show dot1x statistics		Show or verify 802.1x statistics.
Switch(config)# show dot1x statistics [port_list]	[port_list]	Show or verify the selected interfaces' statistics.
Switch(config)# show dot1x status		Show or verify 802.1x status.
Switch(config)# show dot1x status [port_list]	[port_list]	Show or verify the selected interfaces' 802.1x status.
Command example		
Switch(config)# interface 1-3		Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-1-3)# dot1x port-control auto		Set the selected ports to "auto" state.
Switch(config-if-1-3)# dot1x reauthenticate		Re-authenticate the selected interfaces immediately.

7. To configure the QoS user priority:

Command	Parameter	Description
Switch(config-if-PORT-PORT)# qos user-priority [0-7]	[0-7]	Specify a 802.1p bit between 0 and 7 to the selected port(s).

No command		
Switch(config-if-PORT-PORT)# no qos user-priority		Set the ports’ 802.1p bit back to the default.

8. To shutdown the selected interface:

Command	Parameter	Description
Switch(config-if-PORT-PORT)# shutdown		Administratively disable the selected port(s).
No command		
Switch(config-if-PORT-PORT)# no shutdown		Administratively enable the selected port(s).

9. To configure the speed operation:

Command	Parameter	Description
Switch(config-if-PORT-PORT)# speed [1000 | 100 | 10]	[1000 | 100 | 10]	Set up the selected interfaces’ speed. The speed configuration only works when the interfaces are not under the auto-negotiation mode.
No command		
Switch(config-if-PORT-PORT)# no speed		Set the selected interfaces’ speed to the default setting.

10. To set the VLAN configuration:

Command	Parameter	Description
Switch(config-if-PORT-PORT)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Configure the ports’ PVID. The default VID is “1”.
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode access		Set the selected port(s) to Access mode.
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk		Set the selected port(s) to Trunk mode.
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk native		Set the selected port(s) to Trunk-Native mode.
Switch(config-if-PORT-PORT)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Configure the ports’ VID. The default VID is “1”.
Switch(config-if-PORT-PORT)# vlan port-based [name]	[name]	Add the port(s) to the specific port-based VLAN group. **Note:** Before adding a port to a VLAN group, it’s necessary to create a port-based VLAN group first by the “vlan port-based [name]” command.

No command		
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan access-vlan		Set the selected ports' PVID to the default setting.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan mode		Set the VLAN mode of the selected port(s) to Access mode.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan mode trunk native		Set the VLAN mode of the selected port(s) to Trunk mode.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected port(s) from the specified trunk VLAN group.
Switch(config-if-PORT-PORT)# no vlan port-based [name]	[name]	Remove the selected port(s) from the specified port-based VLAN group.

Show command		
Switch(config)# show interface status		Show each interface's status including media type, forwarding state, speed, duplex mode, flow control and link up/down status.
Switch(config)# show interface status [port_list]	[port_list]	Show the selected ports' status including media type, forwarding state, speed, duplex mode, flow control and link up/down status.

Interface command example	
Switch(config)# interface 1-3	Configure the port 1, 2 and 3.
Switch(config-if-1-3)# auto-negotiation	Set the port 1, 2, and 3 to auto-negotiation.
Switch(config-if-1-3)# speed 100	Set the port 1, 2, and 3 speed to 100Mbps.
Switch(config-if-1-3)# shutdown	Administratively disable the port 1, 2, and 3.

11. To set up PoE configuration

Command	Parameter	Description
Switch(config-if-PORT-PORT)# poe operation [shutdown | injector-30watt | auto-af/at]	[shutdown | injector-30watt | auto-af/at]	There are three modes available. Shutdown mode refers to disable PoE on a port permanently. Injector-30Watt mode refers to enable PoE on a port permanently. Auto AF/AT mode refers to flexibly enable PoE on a port the connected device at the other end. Under Semi-Auto mode, it automatically detects the connected

		device if the device supports PoE feature. If not, it won't give the connected device power.
Switch(config-if-PORT-PORT)# poe pdname [device_name]	[device_name]	Specify the connected power device name.
Switch(config-if-PORT-PORT)# poe schedule		Enable a specified PoE schedule.
Switch(config-if-PORT-PORT)# poe schedule [time-range-name]	[time-range-name]	Assign PoE schedule a time range. It defines which previous-configured time interval the port should follow. One set of time interval can be accepted at a time.
No command		
Switch(config-if-PORT-PORT)# no poe operation		Return PoE mode to default.
Switch(config-if-PORT-PORT)# no poe pdname		Remove the powered device name.
Switch(config-if-PORT-PORT)# no poe schedule		Disable PoE schedule fumction.
Switch(config-if-PORT-PORT)# no poe schedule [time-range-name]	[time-range-name]	Remove PoE schedule setting on the port.
Show command		
Switch(config)# show poe status		Show the current status of overall PoE
Switch(config)# show poe interface		Show the current status of Powered Device and Operation used on each port.
Switch(config)# show poe interface [port_list]		Show the current status of Powered Device and Operation on specified port
Switch(config)# show poe interface schedule		Show the current schedule used on each port.
Switch(config)# show poe interface schedule [port_list]		Show the current schedule used on specified port.

12. To set up static MAC address table

Command	Parameter	Description
Switch(config-if-PORT-PORT)# mac address-table static-mac [xx:xx:xx:xx:xx:xx] vlan	[xx:xx:xx:xx:xx:xx:]	Specify a static MAC address
	[1-4094]	Specify VLAN ID

[1-4094]		
No command		
Switch(config-if-PORT-PORT)# no mac address-table static-mac [xx:xx:xx:xx:xx:xx] vlan [1-4094]	[xx:xx:xx:xx:xx:]	Delete static MAC address entry
	[1-4094]	

6.5.20 show interface statistics command

The command “show interface statistics” that displays port traffic statistics, port packet error statistics and port analysis history can be used either in Privileged mode # and Global Configuration mode (config)#. The “show interface statistics” command is useful for network administrators to diagnose and analyze the port traffic real-time conditions.

Command	Parameter	Description
Switch(config)# show interface statistics analysis		Display the accumulated packets analysis for each port.
Switch(config)# show interface statistics analysis [port_list]	[port_list]	Display the accumulated packets analysis of the selected ports.
Switch(config)# show interface statistics analysis rate		Display the real-time packets analysis for each port.
Switch(config)# show interface statistics analysis rate [port_list]	[port_list]	Display the real-time packets analysis of the selected ports.
Switch(config)# show interface statistics error		Display the accumulated error packets statistics for each port.
Switch(config)# show interface statistics error [port_list]	[port_list]	Display the accumulated error packets statistics for the selected ports.
Switch(config)# show interface statistics error rate		Display the real-time error packets statistics for each port.
Switch(config)# show interface statistics error rate [port_list]	[port_list]	Display the real-time error packets statistics for the selected ports.
Switch(config)# show interface statistics traffic		Display the accumulate traffic statistics for each port.
Switch(config)# show interface statistics traffic [port_list]	[port_list]	Display the accumulated traffic statistics for the selected ports.
Switch(config)# show interface statistics traffic rate		Display the real-time traffic statistics for each port.
Switch(config)# show interface statistics traffic rate [port_list]	[port_list]	Display the real-time traffic statistics for the selected ports.
Switch(config)# show interface statistics clear		Clear all statistics counters.

6.5.21 show sfp command

When you slide in SFP transceivers, the detailed information about this module can be viewed by using this command.

Command	Description
Switch(config)# show sfp information	Display the slide-in SFP information including speed, distance, vendor name, vendor PN and vendor serial number.
Switch(config)# show sfp state	Display the slide-in SFP information including temperature, voltage, TX bias, TX power, and RX power.

6.5.22 show log command

Command	Description
Switch(config)# show log	Show the event logs currently stored in the Managed Industrial PoE Switch. The total number of event logs that can be displayed is 500.

6.5.23 show default-config, running-config and start-up-config command

Command	Description
Switch(config)# show default-config	Display the original configurations assigned to the Managed Industrial PoE Switch by the factory.
Switch(config)# show running-config	Display the configurations currently used in the Managed Industrial PoE Switch. Please note that you must save running configurations into your switch flash before rebooting or restarting the device.
Switch(config)# show start-up-config	Display the system configurations that are stored in flash.

7. WEB MANAGEMENT

The Managed Industrial PoE Switch can be managed via a Web browser. The default IP of the Managed Industrial PoE Switch is **"http://192.168.0.1"**. You can change the Switch's IP address to the needed one later in its **Network Management** menu.

Follow these steps to manage the Managed Industrial PoE Switch through a Web browser:

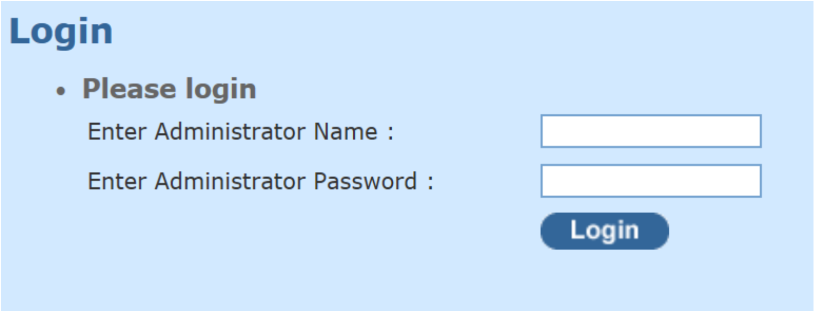
1. Use the RS-232 RJ-45 console port or one of the 10/100/1000Base-T RJ-45 ports (as the temporary RJ-45 Management console port) to login the Managed Industrial PoE Switch and set up the assigned IP parameters including the following:

   - IP address
   - Subnet Mask
   - Default Gateway IP address, if required

2. Run a Web browser and specify the Managed Industrial PoE Switch's IP address to reach it. (The Managed Industrial PoE Switch can be reached at **"http://192.168.0.1"** before any change.)

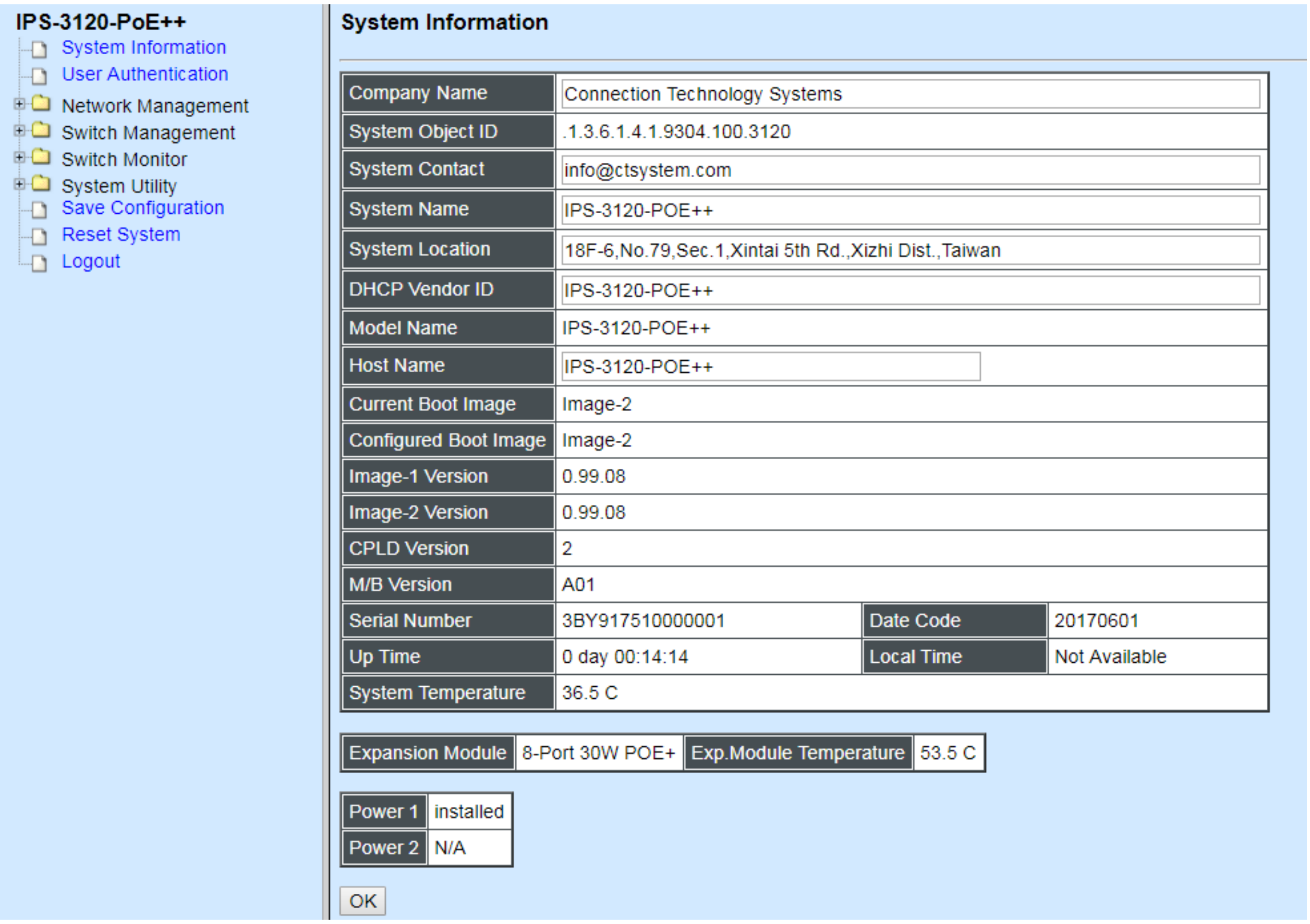
3. Login to the Managed Industrial PoE Switch.

Once you gain the access, you are requested to login.



Enter the administrator name and password for the initial login and then click "Login". The default administrator name is ***admin*** and without a password (leave the password field blank).

After a successful login, the screen page is shown as below:



System Information

Company Name	Connection Technology Systems		
System Object ID	.1.3.6.1.4.1.9304.100.3120		
System Contact	info@ctsystem.com		
System Name	IPS-3120-POE++		
System Location	18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan		
DHCP Vendor ID	IPS-3120-POE++		
Model Name	IPS-3120-POE++		
Host Name	IPS-3120-POE++		
Current Boot Image	Image-2		
Configured Boot Image	Image-2		
Image-1 Version	0.99.08		
Image-2 Version	0.99.08		
CPLD Version	2		
M/B Version	A01		
Serial Number	3BY917510000001	Date Code	20170601
Up Time	0 day 00:14:14	Local Time	Not Available
System Temperature	36.5 C		

Expansion Module	8-Port 30W POE+	Exp.Module Temperature	53.5 C

Power 1	installed
Power 2	N/A

1. **System Information:** Name the Managed Industrial PoE Switch, specify the location and check the current version of information.

2. **User Authentication:** Create and view the registered user list.

3. **Network Management:** Set up or view the IP address and related information about the Managed Industrial PoE Switch required for network management applications.

4. **Switch Management:** Set up switch or port configuration, VLAN configuration, QoS and other functions.

5. **Switch Monitor:** View the operation status and traffic statistics of the ports.

6. **System Utility:** Upgrade firmware and load factory settings.

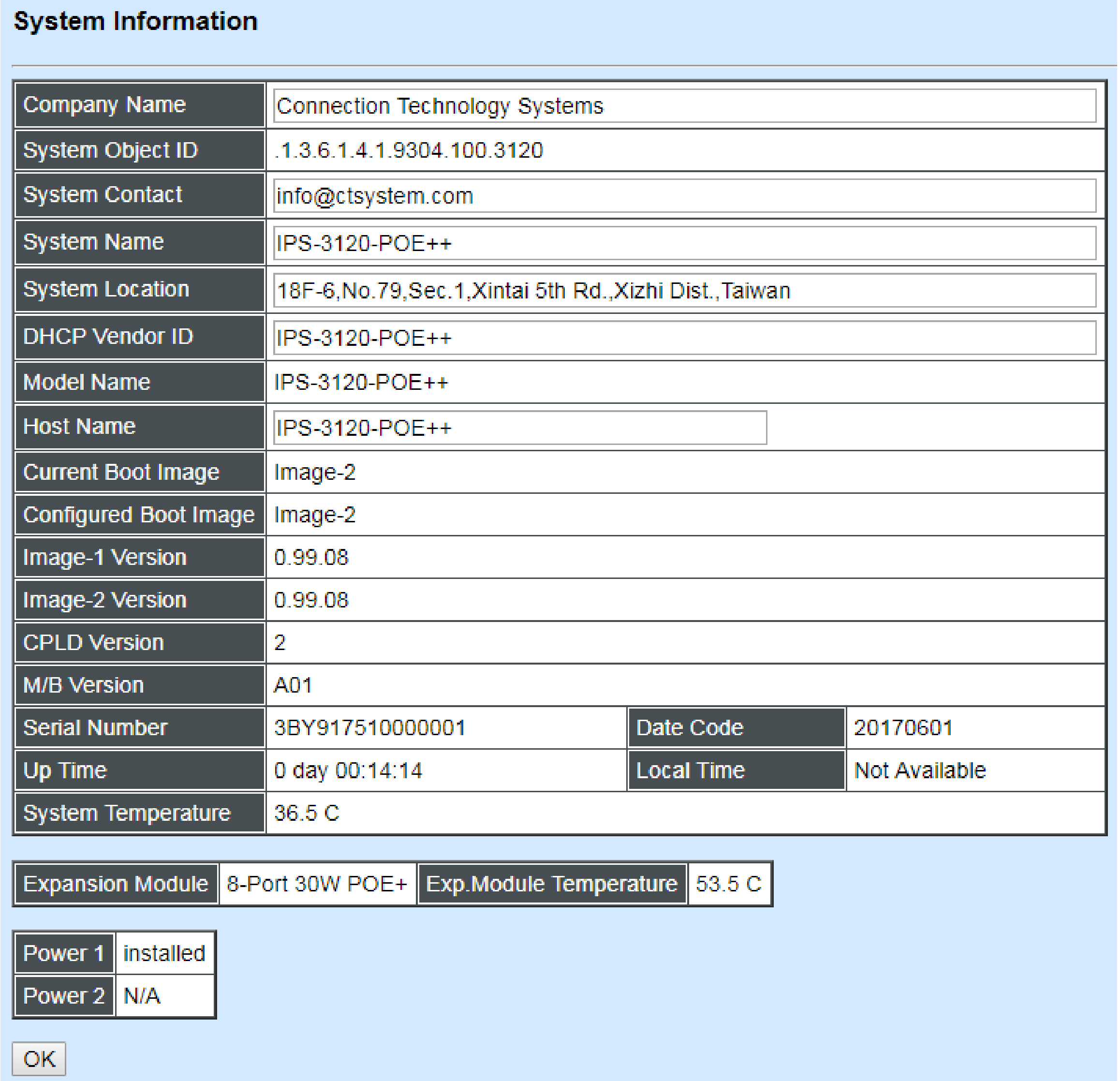
7. **Save Configuration:** Save all changes to the system.

8. **Reset System:** Reset the Managed Industrial PoE Switch.

9. **Logout:** Exit the management interface.

7.1 System Information

Select **System Information** from the left column and then the following screen page shows up.



System Information

Company Name	Connection Technology Systems
System Object ID	.1.3.6.1.4.1.9304.100.3120
System Contact	info@ctsystem.com
System Name	IPS-3120-POE++
System Location	18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan
DHCP Vendor ID	IPS-3120-POE++
Model Name	IPS-3120-POE++
Host Name	IPS-3120-POE++
Current Boot Image	Image-2
Configured Boot Image	Image-2
Image-1 Version	0.99.08
Image-2 Version	0.99.08
CPLD Version	2
M/B Version	A01
Serial Number	3BY917510000001
Date Code	20170601
Up Time	0 day 00:14:14
Local Time	Not Available
System Temperature	36.5 C

Expansion Module	8-Port 30W POE+	Exp.Module Temperature	53.5 C

Power 1	installed
Power 2	N/A

Company Name: Enter a company name up to 55 alphanumeric characters for this Managed Industrial PoE Switch.

System Object ID: View-only field that shows the predefined System OID.

System Contact: Enter contact information up to 55 alphanumeric characters for this Managed Industrial PoE Switch.

System Name: Enter a unique name up to 55 alphanumeric characters for this Managed Industrial PoE Switch. Use a descriptive name to identify the Managed Industrial PoE Switch in relation to your network, for example, “Backbone 1”. This name is mainly used for reference.

System Location: Enter a brief description of the Managed Industrial PoE Switch location up to 55 alphanumeric characters. The location shown is for reference only.

DHCP Vendor ID: Enter the user-defined vendor ID up to 55 alphanumeric characters. Please make sure you have an exact DHCP Vendor ID with the value specified in “vendor-classes” in your dhcp.conf file. For detailed information, see Appendix A.

Model Name: View-only field that shows the product’s model name.

Host Name: View-only field that shows the product’s host name.

Current Boot Image: View-only field that shows the image in use.

Configured Boot Image: View-only field that shows the image which would be used after rebooting.

Image-1 Version: View-only field that shows the firmware version of the first image.

Image-2 Version: View-only field that shows the firmware version of the second image.

1000M Port Number: The number of ports transmitting at the speed of 1000Mbps.

100M Port Number: The number of ports transmitting at the speed of 100Mbps.

M/B Version: View-only field that shows the main board version.

Serial Number: View-only field that shows the serial number of this switch.

Date Code: View-only field that shows the Managed Industrial PoE Switch firmware date code.

Up time: View-only field that shows how long the device has been powered on.

Local Time: View-only field that shows the time of the location where the switch is.

CPU Temperature: View-only field that shows the current temperature of the CPU.

PHY1 Temperature: A PHY connects a link layer device to a physical medium such as an copper cable optical fiber. View-only field that shows the PHY 1's temperature.

PHY2 Temperature: View-only field that shows the PHY 2's temperature.

PHY3 Temperature: View-only field that shows the PHY 3's temperature.

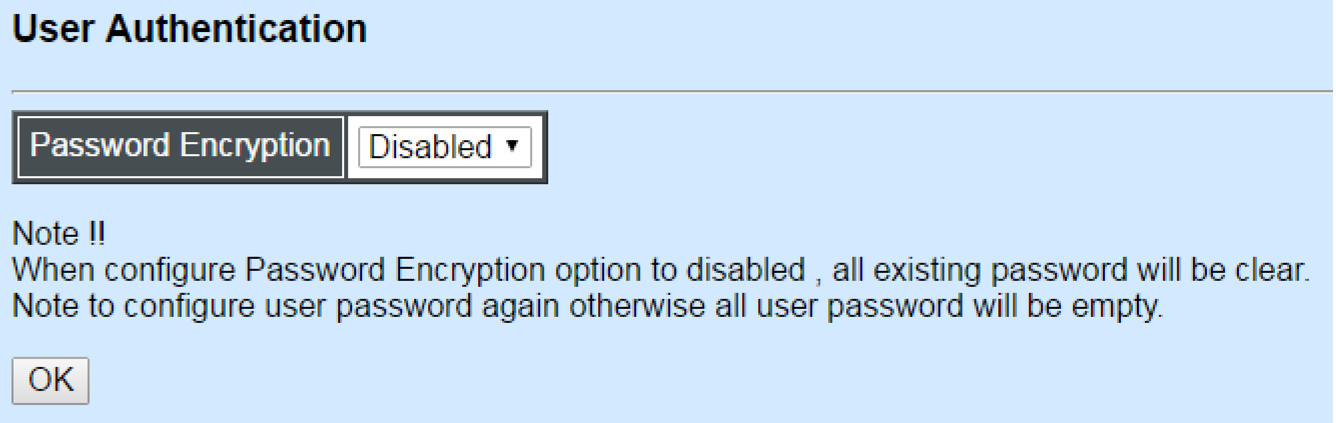
Click the **“OK”** button to apply the modifications.

***Fiber 2 information for 2-fiber model only**

7.2 User Authentication

To prevent any un-authorized access, only registered users are allowed to access the Managed Industrial PoE Switch. Users who want to access the Managed Industrial PoE Switch need to register in the user’s list first.

To view or change current registered users, select **User Authentication** from the left column and then the following screen page shows up.

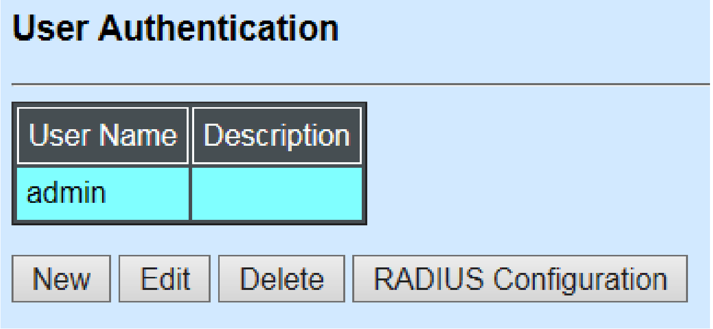


User Authentication

Password Encryption: Disabled ▾

Note !!
When configure Password Encryption option to disabled , all existing password will be clear.
Note to configure user password again otherwise all user password will be empty.

Password Encryption: Click drop-down box to disable or enable MD5(Message-Digest Algorithm). It is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. The default setting is disabled.



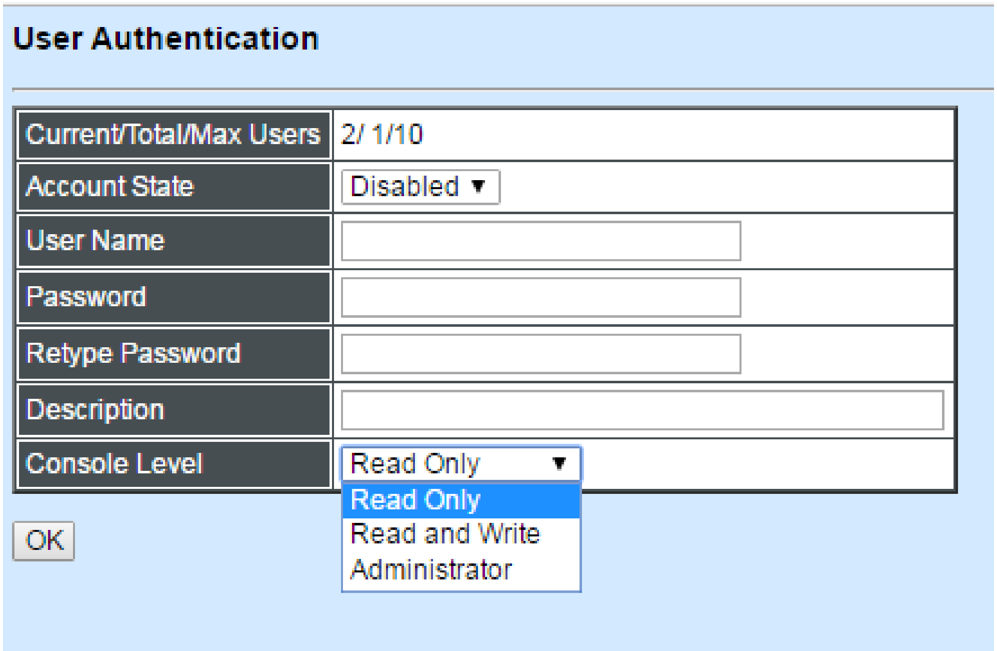
User Authentication

User Name	Description
admin	

Click **New** to add a new user account, then the following screen page appears.

Click **Edit** to view and edit a registered user setting.

Click **Delete** to remove a registered user setting.



User Authentication

Current/Total/Max Users	2/ 1/10
Account State	Disabled ▾
User Name	
Password	
Retype Password	
Description	
Console Level	Read Only ▾

Current/Total/Max Users: View-only field

Current: This shows the number of current registered user.

Total: This shows the number of the registered users.

Max: This shows the maximum number available for registration. The maximum number is 10.

Account State: Enable or disable the selected account.

User Name: Specify the authorized user login name, up to 20 alphanumeric characters.

Password: Enter the desired user password, up to 20 alphanumeric characters.

Retype Password: Enter the password again to confirm.

Description: Enter a unique description up to 35 alphanumeric characters for this user. This is mainly for reference only.

Console Level: Select the preferred access level for this newly created account.

Administrator: Full access right, including maintaining the user account, system information, loading factory settings, etc.

Read & Write: Partial access right, unable to modify the system information, user account, load factory settings and firmware upgrade.

Read Only: Read only access right.

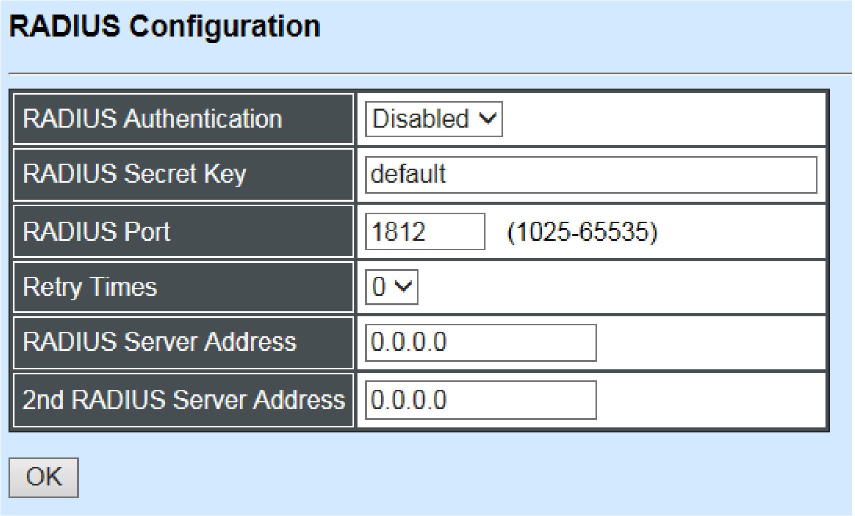
NOTE: *If you forget the login password, the only way to gain access to the Web Management is to set the Managed Industrial PoE Switch back to the factory default setting by pressing the Reset button for 10 seconds (The Reset button is located on the Front Panel of the Managed Industrial PoE Switch.).*

When the Managed Industrial PoE Switch returns back to the default setting, you can log in with the default login username and password (By default, no password is required. Leave the field empty and then press Login.)

Click the **"OK"** button to apply the settings.

RADIUS Configuration

Click **RADIUS Configuration** in **User Authentication** and then the following screen page appears.



RADIUS Configuration

RADIUS Authentication	Disabled
RADIUS Secret Key	default
RADIUS Port	1812 (1025-65535)
Retry Times	0
RADIUS Server Address	0.0.0.0
2nd RADIUS Server Address	0.0.0.0

When **RADIUS Authentication** is enabled, User Login will be according to those settings on the RADIUS server(s).

NOTE: *For advanced RADIUS Server setup, please refer to APPENDIX B or the "free RADIUS readme.txt" file on the disc provided with this product.*

Secret Key: The word to encrypt data of being sent to RADIUS server.

RADIUS Port: The RADIUS service port on RADIUS server. The default value is "1812".

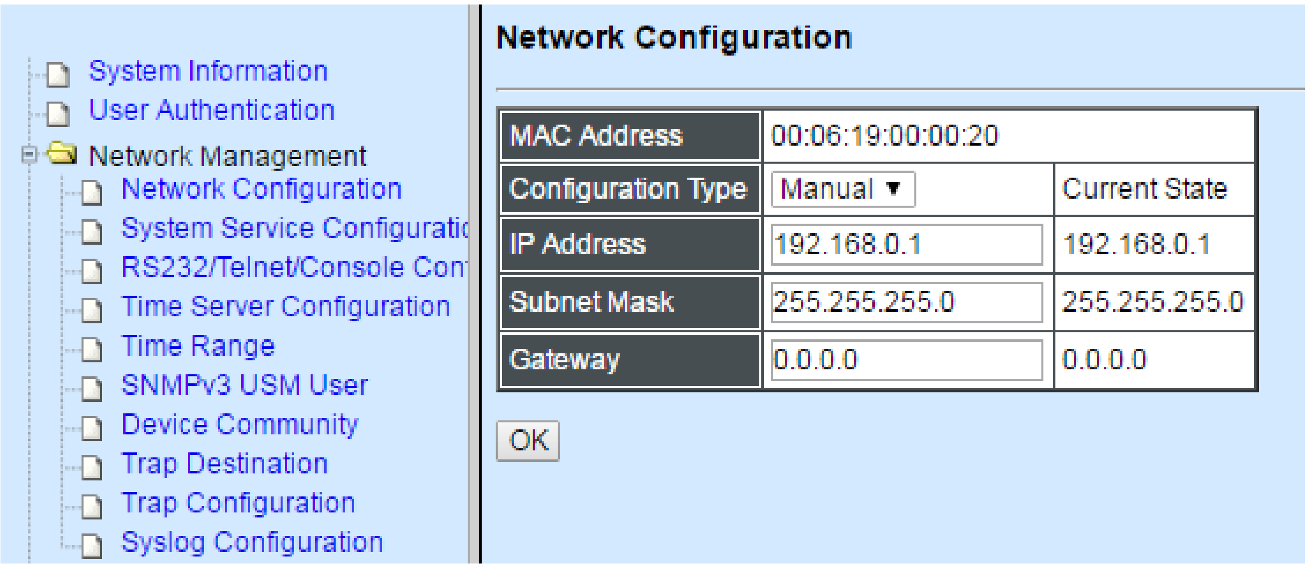
Retry Time: Times of trying to reconnect if the RADIUS server is not reachable. The default value is "0".

RADIUS Server Address: The IP address of the first RADIUS server.

2nd RADIUS Server Address: The IP address of the second RADIUS server.

7.3 Network Management

In order to enable network management of the Managed Industrial PoE Switch, proper network configuration is required. To do this, click the folder **Network Management** from the left column and then the following screen page appears.



Network Configuration

MAC Address	00:06:19:00:00:20	
Configuration Type	Manual ▼	Current State
IP Address	192.168.0.1	192.168.0.1
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0

1. **Network Configuration:** Set up the required IP configuration of the Managed Industrial PoE Switch.

2. **System Service Configuration:** Set up the system service type.

3. **RS232/Telnet/Console Configuration:** Set up RS232/Telnet/Console configuration.

4. **Time Server Configuration:** Set up the time server’s configuration.

5. **Time Range:** Set up an event at a period of time specified.

6. **SNMPv3 USM User:** View the registered SNMPv3 user name list. Edit an existing user name.

7. **Device Community:** View the registered SNMP community name list. Add a new community name or remove an existing community name.

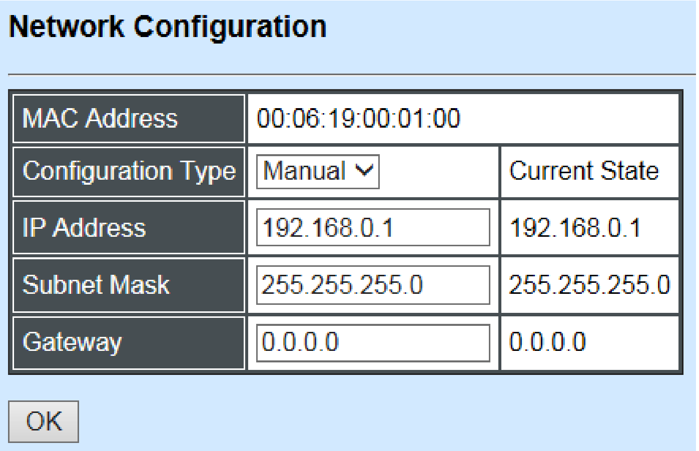
8. **Trap Destination:** View the registered SNMP trap destination list. Add a new trap destination or remove an existing trap destination.

9. **Trap Configuration:** View the Managed Switch trap configuration. Enable or disable a specific trap.

10. **Syslog Configuration:** Enable or disable Log Server and set up its IP configuration.

7.3.1 Network Configuration

Click the option **Network Configuration** from the **Network Management** menu and then the following screen page appears.



Network Configuration

MAC Address	00:06:19:00:01:00	
Configuration Type	Manual	Current State
IP Address	192.168.0.1	192.168.0.1
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0

MAC Address: This view-only field shows the unique and permanent MAC address pre-assigned to the Managed Industrial PoE Switch. You cannot change the Managed Industrial PoE Switch's MAC address.

Configuration Type: There are two configuration types that users can select from the pull-down menu: **"DHCP"** and **"Manual"**. When **"DHCP"** is selected and a DHCP server is also available on the network, the Managed Industrial PoE Switch will automatically get the IP address from the DHCP server. If "**Manual"** is selected, users need to specify the IP address, Subnet Mask and Gateway.

NOTE: *This* Managed Industrial PoE Switch *supports auto-provisioning function that enables DHCP clients to automatically download the latest firmware and configuration image from the server. For information about how to set up a DHCP server, please refer to APPENDIX A.*

IP Address: Enter the unique IP address for this Managed Industrial PoE Switch. You can use the default IP address or specify a new one when the address duplication occurs or the address does not match up with your network. (The default factory setting is 192.168.0.1.)

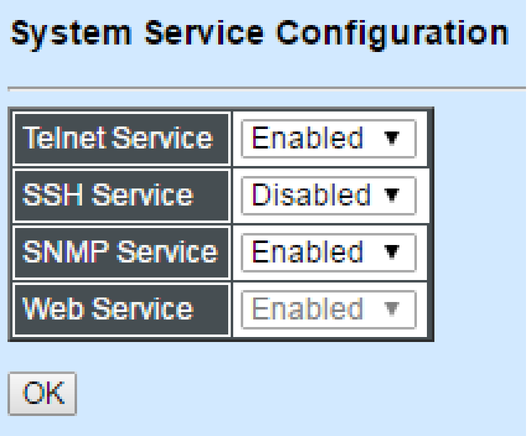
Subnet Mask: Specify the subnet mask. The default subnet mask values for the three Internet address classes are as follows:

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

Gateway: Specify the IP address of a gateway or a router, which is responsible for the delivery of the IP packets sent by the Managed Industrial PoE Switch. This address is required when the Managed Industrial PoE Switch and the network management station are on different networks or subnets. The default value of this parameter is 0.0.0.0, which means no gateway exists and the network management station and Managed Industrial PoE Switch are on the same network.

7.3.2 System Service Configuration

Click the option **System Service Configuration** from the **Network Management** menu and then the following screen page appears.



System Service Configuration

Telnet Service	Enabled ▼
SSH Service	Disabled ▼
SNMP Service	Enabled ▼
Web Service	Enabled ▼

Telnet Service: Select **Disabled** or **Enabled** for the system service type.

SSH Service: Select **Disabled** or **Enabled** for the system service type.

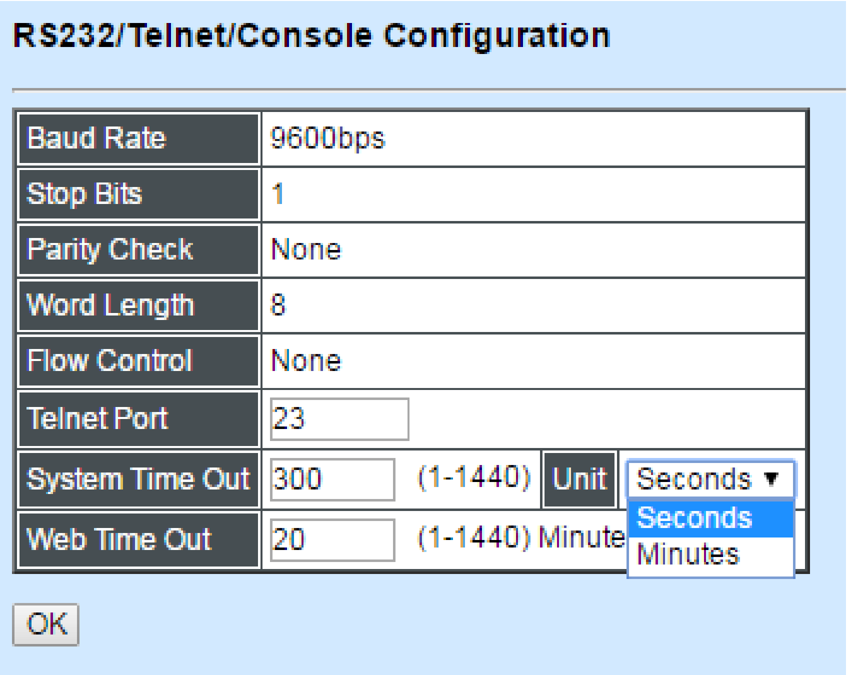
SNMP Service: Select **Disabled** or **Enabled** for the system service type.

Web Service: It is a view-only field. Web service cannot be disabled.

Click the **"OK"** button to apply the settings.

7.3.3 RS232/Telnet/Console Configuration

Click the option **RS232/Telnet/Console Configuration** from the **Network Management** menu and then the following screen page appears.



RS232/Telnet/Console Configuration

Baud Rate	9600bps		
Stop Bits	1		
Parity Check	None		
Word Length	8		
Flow Control	None		
Telnet Port	23		
System Time Out	300 (1-1440)	Unit	Seconds ▼
Web Time Out	20 (1-1440) Minute		

Baud Rate: View-only field that displays *9600bps* for RS-232 setting.

Stop Bits: View-only field that displays *1* for RS-232 setting.

Parity Check: View-only field that displays *None* for RS-232 setting.

Word Length: View-only field that displays *8* for RS-232 setting.

Flow Control: View-only field that displays *None* for RS-232 setting.

Telnet Port: Specify the desired TCP port number for the Telnet console. The default TCP port number of Telnet is *23*.

System Time Out: Specify the desired time that the Managed Industrial PoE Switch will wait before disconnecting an inactive console/telnet. The default value is *300* seconds.

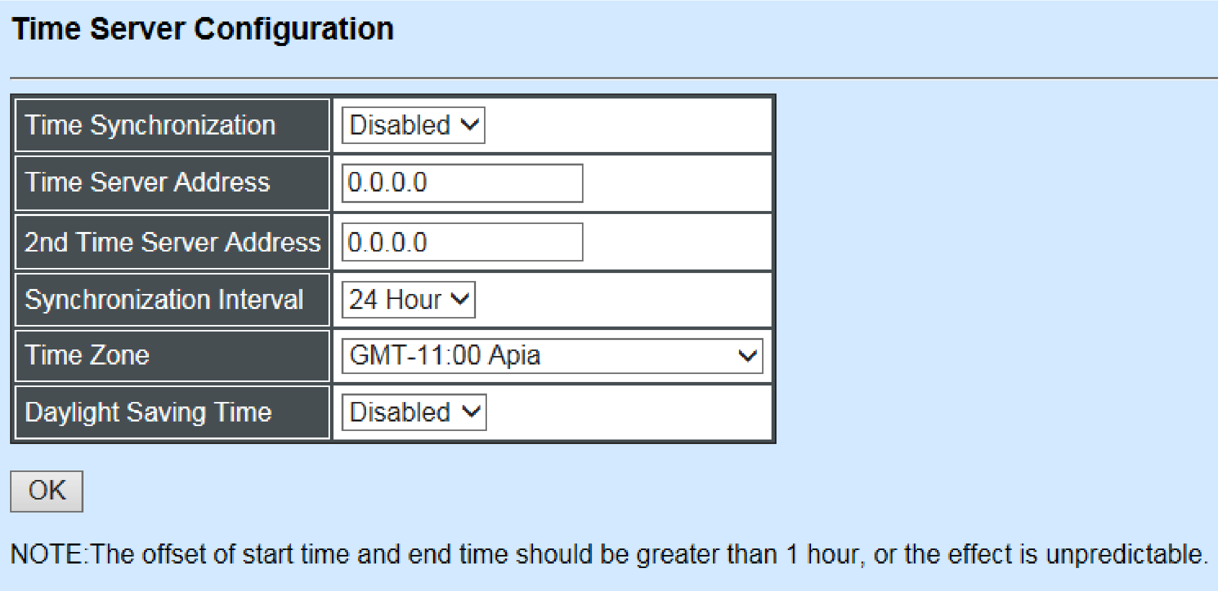
Unit: Select the unit is Seconds or Minutes.

Web Time Out: Specify the desired time that the Managed Industrial PoE Switch will wait before disconnecting an inactive web. The default value is *20* minutes.

Click the **"OK"** button to apply the settings.

7.3.4 Time Server Configuration

Click the option **Time Server Configuration** from the **Network Management** menu and then the following screen page appears.



Time Server Configuration

Time Synchronization	Disabled
Time Server Address	0.0.0.0
2nd Time Server Address	0.0.0.0
Synchronization Interval	24 Hour
Time Zone	GMT-11:00 Apia
Daylight Saving Time	Disabled

NOTE:The offset of start time and end time should be greater than 1 hour, or the effect is unpredictable.

Time Synchronization: Enable or disable the time synchronization.

Time Server Address: Specify the primary NTP time server address.

2nd Time Server Address: When the default time server is down, the Managed Industrial PoE Switch will automatically connect to the 2nd time server.

Synchronization Interval: The time interval to synchronize from NTP time server. The allowable value is from 1 hour to 24 hours.

Time Zone: Select the appropriate time zone from the pull-down menu.

Daylight Saving Time — To enable or disable the daylight saving time function. Daylight saving time is the practice of advancing clocks during summer months by one hour so that evening daylight lasts an hour longer, while sacrificing normal sunrise times.

Daylight Saving Time Date Start — Click the pull-down menu to select the annual start date of daylight saving time.

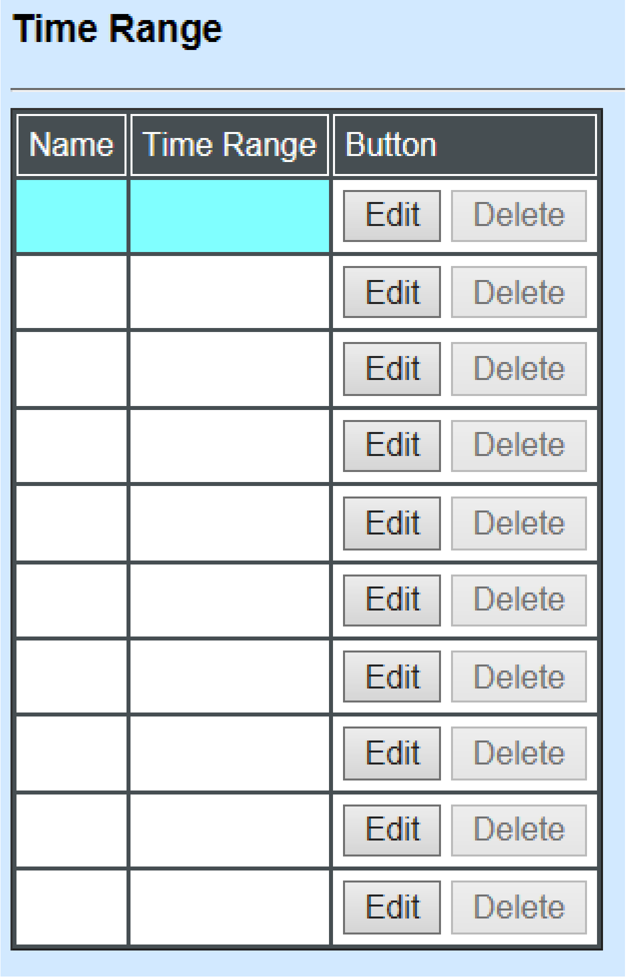
Daylight Saving Time Date End — Click the pull-down menu to select the annual end date of daylight saving time.

Click the **"OK"** button to apply the settings.

7.3.5 Time Range

This command defines a time interval to be activated on a daily or weekly basis. This is convenient to assign when a function should automatically take effect. Before using the function, make sure that gateway is set under either IPv4 mode in **Network Configuration** (Section 3.3.1) and time server is configured in **Time Server Configuration** (Section 3.3.4).

Time Range related function scheduling will only take effect when Switch system time is sync with NTP time server.



Time Range

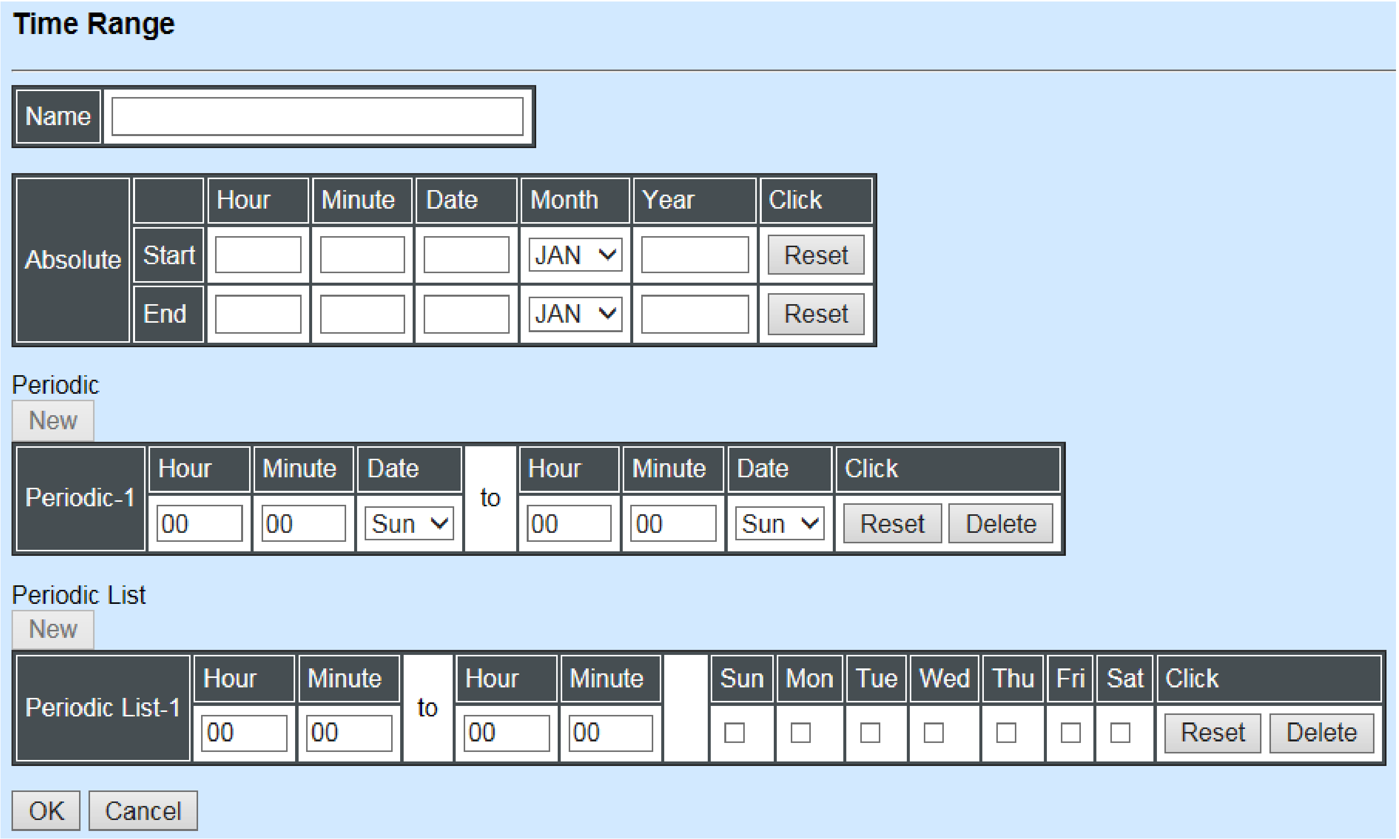
Name	Time Range	Button
		Edit Delete
		Edit Delete
		Edit Delete
		Edit Delete
		Edit Delete
		Edit Delete
		Edit Delete
		Edit Delete
		Edit Delete
		Edit Delete

This table displays the overview of each time range specified. 10 time ranges can be set at most.

Name: The given name for the time range.

Time Range: Displays detailed time intervals spefified.

Click **"Edit"** for further settings or **"Delete"** to erase the name or time range.



Time Range

Name	

		Hour	Minute	Date	Month	Year	Click
Absolute	Start				JAN		Reset
	End				JAN		Reset

Periodic

New

	Hour	Minute	Date		Hour	Minute	Date	Click
Periodic-1	00	00	Sun	to	00	00	Sun	Reset Delete

Periodic List

New

	Hour	Minute		Hour	Minute		Sun	Mon	Tue	Wed	Thu	Fri	Sat	Click
Periodic List-1	00	00	to	00	00		□	□	□	□	□	□	□	Reset Delete

OK Cancel

Name: Specify a name to the time interval. It receives 32 characters at most.

Absolute: An absolute interval to enable a function. Specify an absolute start time or end time to a time interval.

Where:

Hour	0-23
Minute	0-59
Date	1-31
Month	JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC
Year	2000-2097

Note: *No start time assigned refers to start immediately. One absolute start time can be set at most. No end time assigned refers to run a function continuously. One absolute end time can be set at most.*

Periodic: An interval to enable a function on a weekly basis. The periodic interval only takes effect within specified absolute interval.Specify weekly recurring time interval. Two periodic intervals can be set at most.

Where:

Hour 0-23

Minute 0-59

Days(7 days) including Monday(Mon), Tuesday(Tue), Wednesday(Wed), Thursday(Thu), Friday(Fri), Saturday(Sat), Sunday(Sun).

Periodic List: An interval to enable a function on a daily basis. The periodic list interval only takes effect within specified absolute interval. Specify a list of days in a week for periodic run.

Where:

Hour 0-23

Minute 0-59

days(7 days) including Monday(Mon), Tuesday(Tue), Wednesday(Wed), Thursday(Thu), Friday(Fri), Saturday(Sat), Sunday(Sun).

Cross-day setting is feasible. In other words, the second occurrence of time can be set on the following day, e.g. "22:00-2:00".

Note: *Two set of periodic list intervals can be set at most.*

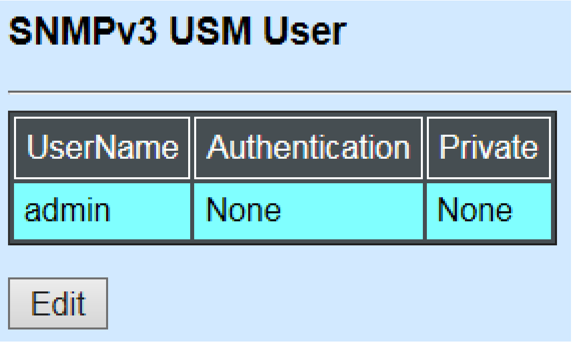
Under a time range name, user may add one absolute start time and one absolute end time at most. Users may also add two optional time ranges at most using Periodic and Periodic List time range.

For example, Users may set:
1. Two Periodic in time range, or
2. One Periodic and one Periodic List in time range, or
3. Two Periodic List in time range.

7.3.6 SNMPv3 USM User

Simple Network Management Protocol Version 3, SNMPv3 in short, features stronger security mechanism, including authentication and encryption that helps ensure that the message is from a valid source and scramble the content of a packet, to prevent from being learned by an unauthorized source. Select the option SNMPv3 USM User from the **Network Management** menu, then the **SNMPv3 USM Use**r page shows up.

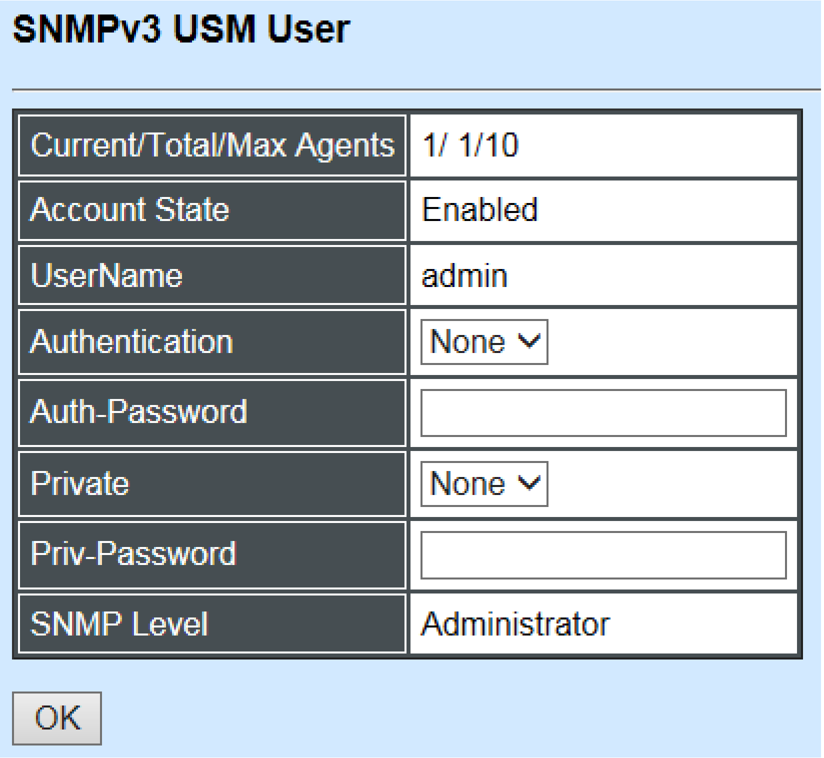
Note: *The SNMPv3 user account is generated from "User Authentication" (Section 4.2)*



SNMPv3 USM User

UserName	Authentication	Private
admin	None	None

Click **“Edit”** for further settings.



SNMPv3 USM User

Current/Total/Max Agents	1/ 1/10
Account State	Enabled
UserName	admin
Authentication	None
Auth-Password	
Private	None
Priv-Password	
SNMP Level	Administrator

Current/Total/Max Agents: View-only field.

Current: This shows the number of currently registered communities.

Total: This shows the number of total registered community users.

Max Agents: This shows the number of maximum number available for registration. The default maximum number is 10.

Account State: View-only field that shows this user account is enabled or disabled.

User Name: View-only field that shows the authorized user login name.

Authentication: This is used to ensure the identity of users. The following is the method to perform authentication.

None: Disable authentication function. Click “None” to disable it.

MD5(Message-Digest Algorithm): A widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. Click “MD5” to enable authentication.

SHA(Secure Hash Algorithm): A 160-bit hash function which resembles the said MD5 algorithm. Click “SHA” to enable authentication.

Auth-Password: Specify the passwords, up to 20 characters.

Private: It allows for encryption of SNMP v3 messages to ensure confidentiality of data. The following is the method to perform encryption.

None: Disable Private function. Click “None” to disable it.

DES(Data Encryption Standard): An algorithm to encrypt critical information such as message text message signatures…etc. Click “DES” to enable it.

Priv-Password: Specify the passwords, up to 20 characters.

SNMP-Level: View-only field that shows user’s authentication level.

Administrator: Full access right including maintaining user account & system information, load factory settings …etc.

Read & Write: Full access right but cannot modify user account & system information, cannot load factory settings.

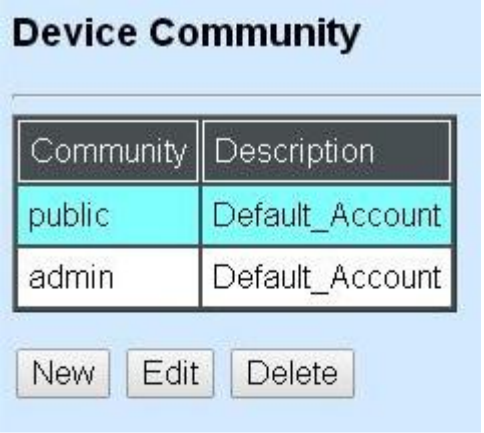
Read Only: Allow to view only.

A combination of a security event as below indicates which security mechanism is used when handling an SNMP packet.

Authentication	**Private**	**Result**
None	None	Uses a username match for authentication
Message Digest Algorithm(MD5) or Secure Hash Algorithm(SHA)	None	Provides authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms.
MD5 or SHA	Data Encryption Standard(DES)	Provides authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms. What’s more, provides DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES standard.

7.3.7 Device Community

Click the option **Device Community** from the **Network Management** menu and then the following screen page appears.



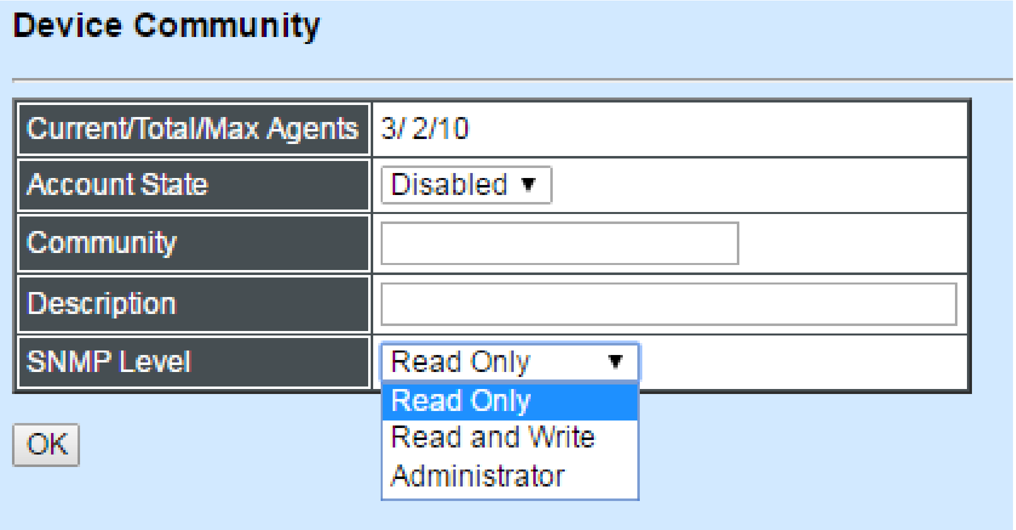
Device Community

Community	Description
public	Default_Account
admin	Default_Account

Click **New** to add a new community, then the following screen page appears.

Click **Edit** to view and edit a community setting.

Click **Delete** to remove a community setting.



Device Community

Current/Total/Max Agents	3/ 2/10
Account State	Disabled ▾
Community	
Description	
SNMP Level	Read Only ▾

Current/Total/Max Agents: View-only field.

Current: This shows the number of current community agents.

Total: This shows the total number of the community agents.

Max: This shows the maximum number available for configuration. The maximum number is 3.

Account State: Enable or disable the selected account.

Community: Specify the community name, up to 20 alphanumeric characters.

Description: Enter the description of the community, up to 20 alphanumeric characters.

SNMP Level: Select the preferred SNMP level for this newly created agent.

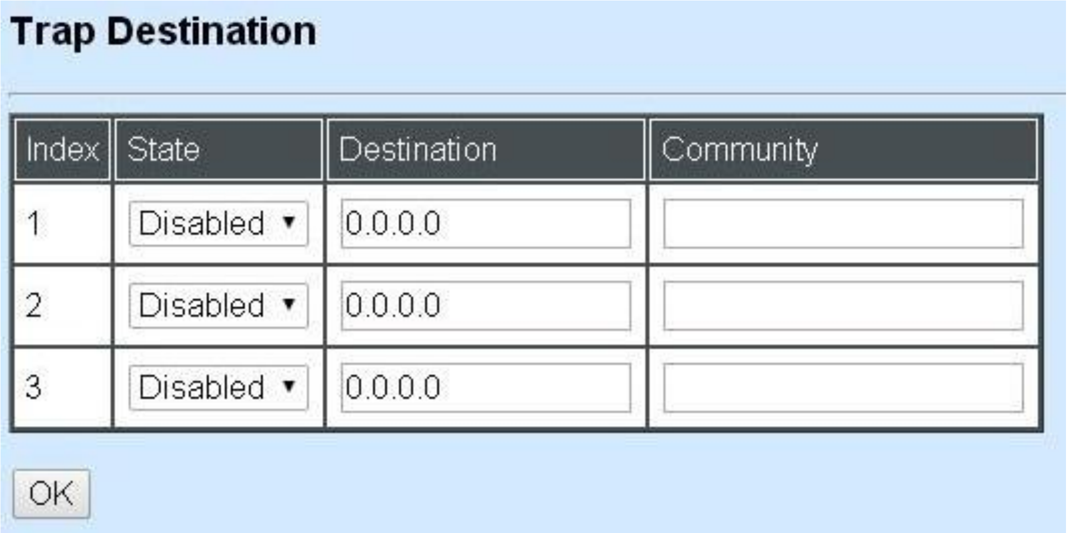
Administrator: Full access right.

Read & Write: Partial access right.

Read Only: Read only access right.

7.3.8 Trap Destination

Click the option **Trap Destination** from the **Network Management** menu and then the following screen page appears.



Trap Destination

Index	State	Destination	Community
1	Disabled ▾	0.0.0.0	
2	Disabled ▾	0.0.0.0	
3	Disabled ▾	0.0.0.0	

Index: The index of the SNMP trap destination.

State: Select **Disabled** or **Enabled** for the trap destination.

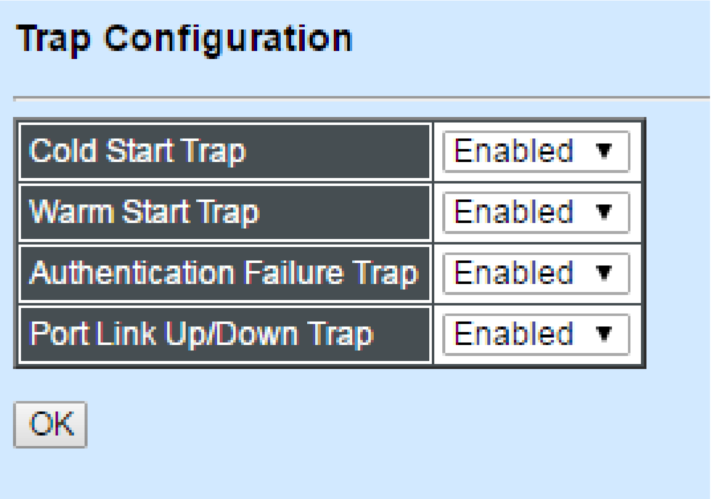
Destination: Set up IP address for the trap destination.

Community: Set up community for the specific trap destination.

Click the **"OK"** button to apply the settings.

7.3.9 Trap Configuration

Click the option **Trap Configuration** from the **Network Management** menu and then the following screen page appears.



Trap Configuration

Cold Start Trap	Enabled ▼
Warm Start Trap	Enabled ▼
Authentication Failure Trap	Enabled ▼
Port Link Up/Down Trap	Enabled ▼

Cold Start Trap: Select **Disabled** or **Enabled** for the SNMP trap.

Warm Start Trap: Select **Disabled** or **Enabled** for the SNMP trap.

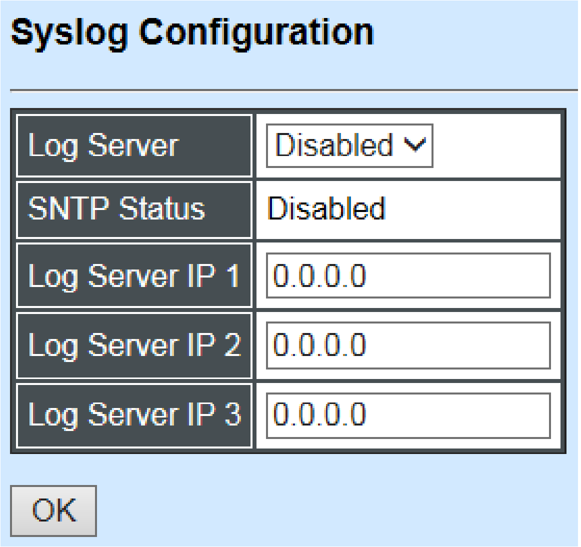
Authentication Failure Trap: Select **Disabled** or **Enabled** for the SNMP trap.

Port Link Up/Down Trap: Select **Disabled** or **Enabled** for the SNMP trap.

Click the **“OK”** button to apply the settings.

7.3.10 Syslog Configuration

Click the option **Syslog Configuration** from the **Network Management** menu and then the following screen page appears.



Syslog Configuration

Log Server	Disabled ⌄
SNTP Status	Disabled
Log Server IP 1	0.0.0.0
Log Server IP 2	0.0.0.0
Log Server IP 3	0.0.0.0

Log server: Select **Disabled** or **Enabled** for the Log server.

SNTP Status: View-only filed for the SNTP status

Log server IP 1: Set up the first Log server's IP address.

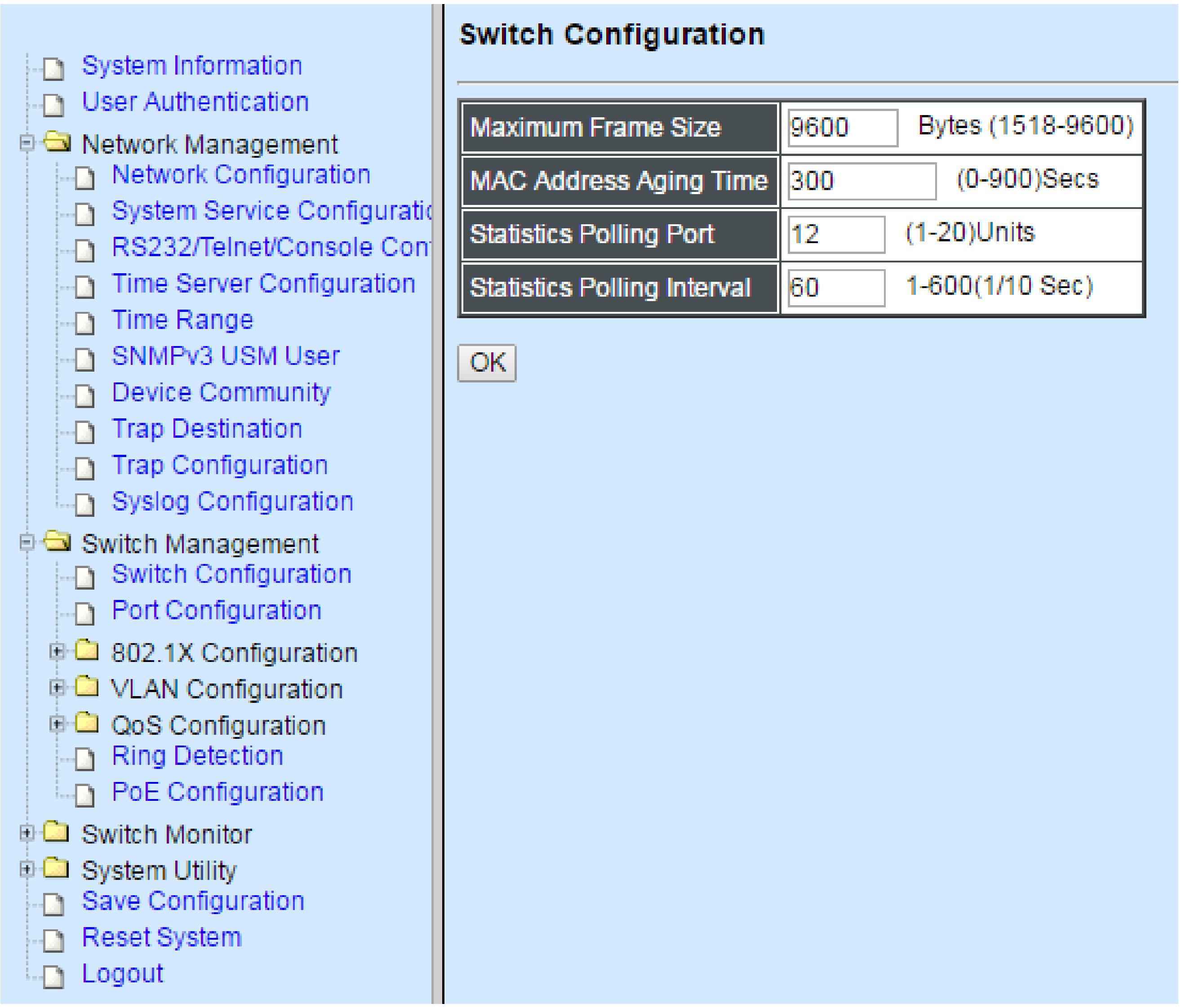
Log server IP 2: Set up the second Log server's IP address if needed

Log server IP 3: Set up the third Log server's IP address if needed.

Click the **"OK"** button to apply the settings.

7.4 Switch Management

To manage the Managed Industrial PoE Switch and set up required switching functions, click the folder **Switch Management** from the left column and then several options and folders will be displayed for your selection.



Switch Configuration

Maximum Frame Size	9600	Bytes (1518-9600)
MAC Address Aging Time	300	(0-900)Secs
Statistics Polling Port	12	(1-20)Units
Statistics Polling Interval	60	1-600(1/10 Sec)

1. **Switch Configuration:** Set up MAC address aging time, and enable/disable SFP Polling and Statistics Polling.

2. **Port Configuration:** Set up the port state, port type and flow control.

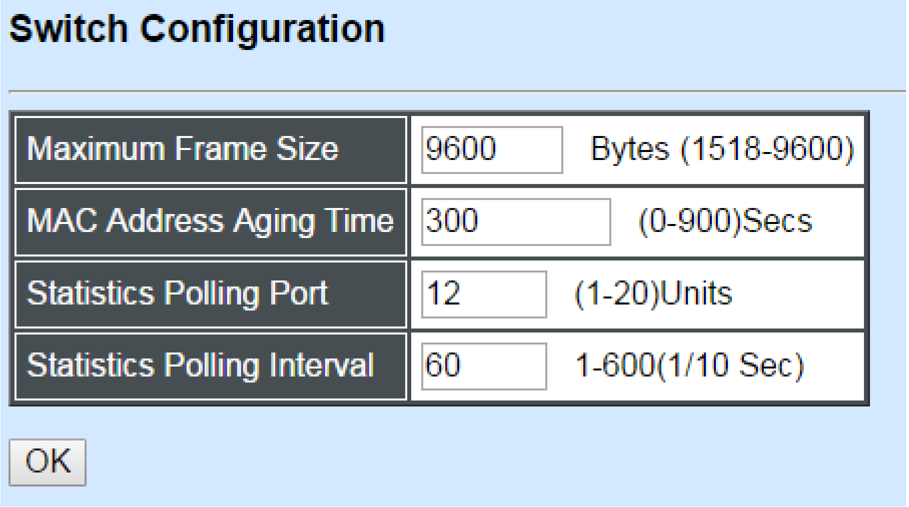
3. **802.1X Configuration:** Set up the 802.1X system, port Admin state, port reauthenticate.

4. **VLAN Configuration:** Set up IEEE 802.1q Tag VLAN and Port Based VLAN.

5. **QoS configuration:** QoS enables users to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

7.4.1 Switch Configuration

Click the option **Switch Configuration** from the **Switch Management** menu and then the following screen page appears.



Switch Configuration

Maximum Frame Size	9600 Bytes (1518-9600)
MAC Address Aging Time	300 (0-900)Secs
Statistics Polling Port	12 (1-20)Units
Statistics Polling Interval	60 1-600(1/10 Sec)

Maximum Frame Size: Specify the maximum frame size between 1518 and 9600 bytes. The default maximum frame size is 9600bytes.

MAC Address Aging Time: Specify MAC Address aging time between 0 and 900 seconds. “0” means that MAC addresses will never age out.

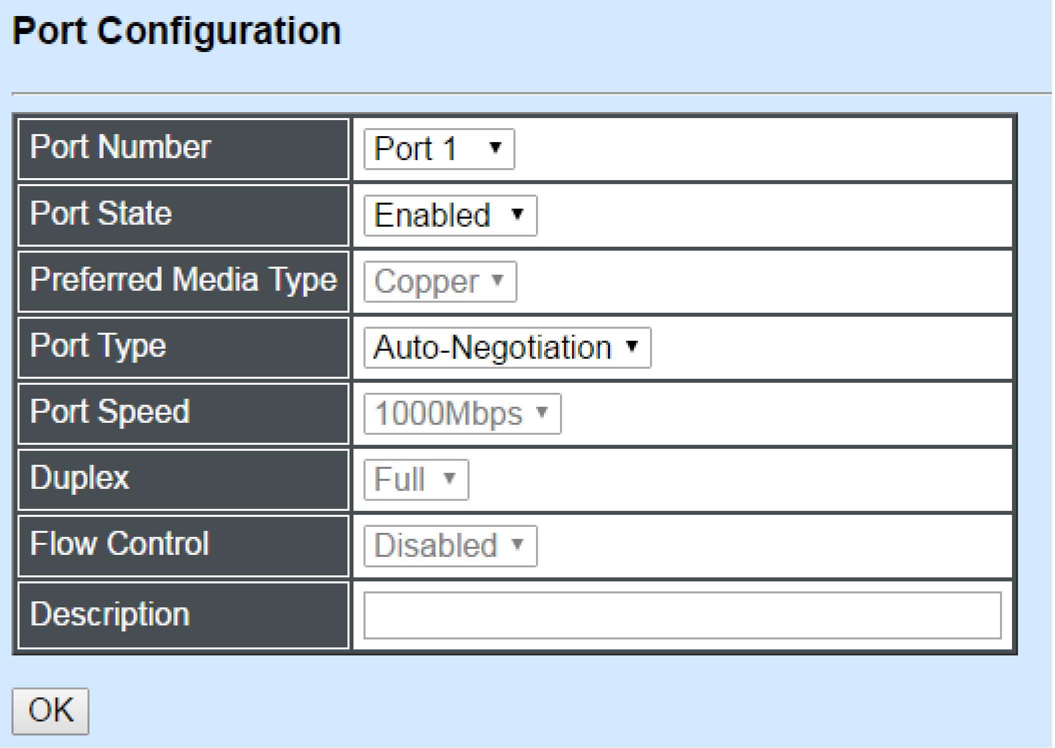
Statistics Polling Port: Specify the number of ports for data acquisition at a time.

Statistics Polling Interval: Specify the time interval in 1/10 seconds for data acquisition.

Click the **“OK”** button to apply the settings.

7.4.2 Port Configuration

Click the option **Port Configuration** from the **Switch Management** menu and then the following screen page appears.



Port Configuration

Port Number	Port 1
Port State	Enabled
Preferred Media Type	Copper
Port Type	Auto-Negotiation
Port Speed	1000Mbps
Duplex	Full
Flow Control	Disabled
Description	

Port Number: Click the pull-down menu to select the port number for configuration.

Port State: Enable or disable the selected port.

Preferred Media Type: This shows the media type (either Fiber or Copper) of the selected port. This field is open to select only when the selected port has two media type.

Port Type: Select Auto-Negotiation or Manual mode as the port type.

Port Speed: When you select Manual port type, you can further specify the transmission speed (10Mbps/100Mbps/1000Mbps/Auto-Sense) of the port(s).

Duplex: When you select Manual port type, you can further specify the current Duplex operation mode (full or half duplex) of the port(s).

Flow Control: Enable or disable Flow Control function.

Description: Add a remark to the description box for the port, up to 35 characters.

Click the **"OK"** button to apply the settings.

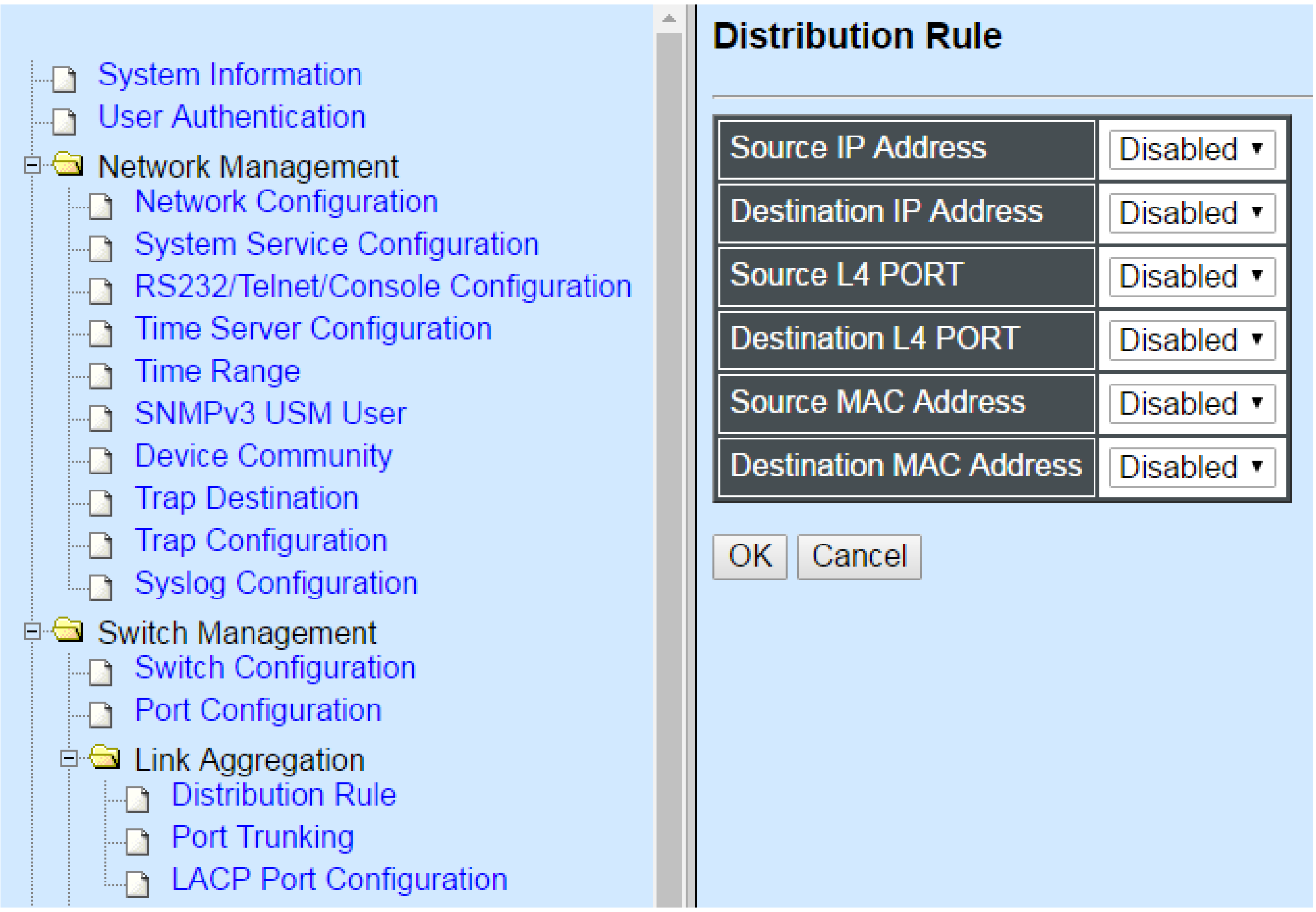
7.4.3 Link Aggregation

Link aggregation is an inexpensive way to set up a high-speed backbone network that transfers much more data than any one single port. Devices can deliver more data without replacing everything and buying new hardware.

For most backbone installations, it is common to install more cabling or fiber optic pairs than initially necessary, even if there is no immediate need for the additional cabling. This action is taken because labor costs are higher than the cost of the cable. Running extra cable reduces future labor costs if networking needs changes. Link aggregation can allow the use of these extra cables to increase backbone speeds with little or no extra cost if ports are available.

By Link Aggregation, devices are allowed to communicate simultaneously at their full single-port speed while any one single device would not occupy all available backbone capacities.

Click the **Link Aggregation** folder from the **Switch Management** menu and then two options will be displayed.



Distribution Rule

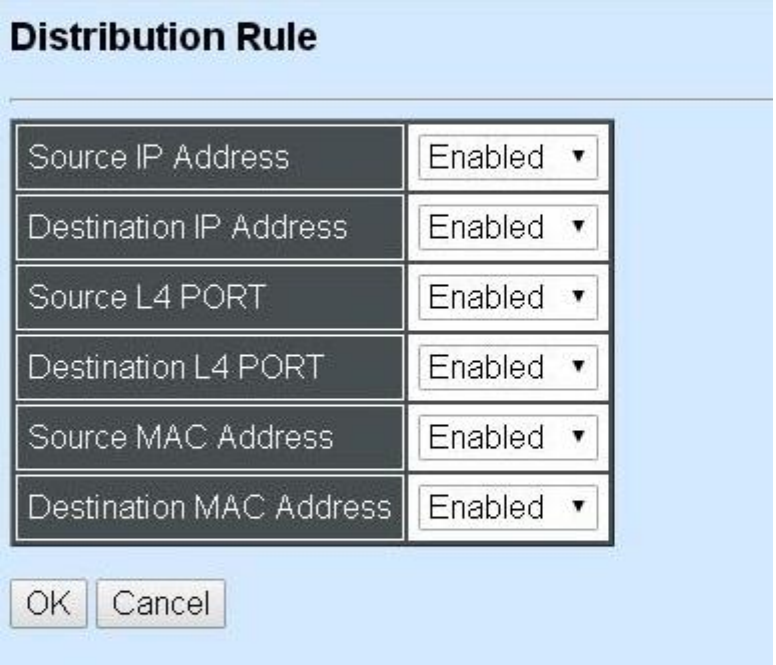
Source IP Address	Disabled
Destination IP Address	Disabled
Source L4 PORT	Disabled
Destination L4 PORT	Disabled
Source MAC Address	Disabled
Destination MAC Address	Disabled

Distribution Rule: Configure the distribution rule of Port Trunking group(s).

Port Trunking: Create, edit or delete port trunking group(s).

7.4.3.1 Distribution Rule

Click **Distribution Rule** from the **Link Aggregation** menu, the following screen page appears.



Distribution Rule

Source IP Address	Enabled
Destination IP Address	Enabled
Source L4 PORT	Enabled
Destination L4 PORT	Enabled
Source MAC Address	Enabled
Destination MAC Address	Enabled

There are six fields for you to set up packets according to operations.

Source IP Address: Enable or disable packets according to source IP address.

Destination IP Address: Enable or disable packets according to Destination IP address.

Source L4 Port: Enable or disable packets according to source L4 Port.

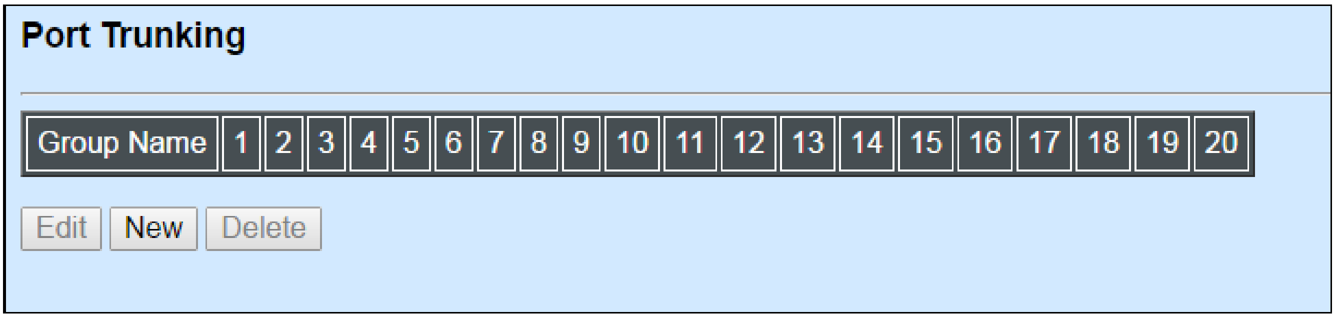
Destination L4 Port: Enable or disable packets according to Destination L4 Port.

Source MAC Address: Enable or disable packets according to source MAC address.

Destination MAC Address: Enable or disable packets according to Destination MAC address.

7.4.3.2 Port Trunking

Click **Port Trunking** from the **Link Aggregation** menu and then the following screen page appears.



Port Trunking

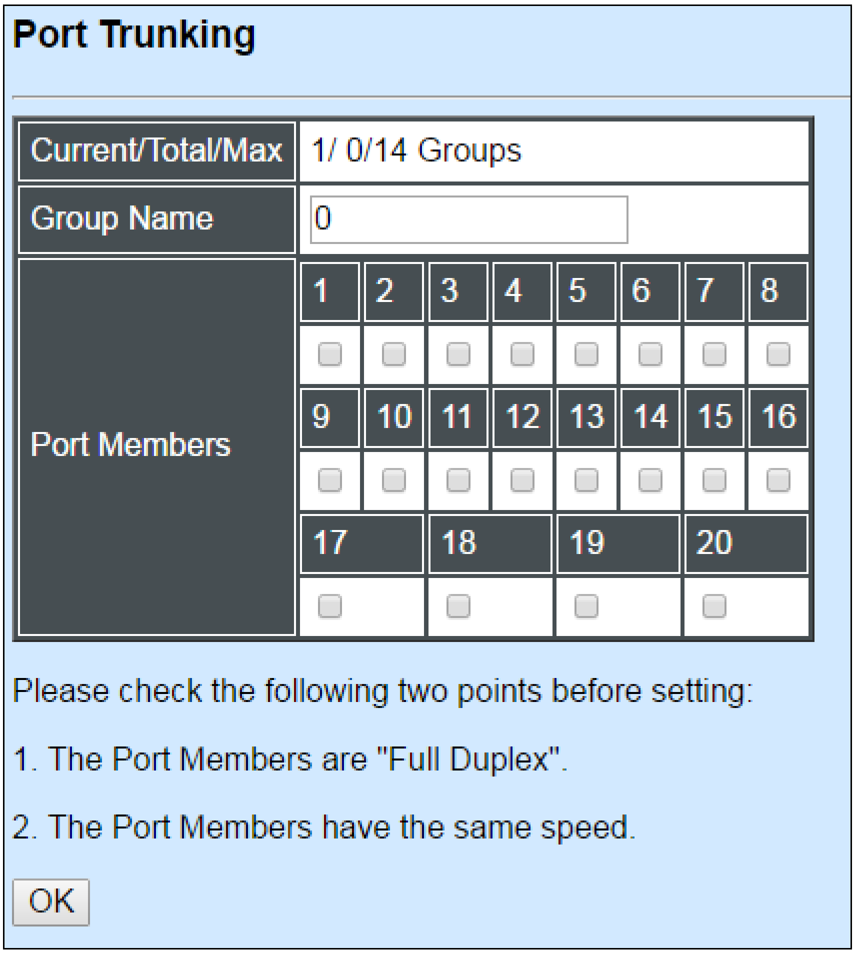
Group Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The Managed Industrial PoE Switch allows users to create at most 5 trunking groups. Each group consists of 2 to 6 links (ports).

Click **New** to add a new trunk group and then the following screen page appears.

Click **Delete** to remove a current registered trunking group setting.

Click **Edit** to view and edit a registered trunking group's settings.



Port Trunking

Current/Total/Max	1/ 0/14 Groups							
Group Name	0							
Port Members	1	2	3	4	5	6	7	8
	☐	☐	☐	☐	☐	☐	☐	☐
	9	10	11	12	13	14	15	16
	☐	☐	☐	☐	☐	☐	☐	☐
	17		18		19		20	
	☐		☐		☐		☐	

Please check the following two points before setting:

1. The Port Members are "Full Duplex".

2. The Port Members have the same speed.

OK

Current/Total/Max Groups: View-only field

Current: It shows the number of currently registered groups.

Total: It shows the number of total registered groups.

Max: It shows the maximum number of groups available for registration. The default maximum number is 5 groups.

Group Name: Specify a trunking group name, up to 15 alphanumeric characters.

Port Members: Select ports that belong to the specified trunking group. Please keep the rules below in mind when assigning ports to a trunking group:

- Must have 2 to 6 ports in each trunking group.

- Each port can only be grouped in one group.

Click **OK** and return back to **Link Aggregation** menu.

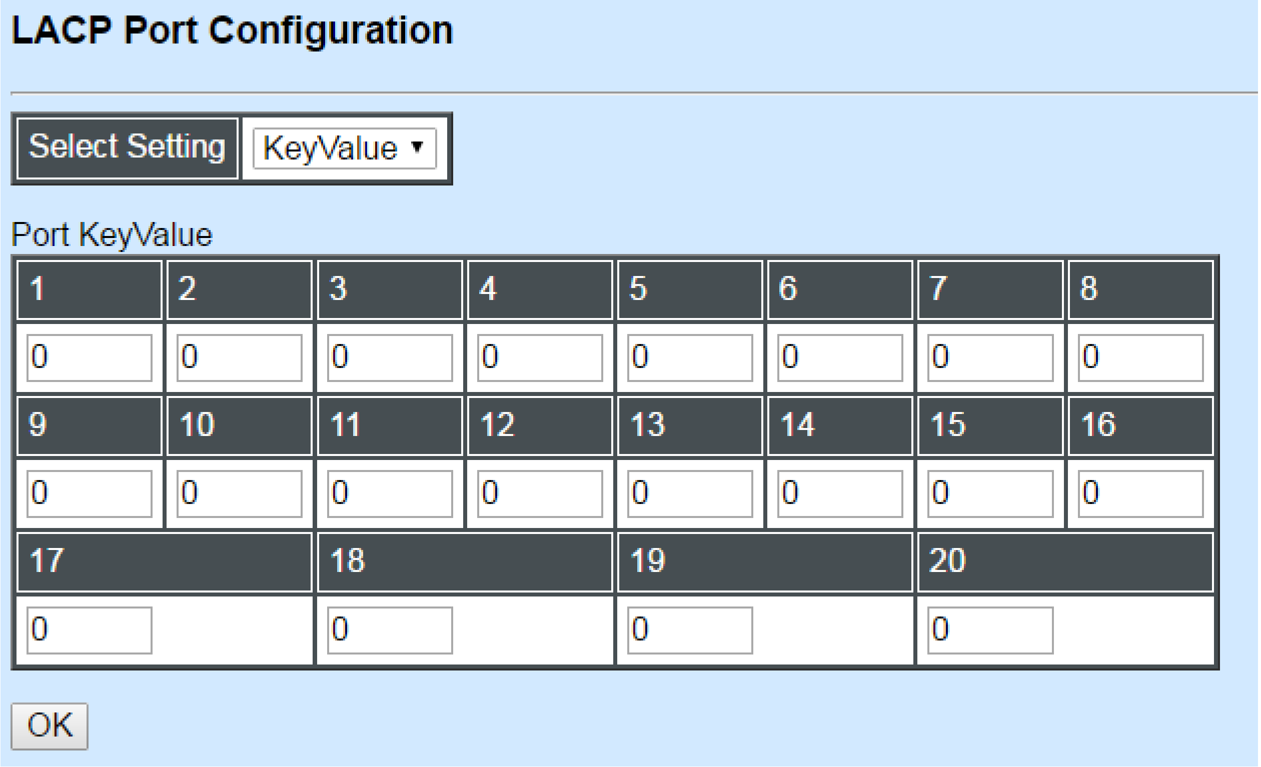
NOTE: *All trunking ports in the group must be members of the same VLAN, and QoS default priority configurations must be identical. Furthermore, all of the LACP aggregated links must be in the same speed and should be configured as full duplex.*

7.4.3.3 LACP Port Configuration

The Industrial Switch supports dynamic Link Aggregation Control Protocol (LACP) which is specified in IEEE 802.3ad. Static trunks have to be manually configured at both ends of the link. In other words, LACP configured ports can automatically negotiate a trunked link with LACP configured ports on other devices. You can configure any number of ports on the Managed Switch as LACP, as long as they are not already configured as part of a static trunk. If ports on other devices are also configured as LACP, the Managed Switch and the other devices will negotiate a trunk link between them. If an LACP trunk consists of more than four ports, all other ports will be placed in a standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

Configure Port Protocol:

Click the option **LACP Port Configuration** from the **Link Aggregation** menu and then select "Role" from the pull-down menu of Select Setting. The screen page is shown below.



LACP Port Configuration

Select Setting: KeyValue ▾

Port KeyValue

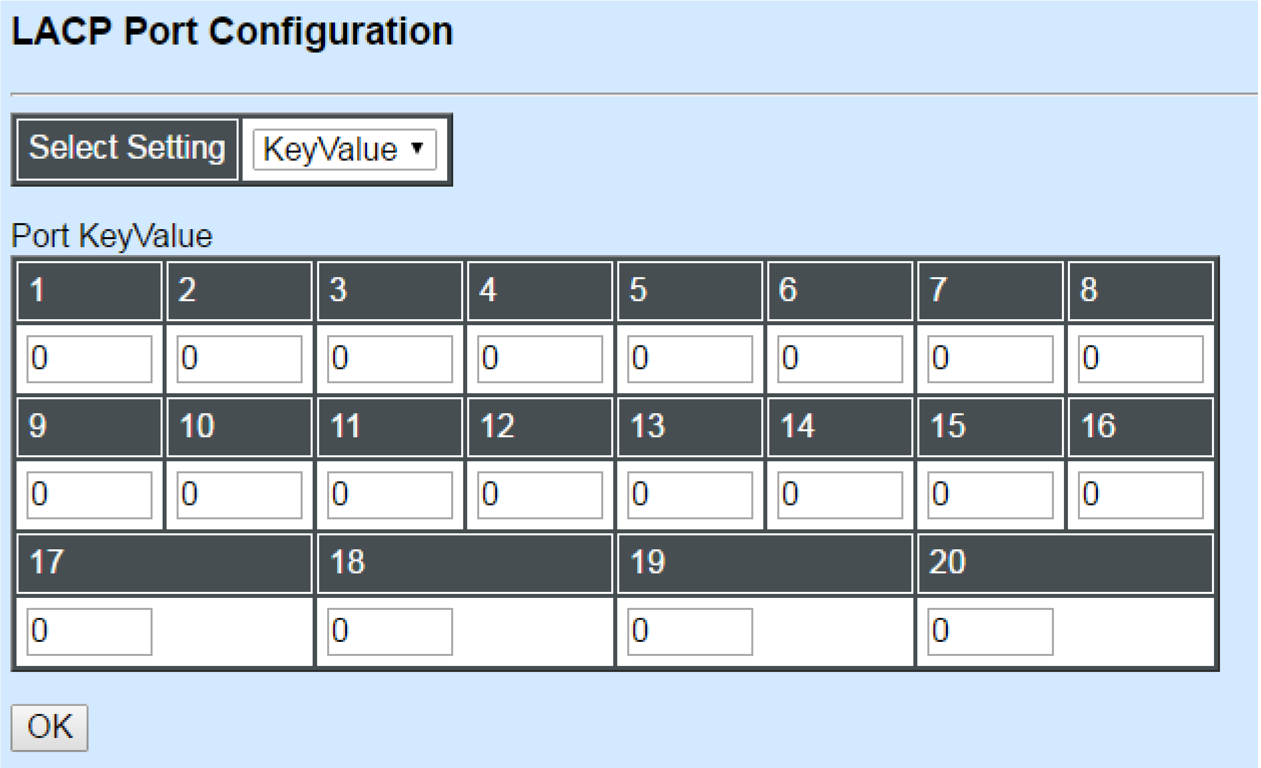
1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0
9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0

17	18	19	20
0	0	0	0

This allows LACP to be enabled (active or passive) or disabled on each port.

Configure Key Value:

Select “Key Value” from the pull-down menu of Select Setting.



LACP Port Configuration

Select Setting: KeyValue

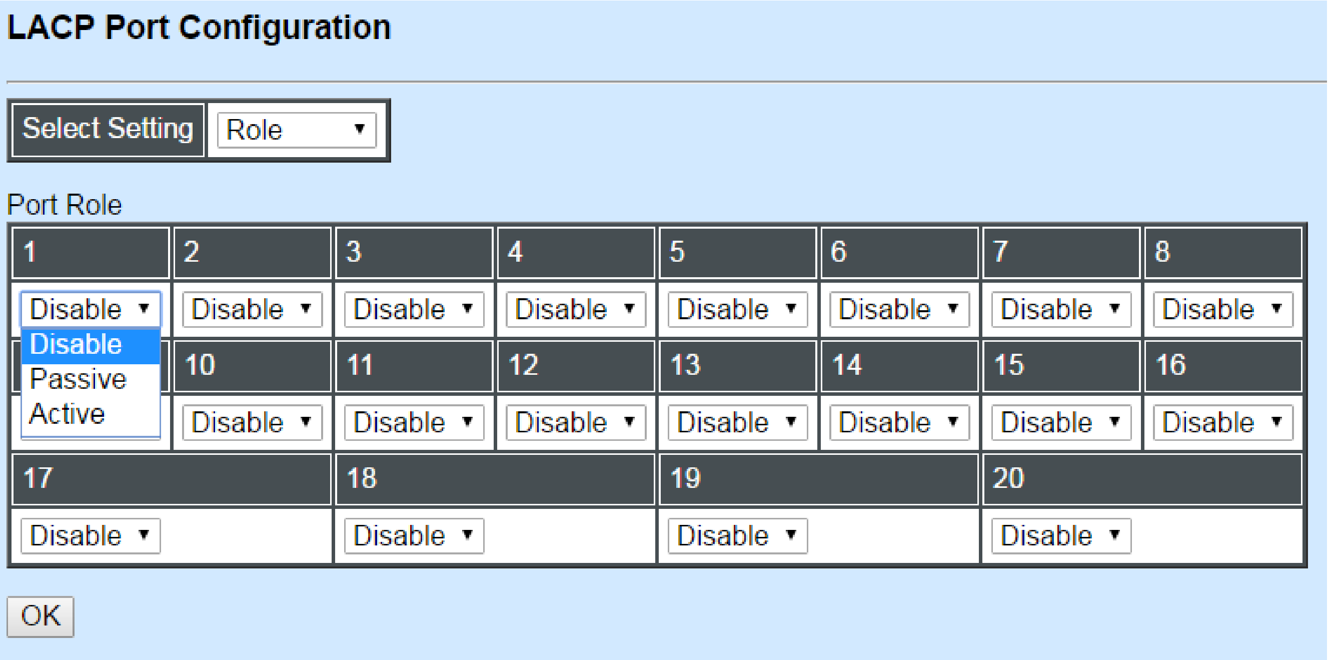
Port KeyValue

1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0
9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0
17		18		19		20	
0		0		0		0	

Ports in an aggregated link group must have the same LACP port Key. In order to allow a port to join an aggregated group, the port Key must be set to the same value. The range of key value is between 0 and 255. When key value is set to 0, the port Key is automatically set by the Managed Switch.

Configure Port Role:

Select “Role” from the pull-down menu of Select Setting.



LACP Port Configuration

Select Setting: Role ▼

Port Role

1	2	3	4	5	6	7	8
Disable ▼	Disable ▼	Disable ▼	Disable ▼	Disable ▼	Disable ▼	Disable ▼	Disable ▼
	10	11	12	13	14	15	16
	Disable ▼	Disable ▼	Disable ▼	Disable ▼	Disable ▼	Disable ▼	Disable ▼
17		18		19		20	
Disable ▼		Disable ▼		Disable ▼		Disable ▼	

“Disable” Port Role: Disable LACP on specified port(s)

“Active” Port Role: Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so that the group may be changed dynamically as required. In order to utilize the ability to change an aggregated port group, that is, to add or remove ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.

“Passive” Port Role: LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have “active” LACP ports.

7.4.4 Rapid Spanning Tree

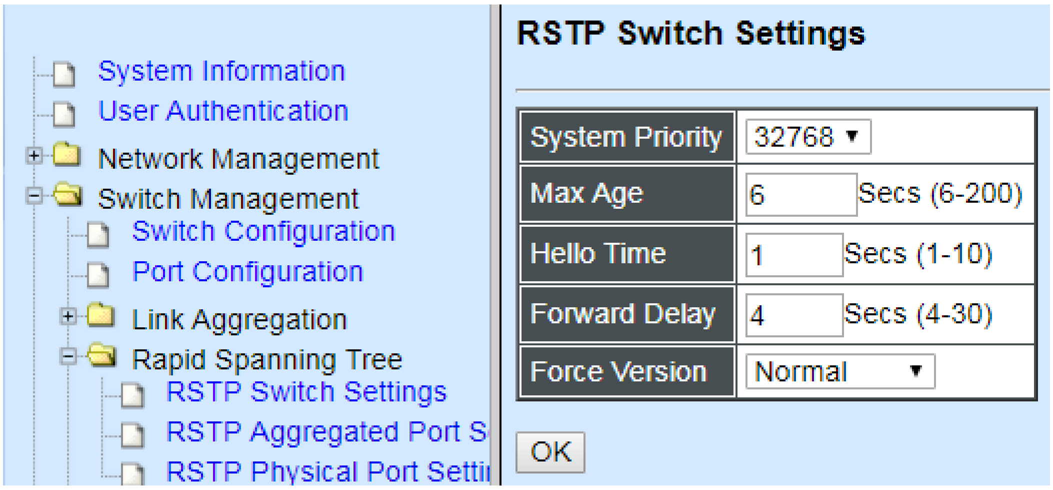
The Spanning Tree Protocol (STP), defined in the IEEE Standard 802.1D, creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches) and disables the links which are not part of that tree, leaving a single active path between any two network nodes.

Multiple active paths between network nodes cause a bridge loop. Bridge loops create several problems. First, the MAC address table used by the switch or bridge can fail, since the same MAC addresses (and hence the same network hosts) are seen on multiple ports. Second, a broadcast storm occurs. This is caused by broadcast packets being forwarded in an endless loop between switches. A broadcast storm can consume all available CPU resources and bandwidth.

Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manually enabling/disabling these backup links.

To provide faster spanning tree convergence after a topology change, an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP), introduced by IEEE with document 802.1w. RSTP, is a refinement of STP; therefore, it shares most of its basic operation characteristics. This essentially creates a cascading effect away from the root bridge where each designated bridge proposes to its neighbors to determine if it can make a rapid transition. This is one of the major elements which allows RSTP to achieve faster convergence times than STP.

Click the folder **Rapid Spanning Tree** from the **Switch Management** menu and then three options within this folder will be displayed as follows.



RSTP Switch Settings

System Priority	32768 ▼
Max Age	6 Secs (6-200)
Hello Time	1 Secs (1-10)
Forward Delay	4 Secs (4-30)
Force Version	Normal ▼

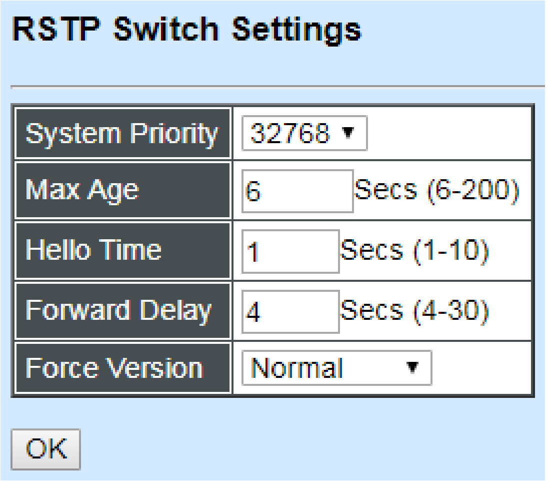
1. **RSTP Switch Settings:** Set up system priority, max Age, hello time, etc.

2. **RSTP Aggregated Port Settings:** Set up aggregation, path cost, priority, edge, etc.

3. **RSTP Physical Port Settings:** Set up physical, ability and edge status of port.

7.4.4.1 RSTP Switch Settings

Click the option **RSTP Switch Settings** from the **Rapid Spanning Tree** menu and then the following screen page appears.



RSTP Switch Settings

System Priority	32768 ▼
Max Age	6 Secs (6-200)
Hello Time	1 Secs (1-10)
Forward Delay	4 Secs (4-30)
Force Version	Normal ▼

System Priority: Each interface is associated with a port (number) in the STP code. And, each switch has a relative priority and cost that is used to decide what the shortest path is to forward a packet. The lowest cost path is always used unless the other path is down. If you have multiple bridges and interfaces then you may need to adjust the priority to achieve optimized performance.

The Managed Switch with the lowest priority will be selected as the root bridge. The root bridge is the “central” bridge in the spanning tree.

Max Age: If another switch in the spanning tree does not send out a hello packet for a long period of time, it is assumed to be disconnected. This timeout is set to 20 seconds.

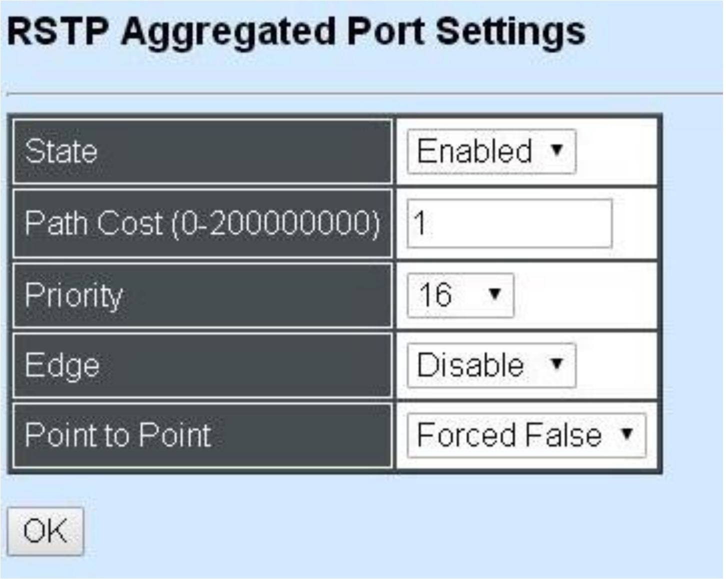
Hello Time: Periodically, a hello packet is sent out by the Root Bridge and the Designated Bridges that are used to communicate information about the topology throughout the entire Bridged Local Area Network.

Forward Delay: It is the time spent in each Listening and Learning state before the Forwarding state is entered. This delay occurs when a new bridge comes onto a busy network.

Force Version: Set and show the RSTP protocol to be used. Normal - use RSTP, Compatible - compatible with STP.

7.4.4.2 RSTP Aggregated Port Settings

Click the option **RSTP Aggregated Port Settings** from the **Rapid Spanning Tree** menu and then the following screen page appears.



RSTP Aggregated Port Settings

State	Enabled ▾
Path Cost (0-200000000)	1
Priority	16 ▾
Edge	Disable ▾
Point to Point	Forced False ▾

State: Enable or disable configured trunking groups in RSTP mode.

Path Cost: This parameter is used by the RSTP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. 0 means auto-generated path cost.

Priority: Choose a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.

Edge: If you know a port is directly connected to an end device (that doesn't support RSTP) then set it as an edge port to ensure maximum performance. This will tell the switch to immediately start forwarding traffic on the port and not bother trying to establish a RSTP connection. Otherwise, turn it off.

Point to Point:

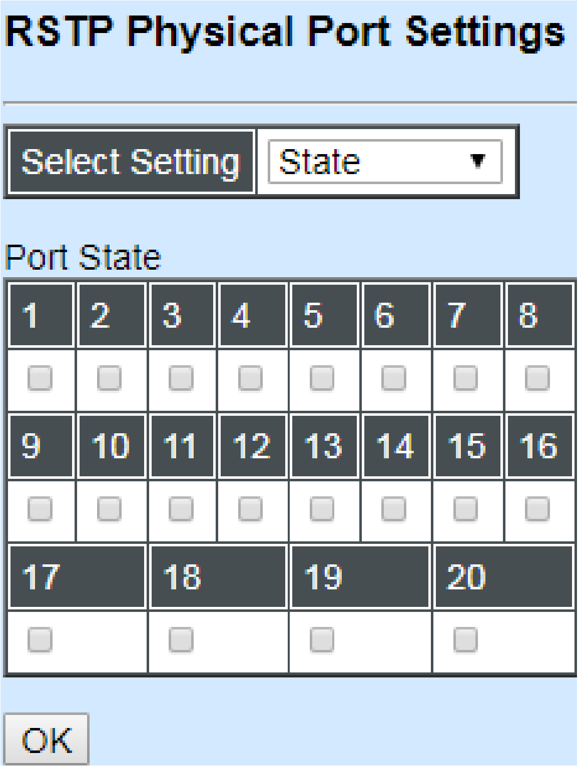
> **Forced True:** indicates a point-to-point (P2P) shared link.P2P ports are similar to edge ports; however, they are restricted in that a P2P port must operate in full duplex. Similar to edge ports, P2P ports transit to a forwarding state rapidly thus benefiting from RSTP.
>
> **Forced False:** the port cannot have P2P status.
>
> **Auto:** allows the port to have P2P status whenever possible and operates as if the P2P status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the P2P status changes to operate as if the P2P value were false. The default setting for this parameter is true.

7.4.4.3 RSTP Physical Port Settings

Click the option **RSTP Physical Port Settings** from the **Rapid Spanning Tree** menu and then the following screen page appears.

Configure Port State:

Select “State” from the pull-down menu of Select Setting.



RSTP Physical Port Settings

Select Setting	State ▼

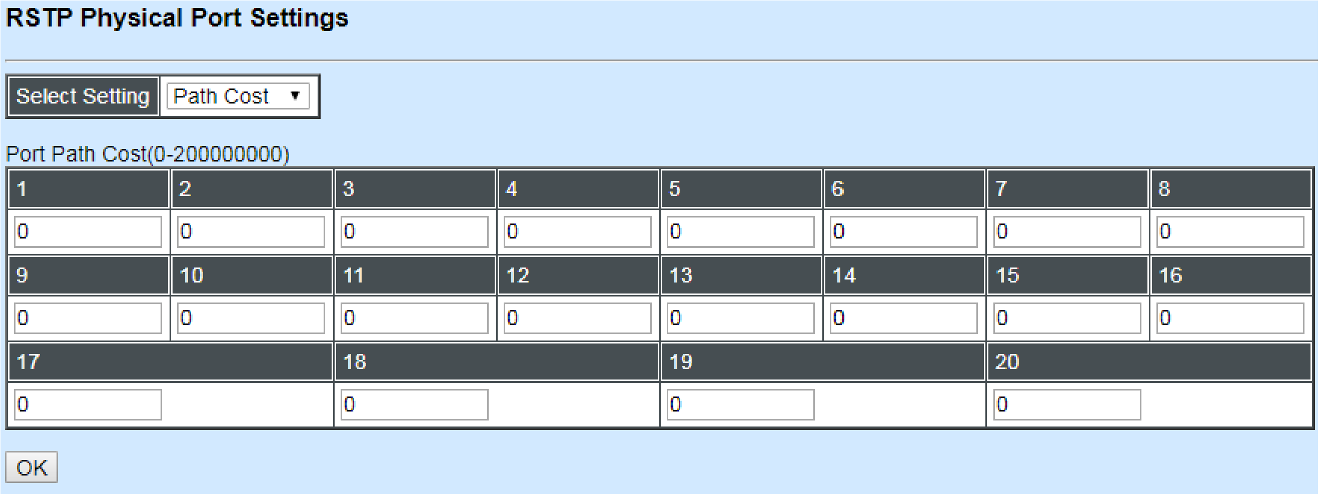
Port State

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☐	☐	☐	☐
9	10	11	12	13	14	15	16
☐	☐	☐	☐	☐	☐	☐	☐
17		18		19		20	
☐		☐		☐		☐	

This allows ports to be enabled or disabled. When it is On, RSTP is enabled.

Configure Port Path Cost:

Select “Path Cost” from the pull-down menu of Select Setting.



RSTP Physical Port Settings

Select Setting	Path Cost ▼

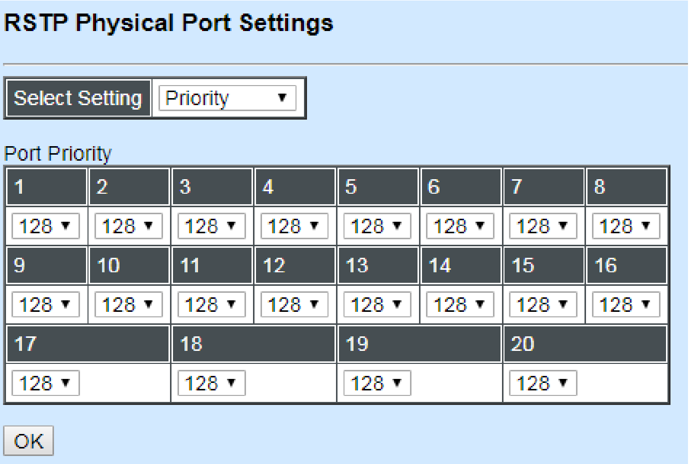
Port Path Cost(0-200000000)

1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0
9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0
17		18		19		20	
0		0		0		0	

This sets up each port's path cost. The default value is "0".

Configure Port Priority:

Select "Priority" from the pull-down menu of Select Setting.



RSTP Physical Port Settings

Select Setting: Priority ▾

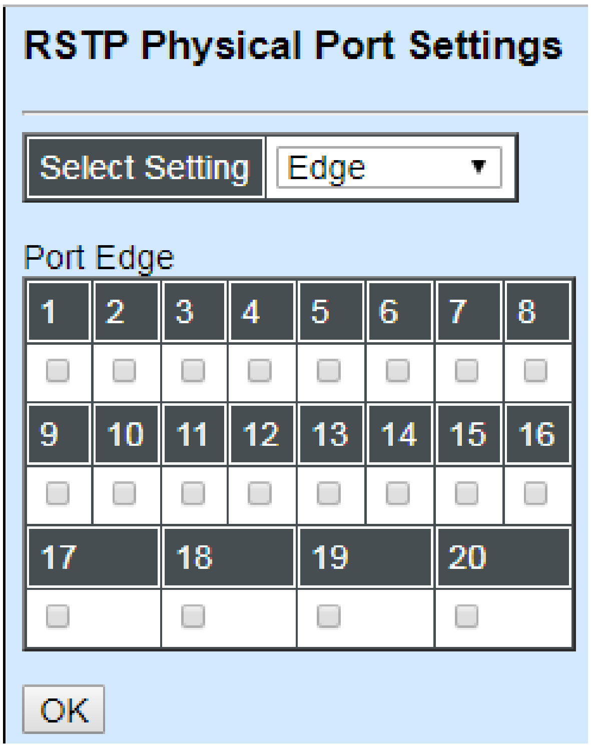
Port Priority

1	2	3	4	5	6	7	8
128 ▾	128 ▾	128 ▾	128 ▾	128 ▾	128 ▾	128 ▾	128 ▾
9	10	11	12	13	14	15	16
128 ▾	128 ▾	128 ▾	128 ▾	128 ▾	128 ▾	128 ▾	128 ▾
17		18		19		20	
128 ▾		128 ▾		128 ▾		128 ▾	

You can choose Port Priority value between 0 and 240. The default value is "128".

Configure Port Edge:

Select "Edge" from the pull-down menu of Select Setting.



RSTP Physical Port Settings

Select Setting: Edge ▾

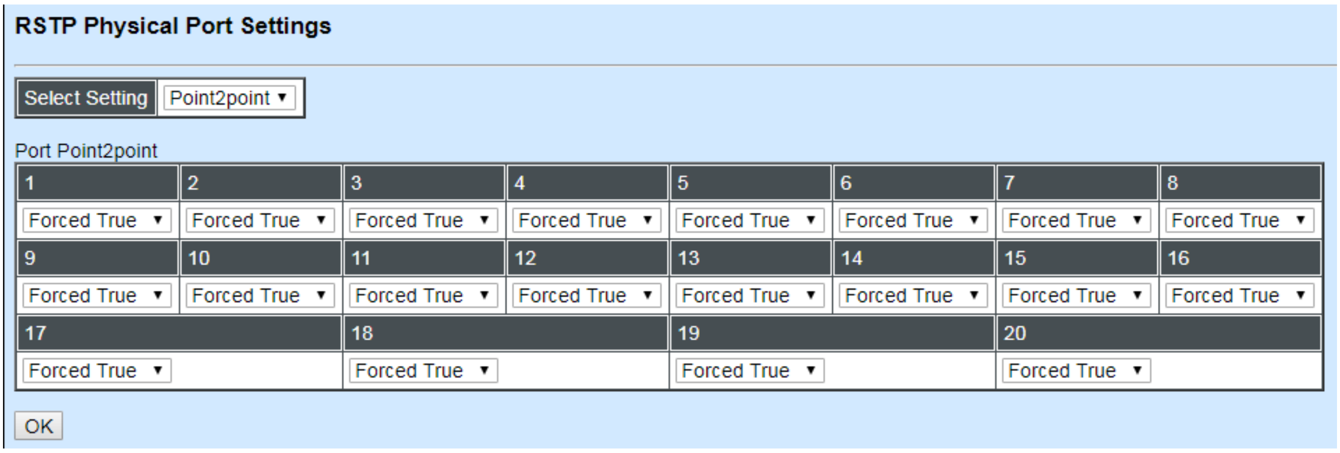
Port Edge

1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□
9	10	11	12	13	14	15	16
□	□	□	□	□	□	□	□
17		18		19		20	
□		□		□		□	

Set the port to "enabled" or "disabled". When it is On, Port Edge is enabled.

Configure Port Point2point:

Select “Point2point” from the pull-down menu of Select Setting.



RSTP Physical Port Settings

Select Setting: Point2point ▾

Port Point2point

1	2	3	4	5	6	7	8
Forced True ▾	Forced True ▾	Forced True ▾	Forced True ▾	Forced True ▾	Forced True ▾	Forced True ▾	Forced True ▾
9	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Forced True ▾	Forced True ▾	Forced True ▾	Forced True ▾	Forced True ▾	Forced True ▾	Forced True ▾	Forced True ▾
17		**18**		**19**		**20**	
Forced True ▾		Forced True ▾		Forced True ▾		Forced True ▾	

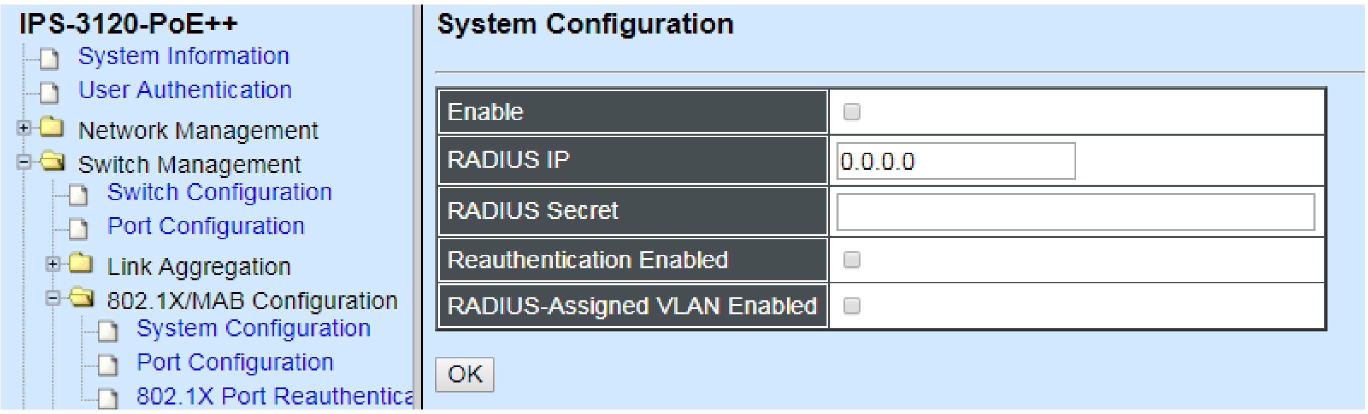
Set up the Point to Point setting. The default setting is “Forced True”.

7.4.5 802.1X/MAB Configuration

The IEEE 802.1X standard provides a port-based network access control and authentication protocol that prevents unauthorized devices from connecting to a LAN through accessible switch ports. Before services are made available to clients connecting to a VLAN, clients that are 802.1X-complaint should successfully authenticate with the authentication server.

Initially, ports are in the authorized state which means that ingress and egress traffic are not allowed to pass through except 802.1X protocol traffic. When the authentication is successful with the authentication server, traffic from clients can flow normally through a port. If authentication fails, ports remain in unauthorized state but retries can be made until access is granted.

Click the folder **802.1X/MAB Configuration** from the **Switch Management** menu and then three options will be displayed as follows.



System Configuration

Enable	□
RADIUS IP	0.0.0.0
RADIUS Secret	
Reauthentication Enabled	□
RADIUS-Assigned VLAN Enabled	□

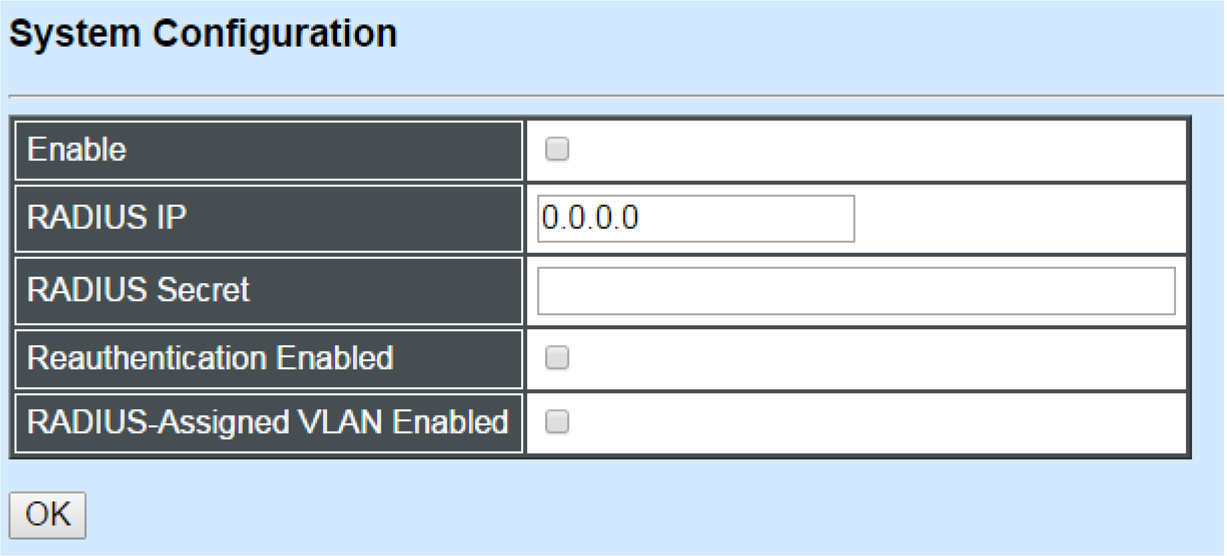
1. **System Configuration:** Set up 802.1X RADIUS IP, RADIUS Secret, Reauthentication, Timeout.

2. **Port Configuration:** Set up aggregation, Path Cost, Priority, Edge, etc.

3. **802.1X Port Reauthenticate:** Set up Physical, ability and edge status of port.

7.4.5.1 System Configuration

Click the option **System Configuration** from the **802.1X/MAB Configuration** folder and then the following screen page appears.



System Configuration

Enable	□
RADIUS IP	0.0.0.0
RADIUS Secret	
Reauthentication Enabled	□
RADIUS-Assigned VLAN Enabled	□

Enable: Enable or disable 802.1X on the Managed Switch. When enabled, the Managed Switch acts as a proxy between the 802.1X-enabled client and the authentication server. In other words, the Managed Switch requests identifying information from the client, verifies that information with the authentication server, and relays the response to the client.

RADIUS IP: Specify RADIUS Authentication server address.

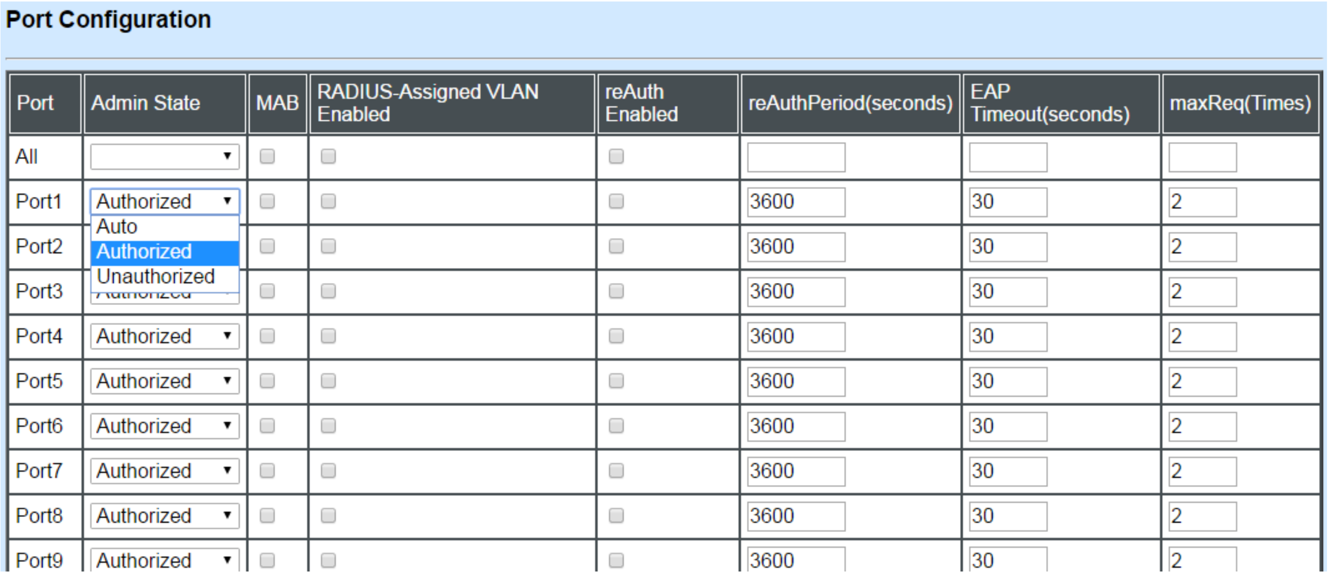
RADIUS Secret: The identification number assigned to each RADIUS authentication server with which the client shares a secret.

Reauthentication Enabled: Globally enable or disable periodic Reauthentication.

RADIUS-Assigned VLAN: Globally enable to allow the Radius server to use the following tunnel attributes for port’s VLAN assignment after successful authentication: Tunnel-Type=VLAN(13), Tunnel-Medium-Type=802, Tunnel-Private-Group-ID=VLANID.

7.4.5.2 Port Configuration

Click the option **Port Configuration** from the **802.1X/MAB Configuration** menu and then the following screen page appears.



Port Configuration

Port	Admin State	MAB	RADIUS-Assigned VLAN Enabled	reAuth Enabled	reAuthPeriod(seconds)	EAP Timeout(seconds)	maxReq(Times)
All	▾	☐	☐	☐			
Port1	Authorized ▾ Auto Authorized Unauthorized	☐	☐	☐	3600	30	2
Port2		☐	☐	☐	3600	30	2
Port3	Authorized	☐	☐	☐	3600	30	2
Port4	Authorized ▾	☐	☐	☐	3600	30	2
Port5	Authorized ▾	☐	☐	☐	3600	30	2
Port6	Authorized ▾	☐	☐	☐	3600	30	2
Port7	Authorized ▾	☐	☐	☐	3600	30	2
Port8	Authorized ▾	☐	☐	☐	3600	30	2
Port9	Authorized ▾	☐	☐	☐	3600	30	2

Admin State: Three states available as below.

Authorized: This forces the Managed Switch to grant access to all clients, either 802.1X-aware or 802.1x-unaware. No authentication exchange is required. By default, all ports are set to “Authorized”.

Unauthorized: This forces the Managed Switch to deny access to all clients, either 802.1X-aware or 802.1X-unaware.

Auto: This requires 802.1X-aware clients to be authorized by the authentication server. Accesses from clients that are not 802.1X-aware will be denied.

MAB: MAC-Authentication Bypass (MAB) is commonly used for devices, such as VoIP phones and Ethernet printers, that do not support the 802.1x protocol. This method allows such devices to be authenticated using the same database infrastructure as that used in 802.1x.

1. The device connects to a switch port.

2. The switch learns the device MAC address upon receiving the first frame from the device (the device usually sends out a DHCP request message when first connected).

3. The switch sends an EAP Request message to the device, attempting to start 802.1X authentication.

4. The switch times out while waiting for the EAP reply, because the device does not support 802.1x.

5. The switch sends an authentication message to the authentication server, using the device MAC address as the username and password.

6. The switch authenticates or rejects the device according to the reply from the authentication server.

RADIUS-Assigned VLAN: Enable to allow the Radius server to use the following tunnel attributes for port's VLAN assignment after successful authentication: Tunnel-Type=VLAN(13), Tunnel-Medium-Type=802, Tunnel-Private-Group-ID=VLANID.

Reauthentication Enabled: Enable or disable periodic Reauthentication.

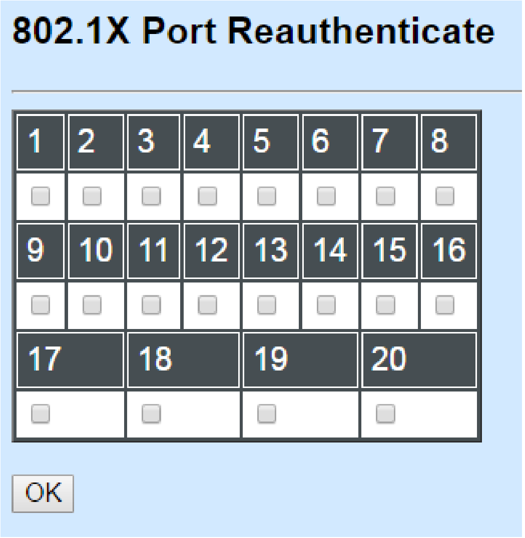
reAuth Period: Specify a period of authentication time in second that a client authenticates with the authentication server.

EAP Timeout: Specify the time value in second that the Managed Switch will wait for a response from the authentication server to an authentication request.

MaxReq(Times): Specify the maximum times the request should be sent. The connected client will be authenticated using MAB if the switch has tried the specified times and receive no EAP reply from the device.

7.4.5.3 802.1X Port Reauthenticate

Click the option **802.1X Port Reauthenticate** from the **802.1X/MAB Configuration** menu and then the following screen page appears.



802.1X Port Reauthenticate

1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□
9	10	11	12	13	14	15	16
□	□	□	□	□	□	□	□
17		18		19		20	
□		□		□		□	

This allows users to enable or disable port Reauthenticate. When enabled, the authentication message will be sent immediately after you click the **"OK"** button.

7.4.6 VLAN Configuration

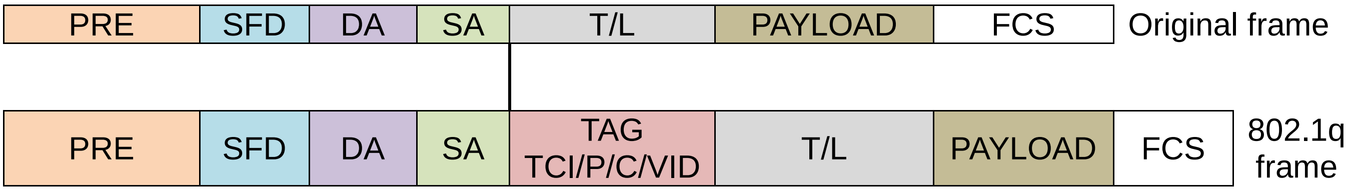
A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the Switch on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. A station can be 'moved' to another VLAN and thus communicates with its members and shares its resources, simply by changing the port settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

The Managed Industrial PoE Switch supports two types of VLAN: **Port Based VLAN** and **IEEE 802.1q Tag VLAN.**

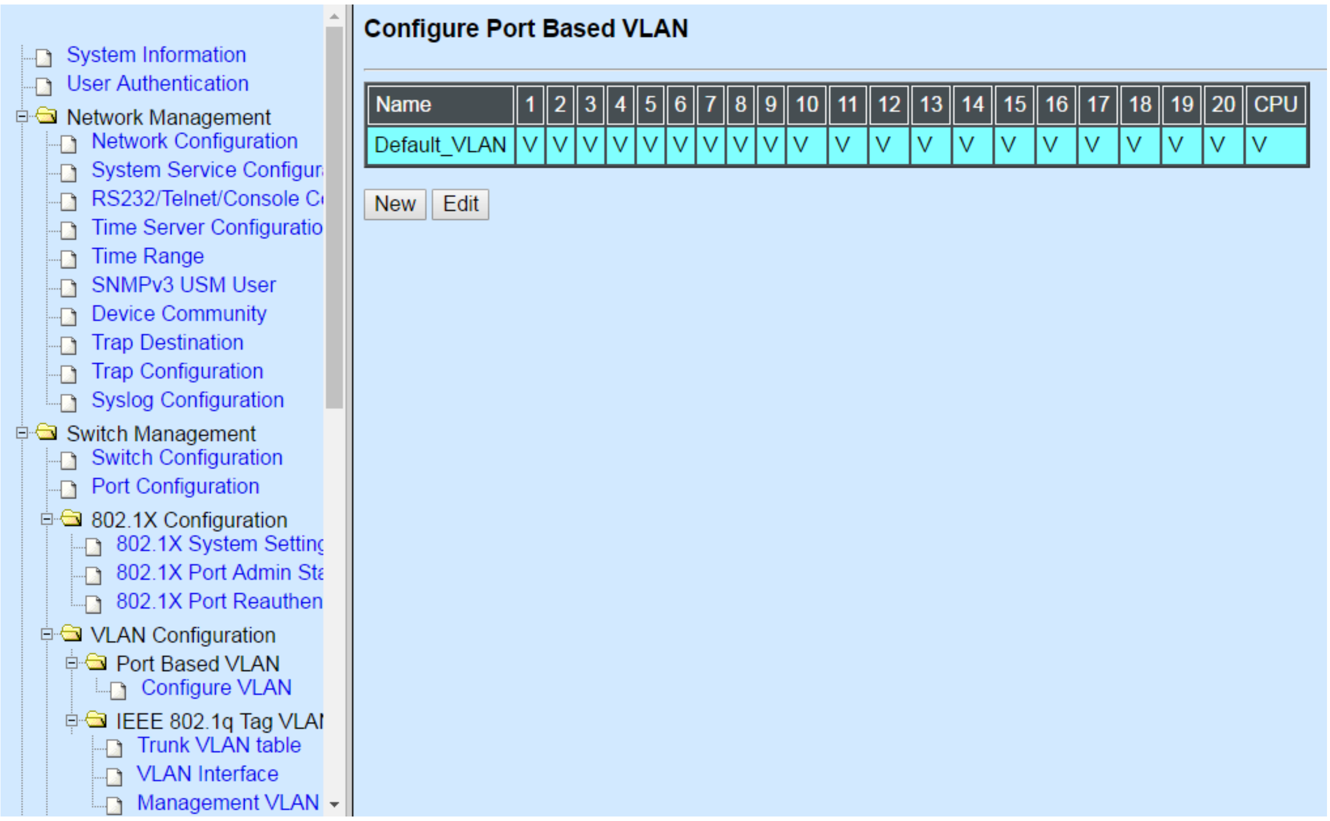
IEEE 802.1Q VLAN Concepts

Introduction of 802.1Q frame format:



PRE Preamble	62 bits	Used to synchronize traffic
SFD Start Frame Delimiter	2 bits	Marks the beginning of the header
DA Destination Address	6 bytes	The MAC address of the destination
SA Source Address	6 bytes	The MAC address of the source
TCI Tag Control Info	2 bytes	Set to 0x8100 for 802.1p and Q tags
P Priority	3 bits	Indicates 802.1p priority level 0-7
C Canonical Indicator	1 bit	Indicates if the MAC addresses are in the canonical format – Ethernet is set to "0".
VID VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload	< or = 1500 bytes	User data
FCS Frame Check Sequence	4 bytes	Cyclical Redundancy Check

Click the folder **VLAN Configuration** from the **Switch Management** menu and then the following screen page appears.



Configure Port Based VLAN

Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	CPU
Default_VLAN	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V

Port Based VLAN: Configure Port-Based VLAN settings.

IEEE 802.1Q Tag VLAN: Configure IEEE 802.1Q Tag VLAN settings.

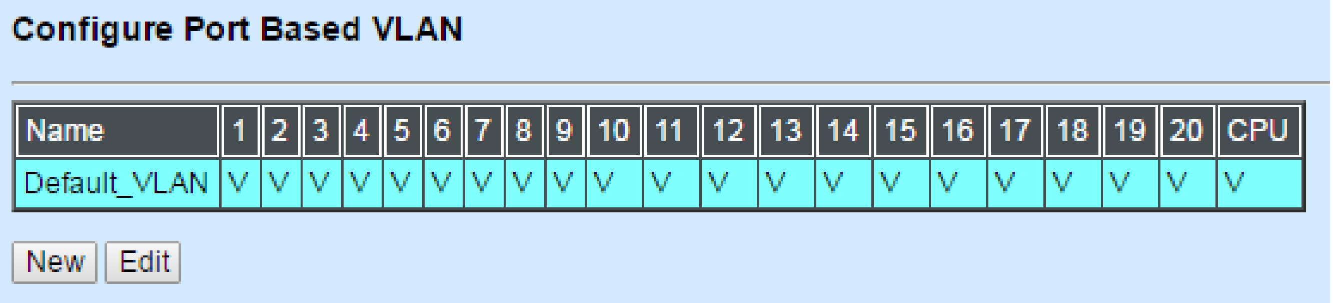
7.4.6.1 Port Based VLAN

Port-Based VLAN can effectively divide one network into multiple logical networks. Broadcast, multicast and unknown packets will be limited within the VLAN. Port-Based VLAN is uncomplicated and fairly rigid in implementation, and useful for network administrators who want to quickly and easily set up VLAN so as to isolate the effect of broadcast packets on their network.

Since source MAC addresses and VID of the packets are listed in the MAC address table (except broadcast/multicast packets), the traffic between two ports in the same VLAN will be two-way without restrictions.

7.4.6.1.1 Configure Port Based VLAN

Click the option **Configure VLAN** from the **Port Based VLAN** folder, and then the following screen page appears.



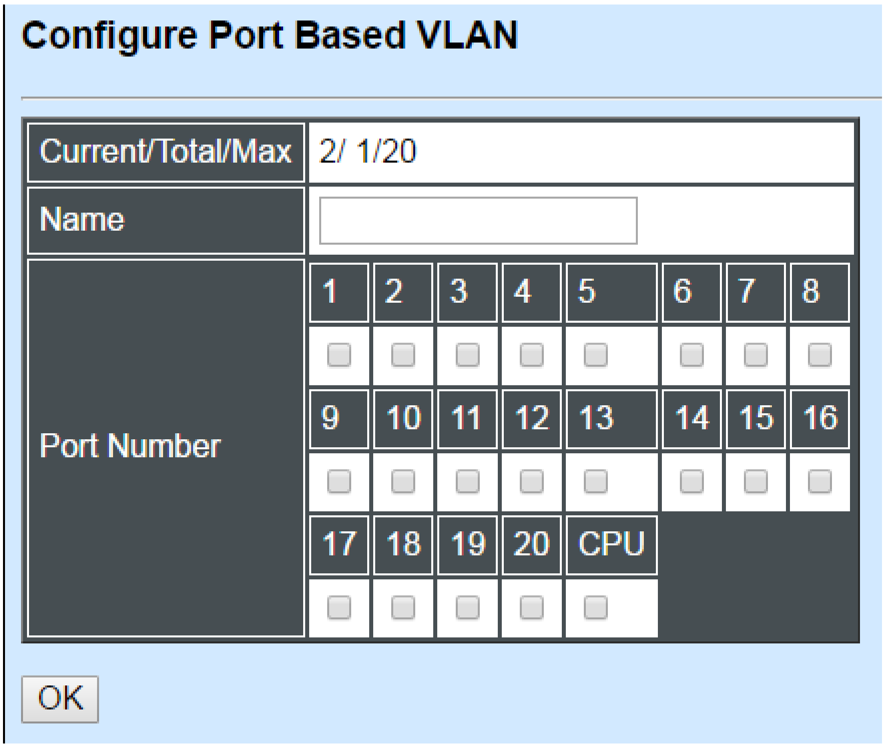
Configure Port Based VLAN

Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	CPU
Default_VLAN	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V

Click **New** to add a new VLAN group and then the following screen page appears.

Use **Edit** to view and edit the current VLAN setting.

Click **Delete** to remove a VLAN group.



Configure Port Based VLAN

Current/Total/Max	2/ 1/20
Name	

Port Number

1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□
9	10	11	12	13	14	15	16
□	□	□	□	□	□	□	□
17	18	19	20	CPU			
□	□	□	□	□			

Current/Total/Max: View-only field.

Current: It shows the number of currently configured VLAN.

Total: It shows the total number of the VLANs.

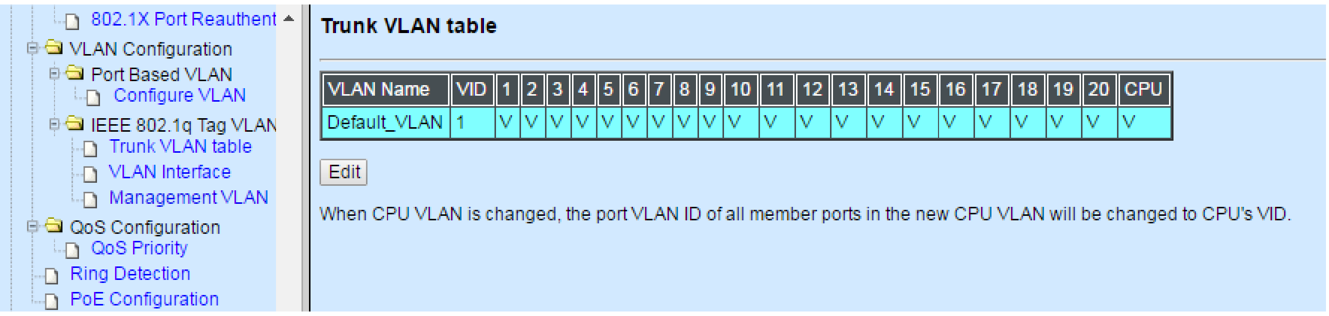
Max: It shows the maximum number available for configuration. The maximum is 10.

Name: Specify a VLAN group name, up to 15 alphanumeric characters.

Check the port number as a VLAN member and click **"OK"**

7.4.6.2 IEEE 802.1q Tag VLAN

Click the folder **IEEE 802.1Q Tag VLAN** from the **VLAN Configuration** menu and then the following screen page appears.



Trunk VLAN table

VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	CPU
Default_VLAN	1	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V

When CPU VLAN is changed, the port VLAN ID of all member ports in the new CPU VLAN will be changed to CPU's VID.

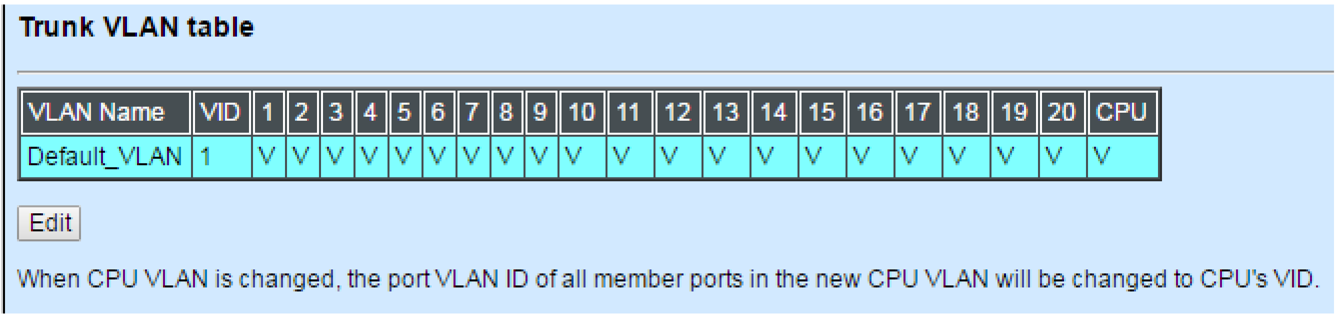
Trunk VLAN table: Edit or apply 802.1Q Tag VLAN settings.

VLAN Interface: Globally set up switch VLAN mode and per port VLAN mode.

Management VLAN: Set up management VLAN and management port(s).

7.4.6.2.1 Trunk VLAN Table

Click the option **Trunk VLAN Table** from the **IEEE 802.1q Tag VLAN** menu and then the following screen page appears.

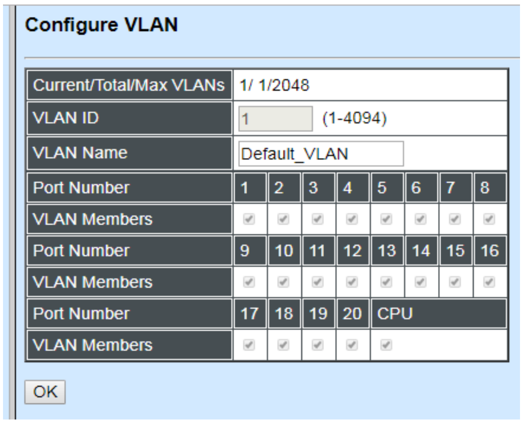


Trunk VLAN table

VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	CPU
Default_VLAN	1	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V

When CPU VLAN is changed, the port VLAN ID of all member ports in the new CPU VLAN will be changed to CPU's VID.

Click **Edit** to view and edit current IEEE 802.1Q Tag VLAN setting, and then the following screen page appears.



Configure VLAN

Current/Total/Max VLANs	1/ 1/2048							
VLAN ID	1 (1-4094)							
VLAN Name	Default_VLAN							
Port Number	1	2	3	4	5	6	7	8
VLAN Members	☑	☑	☑	☑	☑	☑	☑	☑
Port Number	9	10	11	12	13	14	15	16
VLAN Members	☑	☑	☑	☑	☑	☑	☑	☑
Port Number	17	18	19	20	CPU			
VLAN Members	☑	☑	☑	☑	☑			

Current/Total/Max VLANs: View-only field

Current: It shows the number of currently registered VLAN.

Total: It shows the total number of registered VLANs.

Max: It shows the maximum number of available VLANs which could be registered.

VLAN ID: Display the ID for the currently registered VLAN.

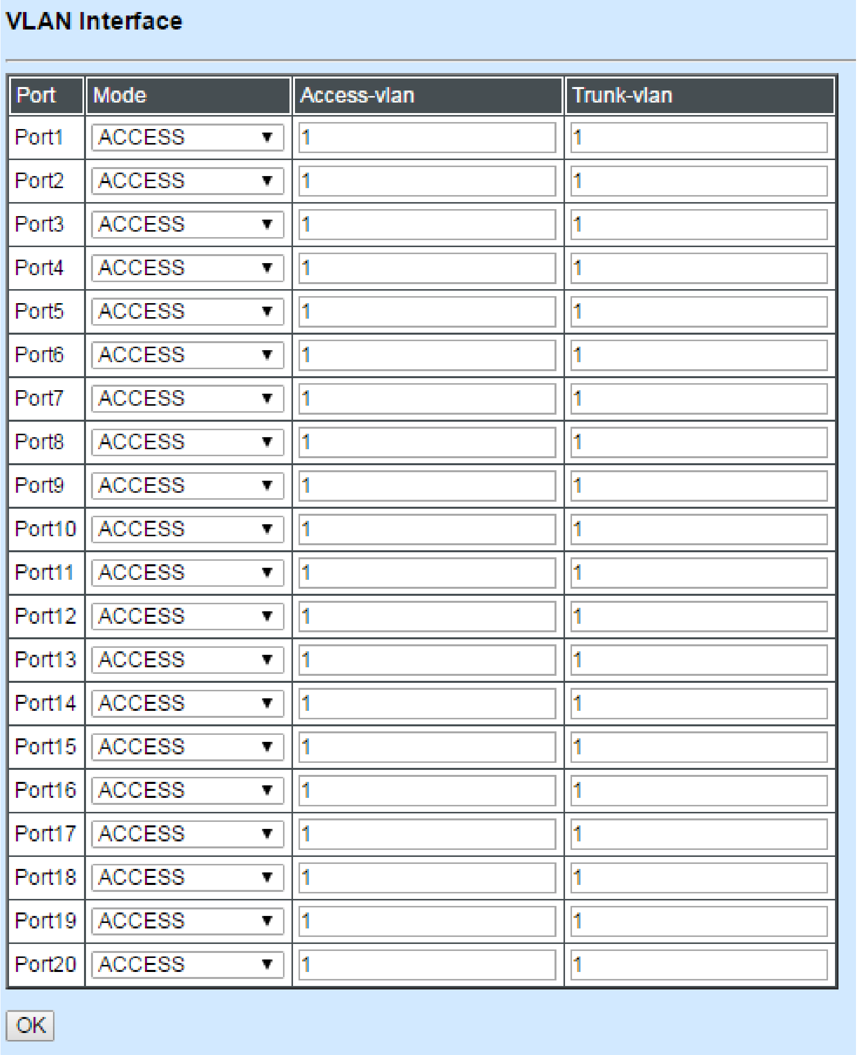
VLAN Name: Specify the name for the currently registered VLAN.

VLAN Member: Check the ports to be the members of the currently registered VLAN.

Click **OK** to make the current VLAN settings effective.

7.4.6.2.2 VLAN Interface

Click the option **VLAN Interface** from the **IEEE 802.1q Tag VLAN** menu and then the following screen page appears.



VLAN Interface

Port	Mode	Access-vlan	Trunk-vlan
Port1	ACCESS ▼	1	1
Port2	ACCESS ▼	1	1
Port3	ACCESS ▼	1	1
Port4	ACCESS ▼	1	1
Port5	ACCESS ▼	1	1
Port6	ACCESS ▼	1	1
Port7	ACCESS ▼	1	1
Port8	ACCESS ▼	1	1
Port9	ACCESS ▼	1	1
Port10	ACCESS ▼	1	1
Port11	ACCESS ▼	1	1
Port12	ACCESS ▼	1	1
Port13	ACCESS ▼	1	1
Port14	ACCESS ▼	1	1
Port15	ACCESS ▼	1	1
Port16	ACCESS ▼	1	1
Port17	ACCESS ▼	1	1
Port18	ACCESS ▼	1	1
Port19	ACCESS ▼	1	1
Port20	ACCESS ▼	1	1

802.1q Tag VLAN Mode: Two options are available: Port Based VLAN, IEEE 802.1q VLAN.

Mode: To specify the VLAN mode for each port, there are three options available: ACCESS, TRUNK, TRUNK-NATIVE.

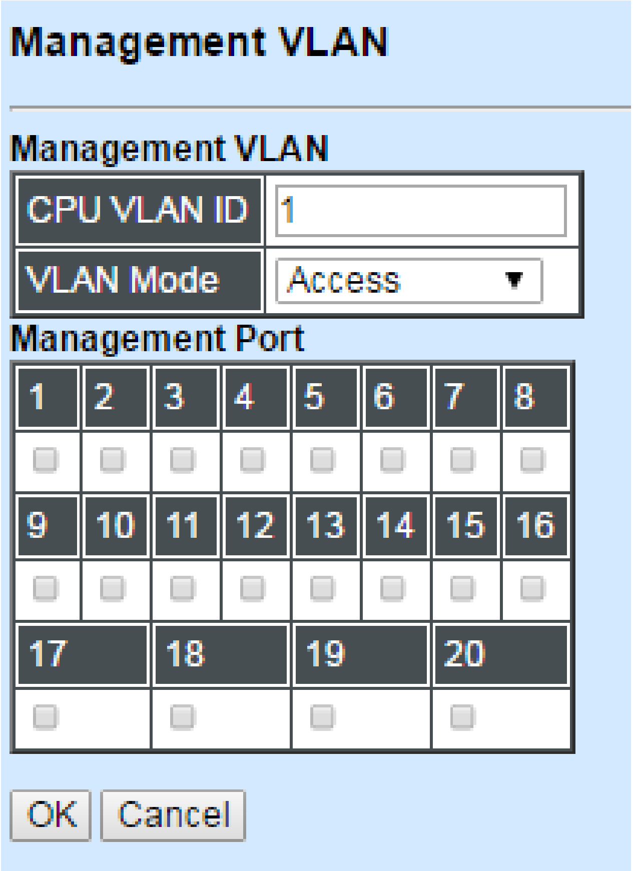
Access-VLAN: Specify the Access-VLAN ID (PVID) for each port. The default VLAN ID is “1”.

Trunk-VLAN: Specify the Trunk-VLAN ID (802.1q tag) for each port. Use “-” or “,” to assign multiple VIDs, for example, 1-4 and 1,2,3,4. The default VLAN ID is “1”.

Click the **“OK”** button to apply the settings.

7.4.6.2.3 Management VLAN

Click the option **Management VLAN** from the **IEEE 802.1q Tag VLAN** menu and then the following screen page appears.



Management VLAN

Management VLAN

CPU VLAN ID	1
VLAN Mode	Access ▼

Management Port

1	2	3	4	5	6	7	8
☐	☐	☐	☐	☐	☐	☐	☐
9	10	11	12	13	14	15	16
☐	☐	☐	☐	☐	☐	☐	☐
17	18	19	20				
☐	☐	☐	☐				

CPU VLAN ID: Specify the VID for CPU (management). The default VLAN ID is “1”.

VLAN Mode: Specify the VLAN mode for management VLAN. Three options are available: ACCESS, TRUNK, TRUNK-NATIVE.

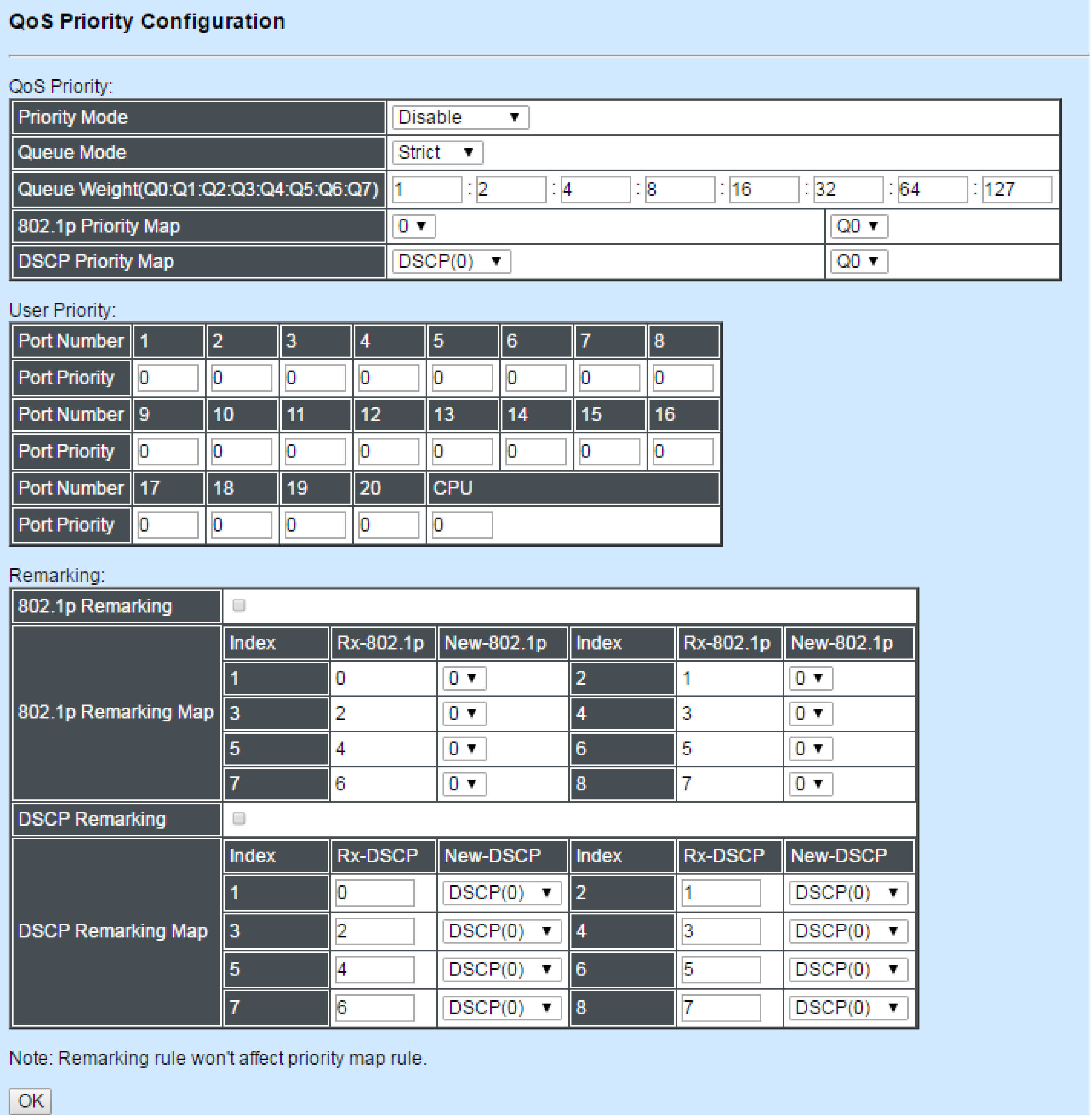
Management Port: Check the port(s) as the management port(s).

Click the **“OK”** button to apply the settings

7.4.7 QoS Configuration

Network traffic is always unpredictable and the only basic assurance that can be offered is the best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. It ensures that network traffic is prioritized according to specified criterion and receives preferential treatments.

QoS enables users to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic. Click the option **QoS Priority Configuration** from the **Switch Management** menu and then the following screen page appears.



QoS Priority Configuration

QoS Priority:

Priority Mode	Disable ▼	
Queue Mode	Strict ▼	
Queue Weight(Q0:Q1:Q2:Q3:Q4:Q5:Q6:Q7)	1 : 2 : 4 : 8 : 16 : 32 : 64 : 127	
802.1p Priority Map	0 ▼	Q0 ▼
DSCP Priority Map	DSCP(0) ▼	Q0 ▼

User Priority:

Port Number	1	2	3	4	5	6	7	8
Port Priority	0	0	0	0	0	0	0	0
Port Number	9	10	11	12	13	14	15	16
Port Priority	0	0	0	0	0	0	0	0
Port Number	17	18	19	20	CPU			
Port Priority	0	0	0	0	0			

Remarking:

802.1p Remarking	□					
802.1p Remarking Map	Index	Rx-802.1p	New-802.1p	Index	Rx-802.1p	New-802.1p
	1	0	0 ▼	2	1	0 ▼
	3	2	0 ▼	4	3	0 ▼
	5	4	0 ▼	6	5	0 ▼
	7	6	0 ▼	8	7	0 ▼
DSCP Remarking	□					
DSCP Remarking Map	Index	Rx-DSCP	New-DSCP	Index	Rx-DSCP	New-DSCP
	1	0	DSCP(0) ▼	2	1	DSCP(0) ▼
	3	2	DSCP(0) ▼	4	3	DSCP(0) ▼
	5	4	DSCP(0) ▼	6	5	DSCP(0) ▼
	7	6	DSCP(0) ▼	8	7	DSCP(0) ▼

Note: Remarking rule won't affect priority map rule.

QoS Priority

Priority Mode: Click the pull-down menu to select the QoS Priority Mode.

IEEE 802.1p: IEEE 802.1p mode utilizes p-bits in VLAN tag for different services.

DSCP: DSCP mode utilizes TOS field in IPv4 header for different services.

Disable: Disable QoS.

Queue Mode: Click the pull-down menu to select the Queue Mode.

Strict mode: This indicates that egress traffic is prioritized based on a queue value assigned to each port. For example, traffic assigned to queue 3 will be transmitted first when congestion happens. The traffic assigned to queue 2 will not be transmitted until queue 3's traffic is done transmitting, and so forth.

Weight mode: This mode enables users to assign different weights to 8 queues, which have fair opportunity of dispatching. Each queue has the specific amount of bandwidth according to its assigned weight.

Queue Weight (Q0:Q1:Q2:Q3:Q4:Q5:Q6:Q7): Specify the weight of eight queues.

802.1p Priority Map: Assign a tag priority to the specific queue.

DSCP Priority Map: Assign a DSCP priority to the specific queue. The DSCP priority includes DSCP (0) to DSCP (63), and the priority queue includes Q0 to Q7.

User Priority

Port Priority: Set up a priority to each port for ingress traffic with allowable value 0~7.

There are eight priority levels that you can choose to classify data packets. Choose one of the listed options from the pull-down menu for CoS (Class of Service) priority tag values. The default value is "0".

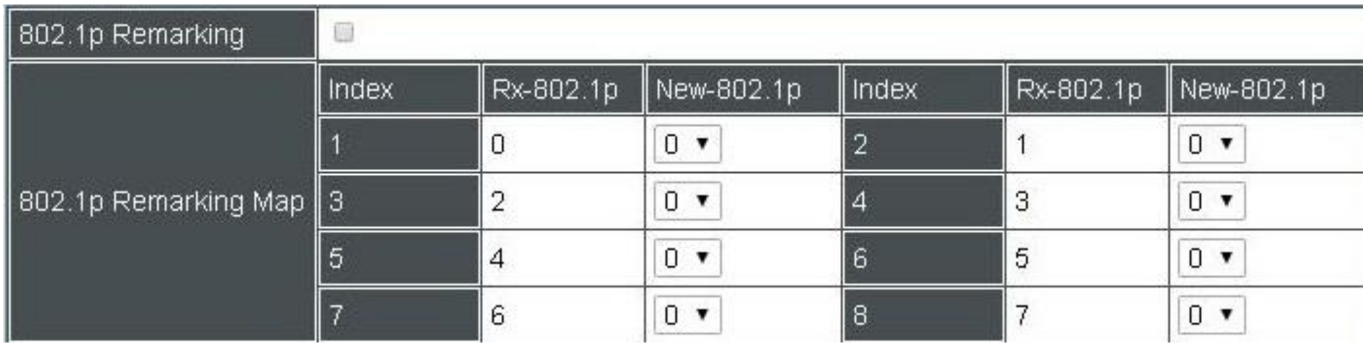
The default 802.1p settings are shown in the following table:

Priority Level	Low	Low	Low	Normal	Medium	Medium	High	High
802.1p Value	0	1	2	3	4	5	6	7

***Note:** 802.1p priority mode can only be applied under 802.1q VLAN mode.*

Configure 802.1p Remark:

Check **802.1p Remarking** to enable.

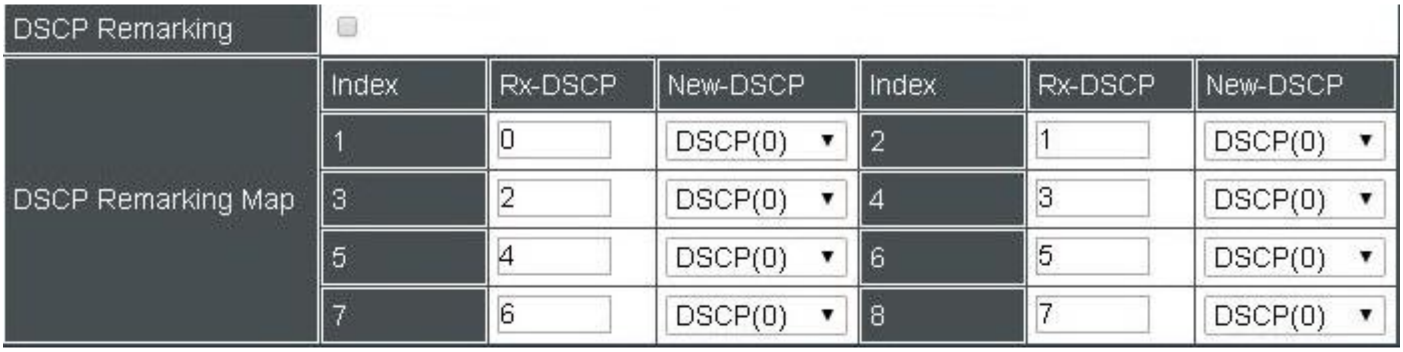


802.1p Remarking	□					
802.1p Remarking Map	Index	Rx-802.1p	New-802.1p	Index	Rx-802.1p	New-802.1p
	1	0	0 ▼	2	1	0 ▼
	3	2	0 ▼	4	3	0 ▼
	5	4	0 ▼	6	5	0 ▼
	7	6	0 ▼	8	7	0 ▼

This allows you to enable or disable 802.1p remarking for each port. The default setting is disabled.

Configure DSCP Remark:

Check **DSCP Remarking** to enable.



DSCP Remarking	□					
DSCP Remarking Map	Index	Rx-DSCP	New-DSCP	Index	Rx-DSCP	New-DSCP
	1	0	DSCP(0) ▼	2	1	DSCP(0) ▼
	3	2	DSCP(0) ▼	4	3	DSCP(0) ▼
	5	4	DSCP(0) ▼	6	5	DSCP(0) ▼
	7	6	DSCP(0) ▼	8	7	DSCP(0) ▼

This allows you to enable or disable DSCP remarking for each port. The default setting is disabled.

7.4.8 IGMP/MLD Snooping

The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It can be used more efficiently when supporting activities, such as online streaming video and gaming.

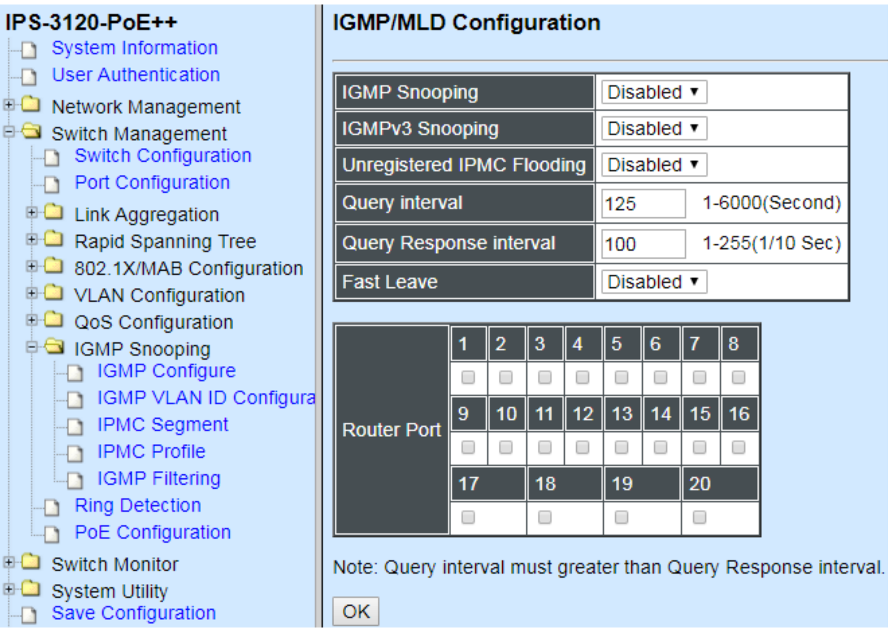
IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers by processing the layer 3 packets that IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch, it analyses all the IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch receives an IGMP report for a given multicast group from a host, the switch adds the host's port number to the multicast list for that group. When the switch hears an IGMP Leave, it removes the host's port from the table entry.

IGMP snooping can reduce multicast traffic from streaming and make other bandwidth intensive IP applications run more effectively. A switch using IGMP snooping will only forward multicast traffic to the hosts in that traffic. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also decreases the workload at the end hosts since their network cards (or operating system) will not receive and filter all the multicast traffic generated in the network.

Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4.

Select the folder **IGMP/MLD Snooping** from the **Switch Management** menu and then the following screen page appears.



IGMP/MLD Configuration

IGMP Snooping	Disabled ▾
IGMPv3 Snooping	Disabled ▾
Unregistered IPMC Flooding	Disabled ▾
Query interval	125 1-6000(Second)
Query Response interval	100 1-255(1/10 Sec)
Fast Leave	Disabled ▾

Router Port	1	2	3	4	5	6	7	8
	☐	☐	☐	☐	☐	☐	☐	☐
	9	10	11	12	13	14	15	16
	☐	☐	☐	☐	☐	☐	☐	☐
	17	18	19	20				
	☐	☐	☐	☐				

Note: Query interval must greater than Query Response interval.

1. **IGMP/MLD Configure:** To enable or disable IGMP, Unregistered IPMC Flooding and set up router ports.

2. **IGMP/MLD VLAN ID Configuration:** To set up the ability of IGMP snooping and querying with VLAN.

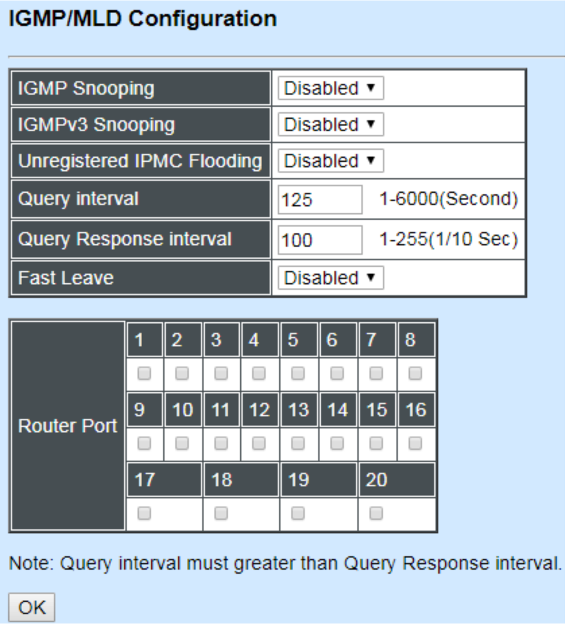
3. **IPMC Segment:** To create, edit or delete IPMC segment.

4. **IPMC Profile:** To create, edit or delete IPMC profile.

5. **IGMP Filtering:** To enable or disable IGMP filter and configure each port’s IGMP filter.

7.4.8.1 IGMP/MLD Configure

Select the option **IGMP/MLD Configure** from the **IGMP/MLD Snooping** menu and then the following screen page appears.



IGMP/MLD Configuration

IGMP Snooping	Disabled ▾	
IGMPv3 Snooping	Disabled ▾	
Unregistered IPMC Flooding	Disabled ▾	
Query interval	125	1-6000(Second)
Query Response interval	100	1-255(1/10 Sec)
Fast Leave	Disabled ▾	

Router Port	1	2	3	4	5	6	7	8
	□	□	□	□	□	□	□	□
	9	10	11	12	13	14	15	16
	□	□	□	□	□	□	□	□
	17		18		19		20	
	□		□		□		□	

Note: Query interval must greater than Query Response interval.

IGMP/MLD Snooping: When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic. This is for IGMPv1,v2 and MLDv1 only.

IGMP/MLD Snooping v3: When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic. This is for IGMPv3 and MLDv2 only.

Unregistered IPMC Flooding: Set forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic will flood when enabled. However, the traffic will be forwarded to router-ports only when disabled.

Query Interval: The Query Interval is used to set the time between transmitting IGMP queries, entries between 1 ~ 6000 seconds are allowed. (Default value 125, One Unit =1 second)

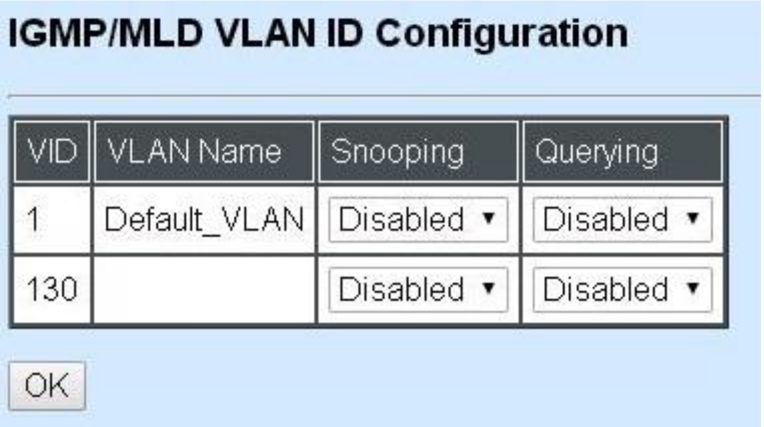
Query Response Interval: This determines the maximum amount of time allowed before sending an IGMP response report. (Default value 100, One Unit=0.1 second)

Fast Leave: The Fast Leave option may be enabled or disabled. When enabled, this allows an interface to be ignored without sending group-specific queries. The default setting is “Enabled”.

Router Ports: When ports are connected to the IGMP administrative routers, they should be checked.

7.4.8.2 IGMP/MLD VLAN ID Configuration

Select the option **IGMP/MLD VLAN ID Configuration** from the **IGMP/MLD Snooping** menu and then the following screen page with the ability information of IGMP Snooping and Querying in VLAN(s) appears.



IGMP/MLD VLAN ID Configuration

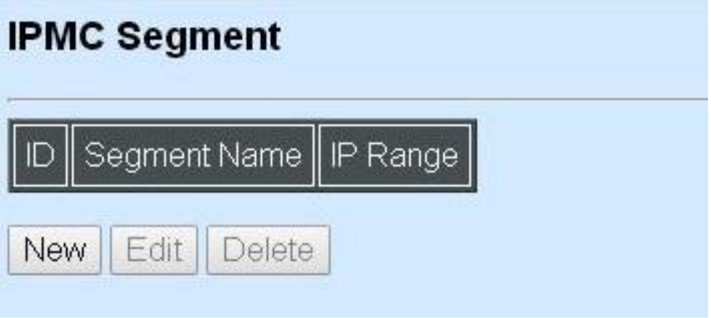
VID	VLAN Name	Snooping	Querying
1	Default_VLAN	Disabled ▾	Disabled ▾
130		Disabled ▾	Disabled ▾

Snooping: When enabled, the port in VLAN will monitor network traffic and determine which hosts to receive the multicast traffic.

Querying: When enabled, the port in VLAN can serve as the Querier which is responsible for asking hosts whether they want to receive multicast traffic.

7.4.8.3 IPMC Segment

Select the option **IPMC Segment** from the **IGMP/MLD Snooping** menu and then the following screen page with the ability information of IPMC Segment **ID**, **Name** and **IP Range** appears.



IPMC Segment

ID	Segment Name	IP Range

ID: View-only field that shows the current registered ID number.

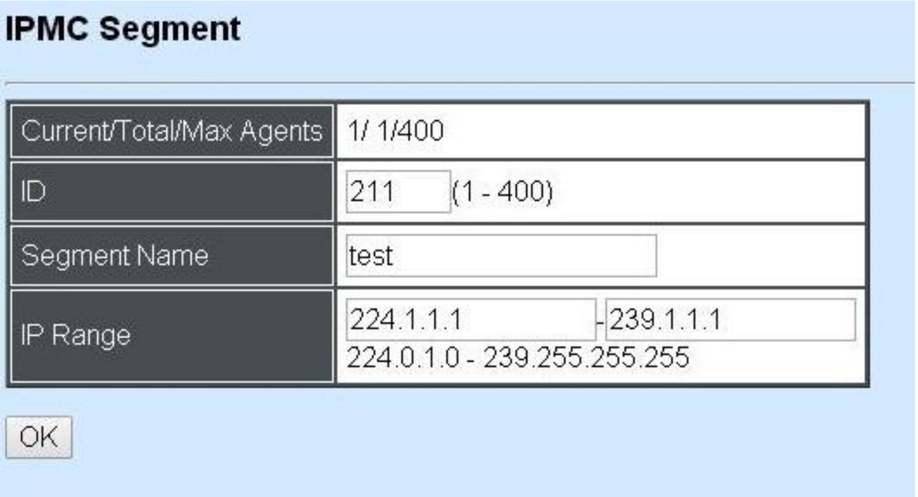
Segment Name: View-only field that shows the current registered Name.

IP Range: View-only field that shows the current registered IP Range.

Click **New** to register a new IPMC Segment and then the following screen page appears.

Click **Edit** to edit and view the IPMC Segment settings.

Click **Delete** to remove a current IPMC Segment registration.



IPMC Segment

Current/Total/Max Agents	1/ 1/400
ID	211 (1 - 400)
Segment Name	test
IP Range	224.1.1.1 - 239.1.1.1 224.0.1.0 - 239.255.255.255

Current/Total/Max Agents: View-only field.

Current: This shows the number of current registered IPMC Segment.

Total: This shows the total number of registered IPMC Segment.

Max: This shows the maximum number available for IPMC Segment. The maximum number is 400.

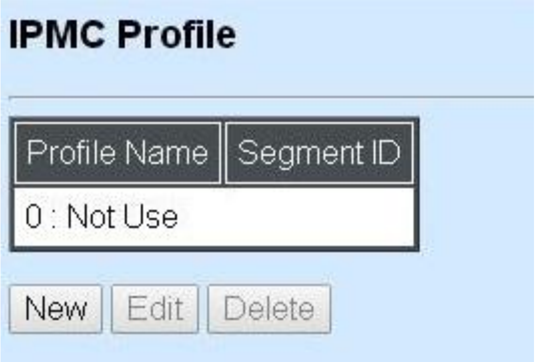
Segment ID: Specify a number from 1~400 for a new ID.

Segment Name: Enter an identification name. This field is limited to 20 characters.

IP Range: Specify the multicast streams IP range for the registered segment. (The IP range is from 224.0.1.0~239.255.255.255.)

7.4.8.4 IPMC Profile

Select the option **IPMC Profile** from the **IGMP/MLD Snooping** menu and then the following screen page with the ability information of IPMC Profile appears.



IPMC Profile

Profile Name	Segment ID
0 : Not Use	

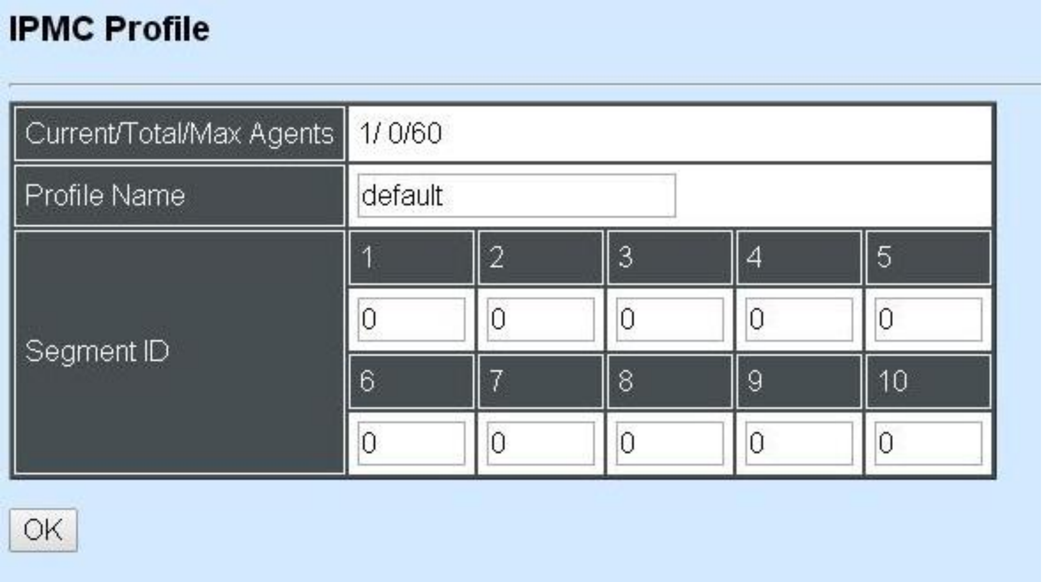
Profile Name: View-only field that shows the current registered profile name.

Segment ID: View-only field that shows the current registered segment ID.

Click **New** to register a new IPMC Profile and then the following screen page appears.

Click **Edit** to edit the IPMC Profile settings.

Click **Delete** to remove a current IPMC Profile registration.



IPMC Profile

Current/Total/Max Agents	1/ 0/60				
Profile Name	default				
Segment ID	1	2	3	4	5
	0	0	0	0	0
	6	7	8	9	10
	0	0	0	0	0

Current/Total/Max Agents: View-only field.

Current: This shows the number of current registered IPMC Profile.

Total: This shows the number of total IPMC Profiles that are registered.

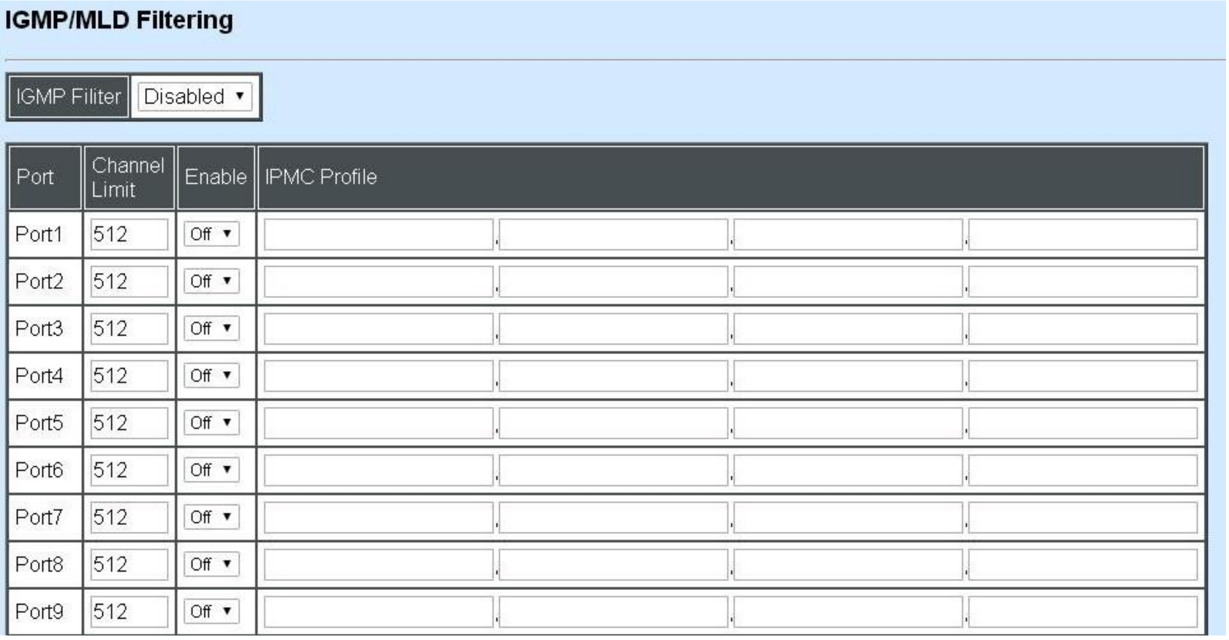
Max: This shows the maximum number available for IPMC Profile. The maximum number is 60.

Profile Name: Enter an identification name. This field is limited to 20 characters.

Segment ID: Specify the segment ID that is registered in **IPMC Segment**.

7.4.8.5 IGMP/MLD Filtering

Select the option **IGMP/MLD Filtering** from the **IGMP/MLD Snooping** menu and then the following screen page appears.



IGMP/MLD Filtering

IGMP Filter: Disabled ▾

Port	Channel Limit	Enable	IPMC Profile
Port1	512	Off ▾	, , ,
Port2	512	Off ▾	, , ,
Port3	512	Off ▾	, , ,
Port4	512	Off ▾	, , ,
Port5	512	Off ▾	, , ,
Port6	512	Off ▾	, , ,
Port7	512	Off ▾	, , ,
Port8	512	Off ▾	, , ,
Port9	512	Off ▾	, , ,

IGMP Filter: This option may enable or disable the IGMP filter. The default setting is “Disabled”.

Port: View-only field that shows the port number that is currently configured.

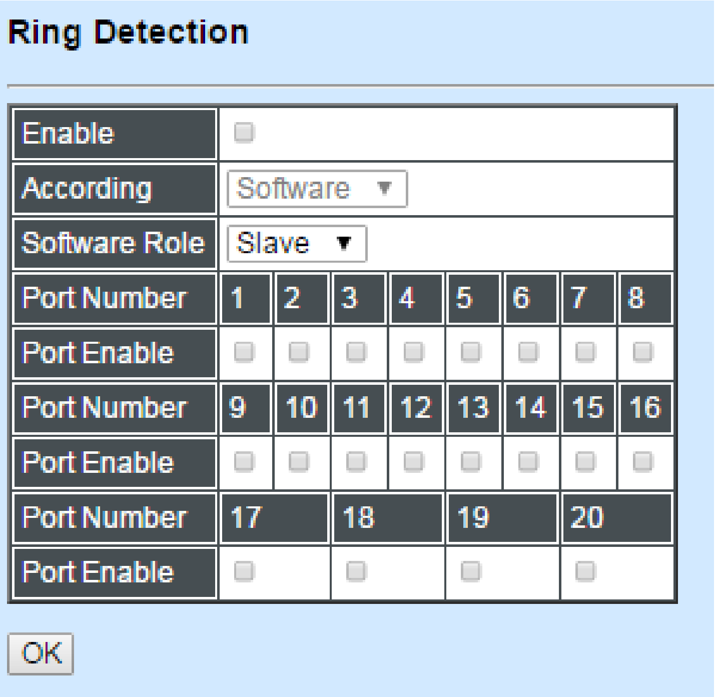
Channel Limit: Specify the maximum transport multicast stream.

Enable: To enable each port’s IGMP filtering function. The default setting is “Off” which is disabled.

IPMC Profile: In IGMP filtering, it only allows information specified in IPMC Profile fields to pass through. (The field for IPMC Profile name is from the entry registered in **IPMC Profile** option.)

7.4.9 Ring Detection

Ring Detection used in ring topology is a helpful way of network recovery, preventing from disconnection resulting from any unexpected link down. The main advantages of Ring Detection are lower cost for cabling and installation, and high-speed recovery time.



Enable	□							
According	Software ▼							
Software Role	Slave ▼							
Port Number	1	2	3	4	5	6	7	8
Port Enable	□	□	□	□	□	□	□	□
Port Number	9	10	11	12	13	14	15	16
Port Enable	□	□	□	□	□	□	□	□
Port Number	17		18		19		20	
Port Enable	□		□		□		□	

Enable: Check Enable box to activate Ring Detection or vice versa.

According: This is a fixed filed that Ring Detection can be configured by software only..

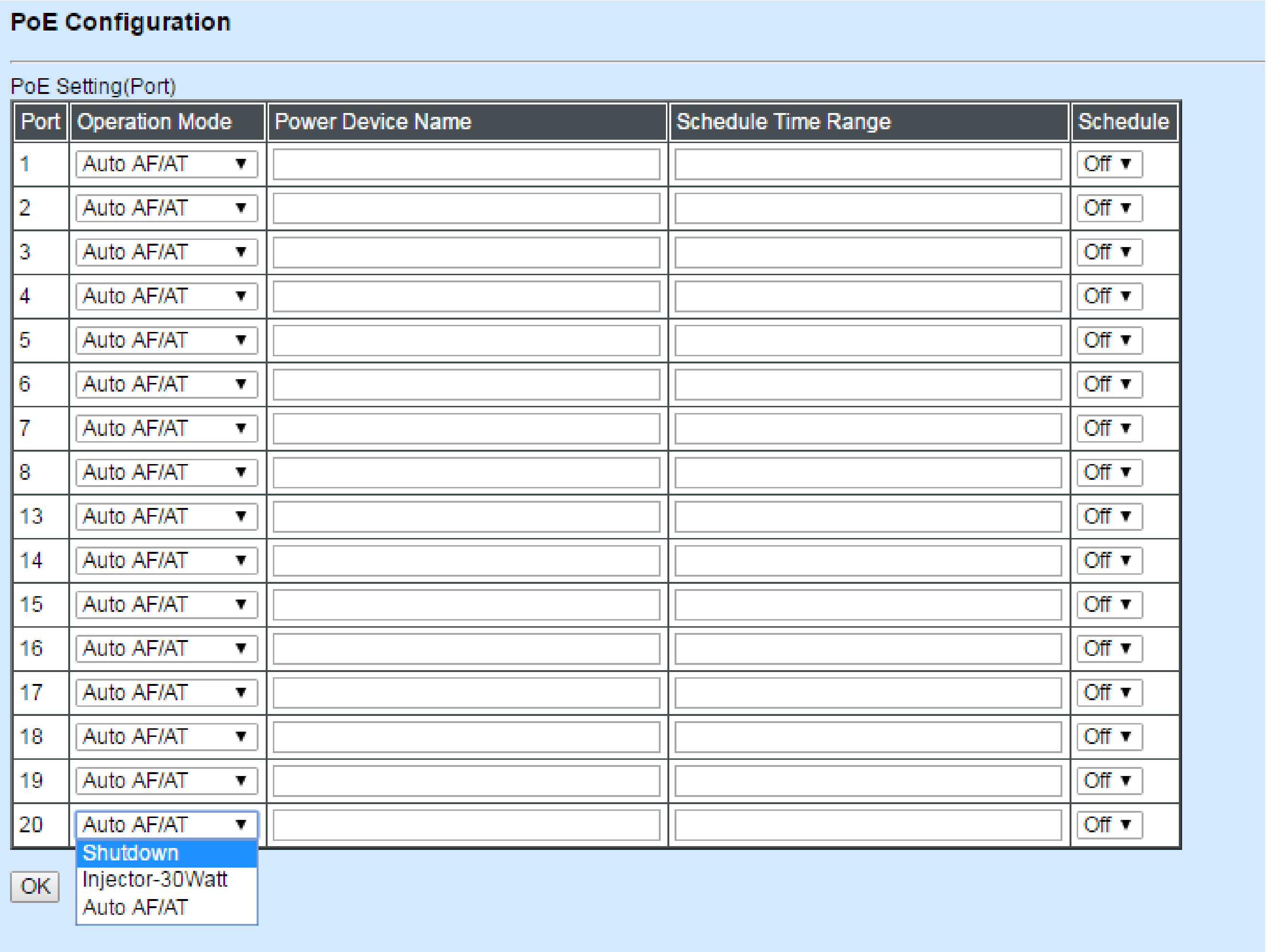
Role: Assign the role of the switch as either Slave or Master. Check the drop-down box to select either Master or Slave.
Master: A role posses the ability of blocking or forwarding packet.
Slave: A role posses the ability of forwarding packet only.

Port Number/Port Enable: Six ports are available at each switch. Select and check two of them for Ring Detection.

Click the **"OK"** button to apply the settings.

7.4.10 PoE Configuration

Click the option **PoE Configuration** from the **Management** menu and then the following screen page appears.



PoE Configuration

PoE Setting(Port)

Port	Operation Mode	Power Device Name	Schedule Time Range	Schedule
1	Auto AF/AT ▼			Off ▼
2	Auto AF/AT ▼			Off ▼
3	Auto AF/AT ▼			Off ▼
4	Auto AF/AT ▼			Off ▼
5	Auto AF/AT ▼			Off ▼
6	Auto AF/AT ▼			Off ▼
7	Auto AF/AT ▼			Off ▼
8	Auto AF/AT ▼			Off ▼
13	Auto AF/AT ▼			Off ▼
14	Auto AF/AT ▼			Off ▼
15	Auto AF/AT ▼			Off ▼
16	Auto AF/AT ▼			Off ▼
17	Auto AF/AT ▼			Off ▼
18	Auto AF/AT ▼			Off ▼
19	Auto AF/AT ▼			Off ▼
20	Auto AF/AT ▼			Off ▼

Operation Mode: There are several modes available.

Shutdown: Refers to disable PoE on a port permanently.

Auto AF/AT: Refers to flexibly enable PoE on a port the connected device at the other end. Under Auto AF/AT mode, it automatically detects the connected device if the device supports PoE feature. If not, it won't give the connected device power.

Injector-30 Watt: Refers to enable PoE on a port permanently at 30 Watt level.
Injector-60 Watt: Refers to enable PoE on a port permanently at 60 Watt level.

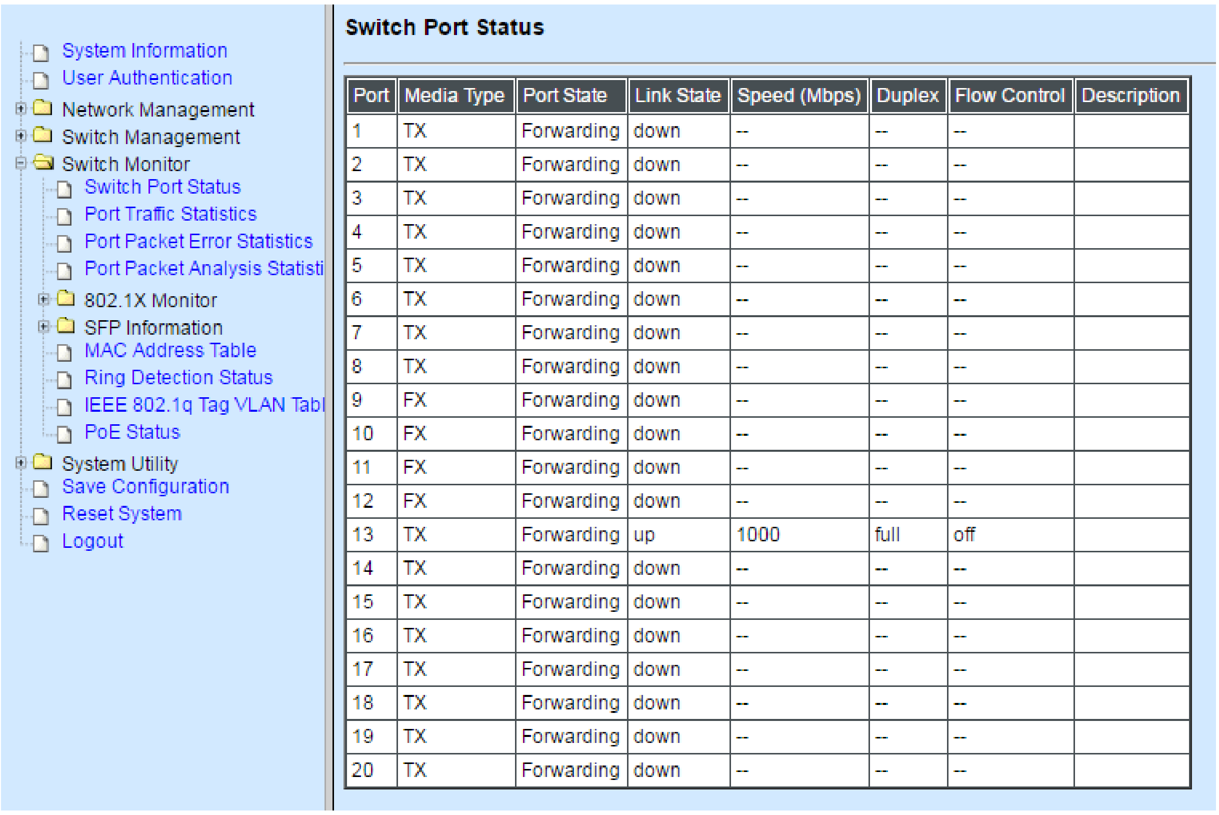
Power Device Name: Specify a name to the powered device connected with the ports.

Schedule Time Range: Assign PoE schedule a time-range. It defines which previously-configured time interval the port should follow. One set of time interval can be accepted at a time.

Schedule: On or Off PoE schedule function.

7.5 Switch Monitor

Switch Monitor allows users to monitor the real-time operation status of the Managed Industrial PoE Switch. Users may monitor the port link-up status or traffic counters for maintenance or diagnostic purposes. Select the folder **Switch Monitor** from the **Main Menu** and then the following screen page appears.



Switch Port Status

Port	Media Type	Port State	Link State	Speed (Mbps)	Duplex	Flow Control	Description
1	TX	Forwarding	down	--	--	--	
2	TX	Forwarding	down	--	--	--	
3	TX	Forwarding	down	--	--	--	
4	TX	Forwarding	down	--	--	--	
5	TX	Forwarding	down	--	--	--	
6	TX	Forwarding	down	--	--	--	
7	TX	Forwarding	down	--	--	--	
8	TX	Forwarding	down	--	--	--	
9	FX	Forwarding	down	--	--	--	
10	FX	Forwarding	down	--	--	--	
11	FX	Forwarding	down	--	--	--	
12	FX	Forwarding	down	--	--	--	
13	TX	Forwarding	up	1000	full	off	
14	TX	Forwarding	down	--	--	--	
15	TX	Forwarding	down	--	--	--	
16	TX	Forwarding	down	--	--	--	
17	TX	Forwarding	down	--	--	--	
18	TX	Forwarding	down	--	--	--	
19	TX	Forwarding	down	--	--	--	
20	TX	Forwarding	down	--	--	--	

1. **Switch Port Status:** View the port status such as media type, port state, etc.

2. **Port Traffic Statistics:** View the real-time statistics of the Managed Industrial PoE Switch,

3. **Port Packet Error Statistics:** View each port's traffic condition of error packets, e.g. CRC, fragment, Jabber, etc.

4. **Port Packet Analysis Statistics:** View each port's traffic condition of error packets, e.g. RX/TX frames of Multicast and Broadcast, etc.

5. **802.1X Port Status:** View port status and Statistics.

6. **802.1X Statistics:** View the real-time 802.1X port statistics status of the Managed Switch.

7. **SFP Port Info:** View the current port's SFP information, e.g. Speed, Distance, Vendor Name, Vendor PN, Vendor SN, Temperature, Voltage, TX Bias, TX Power and RX Power.

8. **SFP Port State:** View the current port's SFP Port State, e.g. Port, Temperature, Voltage, TX Bias, TX Power, RX Power, etc..

9. **MAC Address Table:** List current MAC addresses learned by the Managed Industrial PoE Switch.

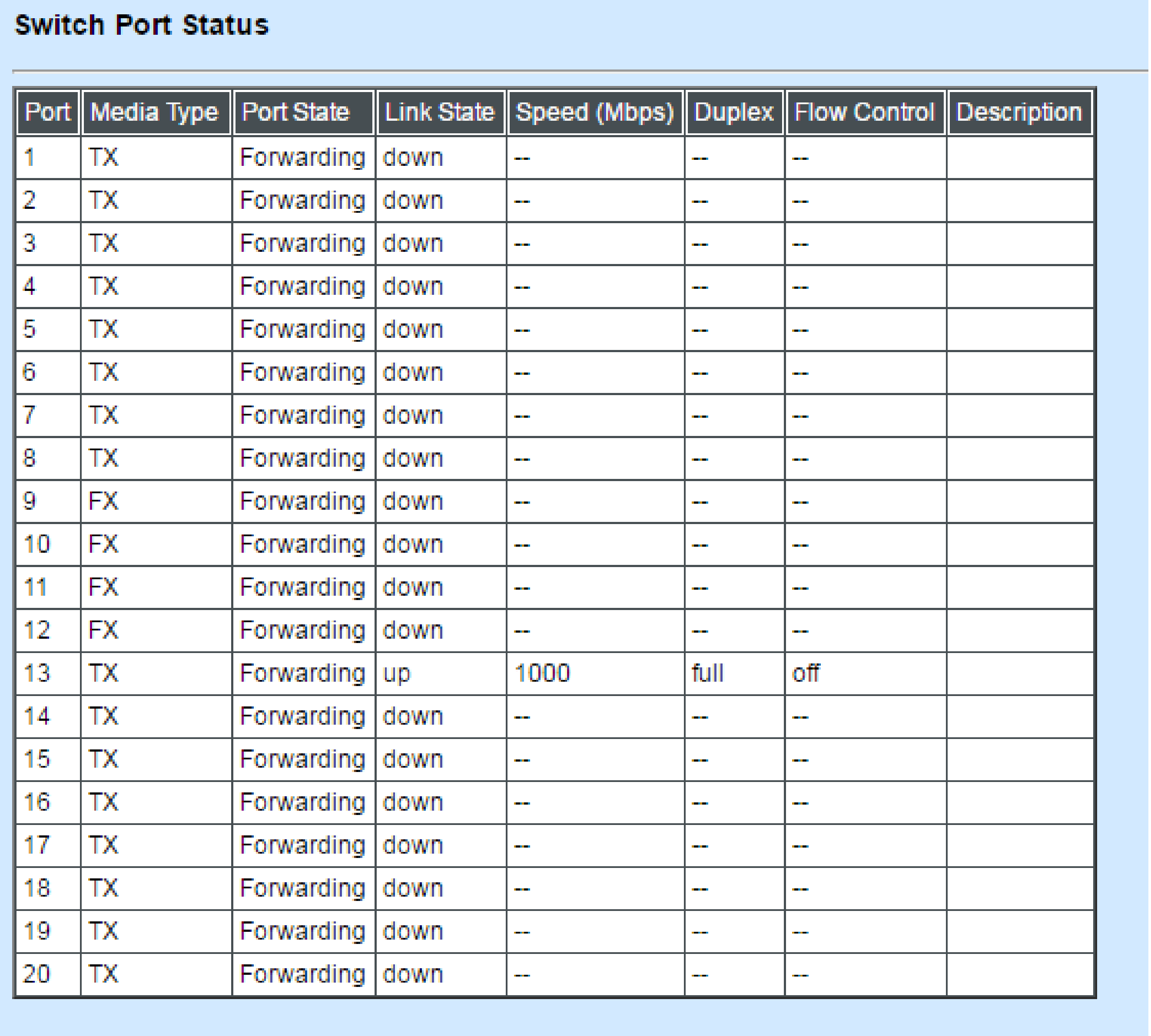
10. **Ring Detection Status:** View the current status of Ring Detection.

11. **PoE IEEE 802.1q Tag VLAN Table:** View the current IEEE 802.1q Tag VLAN Table.

12. **PoE Status:** View the current status of PoE per port.

7.5.1 Switch Port Status

The following screen page appears if you choose **Switch Monitor** menu and then select **Switch Port Status**.



Switch Port Status

Port	Media Type	Port State	Link State	Speed (Mbps)	Duplex	Flow Control	Description
1	TX	Forwarding	down	--	--	--	
2	TX	Forwarding	down	--	--	--	
3	TX	Forwarding	down	--	--	--	
4	TX	Forwarding	down	--	--	--	
5	TX	Forwarding	down	--	--	--	
6	TX	Forwarding	down	--	--	--	
7	TX	Forwarding	down	--	--	--	
8	TX	Forwarding	down	--	--	--	
9	FX	Forwarding	down	--	--	--	
10	FX	Forwarding	down	--	--	--	
11	FX	Forwarding	down	--	--	--	
12	FX	Forwarding	down	--	--	--	
13	TX	Forwarding	up	1000	full	off	
14	TX	Forwarding	down	--	--	--	
15	TX	Forwarding	down	--	--	--	
16	TX	Forwarding	down	--	--	--	
17	TX	Forwarding	down	--	--	--	
18	TX	Forwarding	down	--	--	--	
19	TX	Forwarding	down	--	--	--	
20	TX	Forwarding	down	--	--	--	

Port: It shows the number of the port.

Media Type: It shows the media type of the port, either Copper (TX) or Fiber (FX).

Port State: It shows each port’s state, either **D** (Disabled) or **E** (Enabled).

Disabled: Packets cannot be received and forwarded.

Enabled: Packets can be forwarded.

Link State: It shows the current link status of the port, either up or down.

Speed (Mbps): It shows the current operation speed of each port.

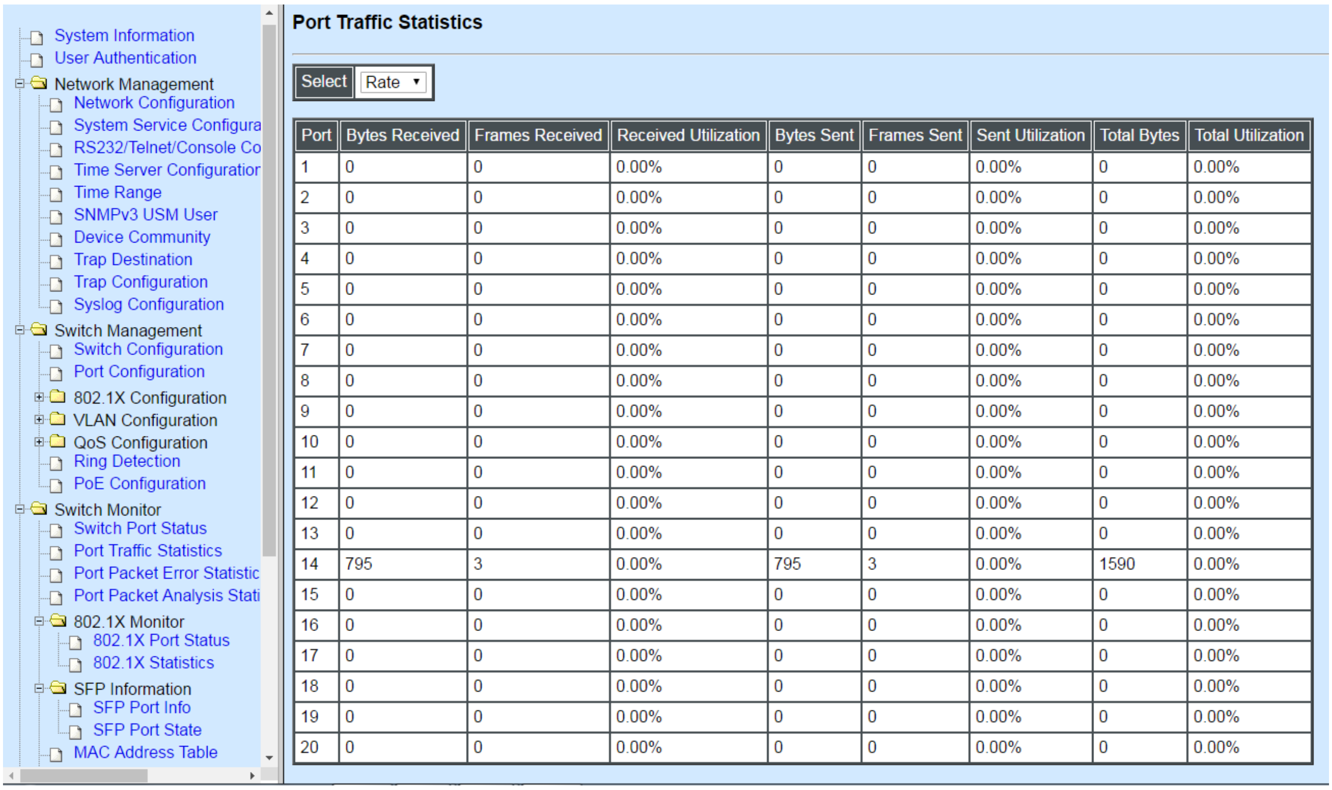
Duplex: It shows the current operation Duplex mode of each port, either Full or Half.

Flow Control: It shows the port status of Flow Control function, either on or off.

Description: It shows the description of the port described in “Port Configuration”.

7.5.2 Port Traffic Statistics

To view the real-time statistics of the Managed Industrial PoE Switch, click **Port Traffic Statistics** folder from **Switch Monitor** menu and then the three options appear.



Port Traffic Statistics

Select: Rate

Port	Bytes Received	Frames Received	Received Utilization	Bytes Sent	Frames Sent	Sent Utilization	Total Bytes	Total Utilization
1	0	0	0.00%	0	0	0.00%	0	0.00%
2	0	0	0.00%	0	0	0.00%	0	0.00%
3	0	0	0.00%	0	0	0.00%	0	0.00%
4	0	0	0.00%	0	0	0.00%	0	0.00%
5	0	0	0.00%	0	0	0.00%	0	0.00%
6	0	0	0.00%	0	0	0.00%	0	0.00%
7	0	0	0.00%	0	0	0.00%	0	0.00%
8	0	0	0.00%	0	0	0.00%	0	0.00%
9	0	0	0.00%	0	0	0.00%	0	0.00%
10	0	0	0.00%	0	0	0.00%	0	0.00%
11	0	0	0.00%	0	0	0.00%	0	0.00%
12	0	0	0.00%	0	0	0.00%	0	0.00%
13	0	0	0.00%	0	0	0.00%	0	0.00%
14	795	3	0.00%	795	3	0.00%	1590	0.00%
15	0	0	0.00%	0	0	0.00%	0	0.00%
16	0	0	0.00%	0	0	0.00%	0	0.00%
17	0	0	0.00%	0	0	0.00%	0	0.00%
18	0	0	0.00%	0	0	0.00%	0	0.00%
19	0	0	0.00%	0	0	0.00%	0	0.00%
20	0	0	0.00%	0	0	0.00%	0	0.00%

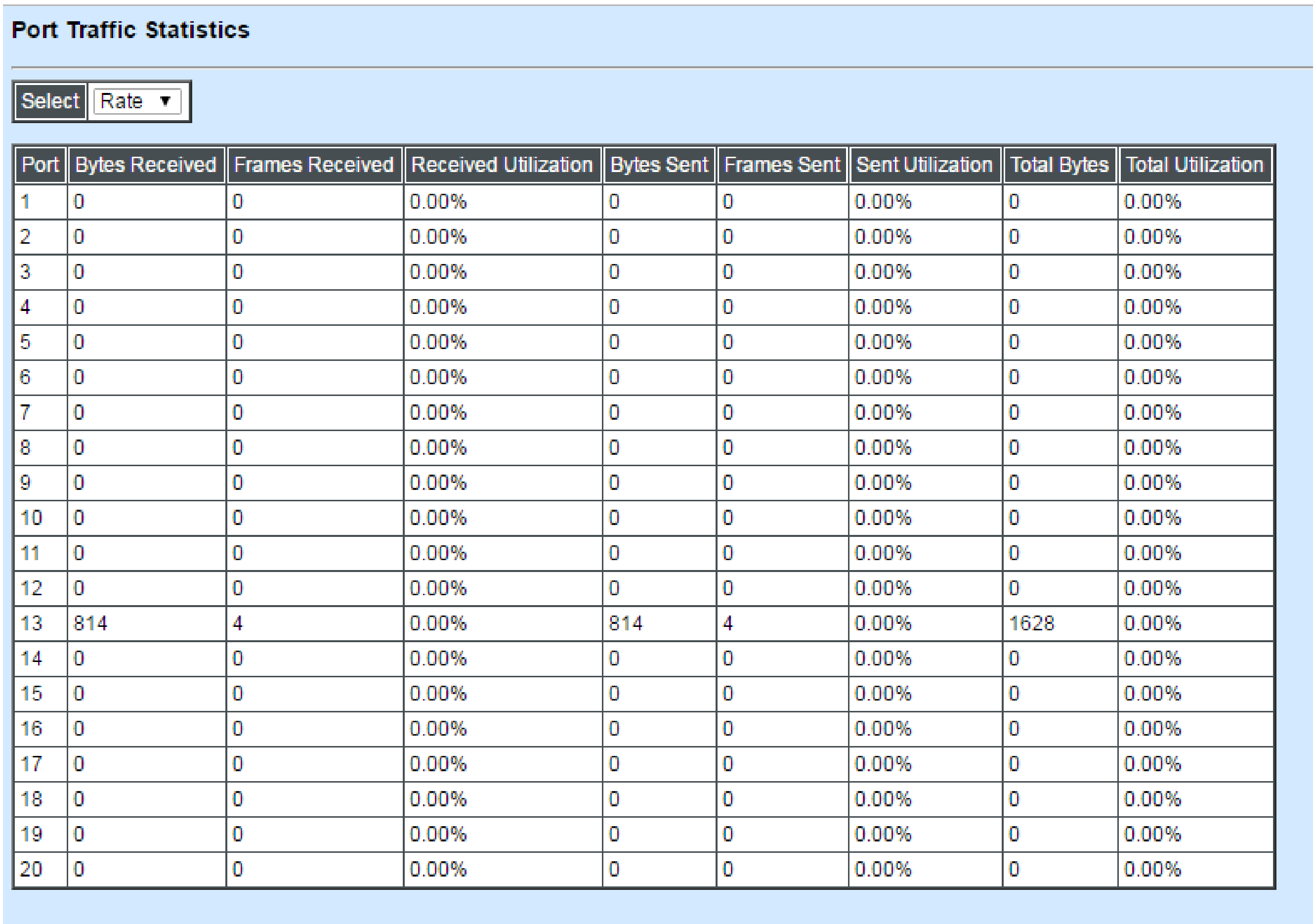
1. **Port Traffic Statistics (Rates):** View the number of bytes received, frames received, bytes sent, frames sent, total bytes, etc.

2. **Port Packet Error Statistics (Rates):** View the number of CRC errors, undersize frames, fragment frames, etc.

3. **Port Packet Analysis Statistics (Rates):** View each port's frames analysis.

7.5.2.1 Port Traffic Statistics (Rate)

The following screen page appears if you choose **Port Traffic Rates** and then select **Port Traffic Statistics (Rate)**.



Port Traffic Statistics

Port	Bytes Received	Frames Received	Received Utilization	Bytes Sent	Frames Sent	Sent Utilization	Total Bytes	Total Utilization
1	0	0	0.00%	0	0	0.00%	0	0.00%
2	0	0	0.00%	0	0	0.00%	0	0.00%
3	0	0	0.00%	0	0	0.00%	0	0.00%
4	0	0	0.00%	0	0	0.00%	0	0.00%
5	0	0	0.00%	0	0	0.00%	0	0.00%
6	0	0	0.00%	0	0	0.00%	0	0.00%
7	0	0	0.00%	0	0	0.00%	0	0.00%
8	0	0	0.00%	0	0	0.00%	0	0.00%
9	0	0	0.00%	0	0	0.00%	0	0.00%
10	0	0	0.00%	0	0	0.00%	0	0.00%
11	0	0	0.00%	0	0	0.00%	0	0.00%
12	0	0	0.00%	0	0	0.00%	0	0.00%
13	814	4	0.00%	814	4	0.00%	1628	0.00%
14	0	0	0.00%	0	0	0.00%	0	0.00%
15	0	0	0.00%	0	0	0.00%	0	0.00%
16	0	0	0.00%	0	0	0.00%	0	0.00%
17	0	0	0.00%	0	0	0.00%	0	0.00%
18	0	0	0.00%	0	0	0.00%	0	0.00%
19	0	0	0.00%	0	0	0.00%	0	0.00%
20	0	0	0.00%	0	0	0.00%	0	0.00%

Bytes Received: The total bytes received from each port.

Frames Received: The total frames received from each port.

Received Utilization: The ratio of each port's receiving traffic to the port's current bandwidth.

Bytes Sent: The total bytes sent from the current port.

Frames Sent: The total frames sent from the current port.

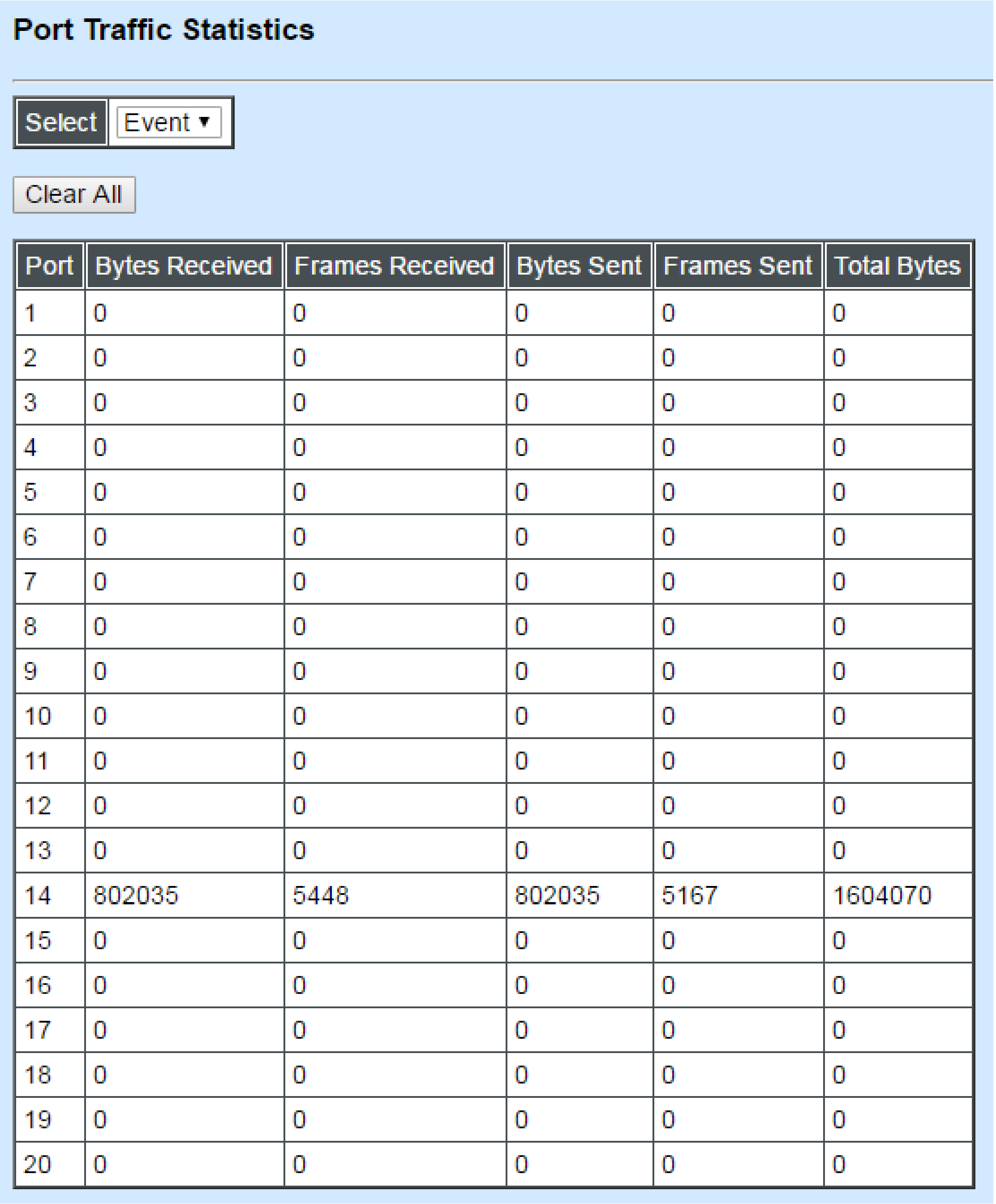
Sent Utilization: The ratio of each port's sending traffic to the port's current bandwidth.

Total Bytes: The total bytes received and sent from the current port.

Total Utilization: The ratio of each port's receiving and sending traffic to the port's current bandwidth.

7.5.2.2 Port Traffic Statistics (Event)

The following screen page appears if you choose **Port Traffic Statistics** and then select **Port Traffic Statistics (Event)**.



Port	Bytes Received	Frames Received	Bytes Sent	Frames Sent	Total Bytes
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0
8	0	0	0	0	0
9	0	0	0	0	0
10	0	0	0	0	0
11	0	0	0	0	0
12	0	0	0	0	0
13	0	0	0	0	0
14	802035	5448	802035	5167	1604070
15	0	0	0	0	0
16	0	0	0	0	0
17	0	0	0	0	0
18	0	0	0	0	0
19	0	0	0	0	0
20	0	0	0	0	0

Bytes Received: The total bytes received from each port.

Frames Received: The total frames received from each port.

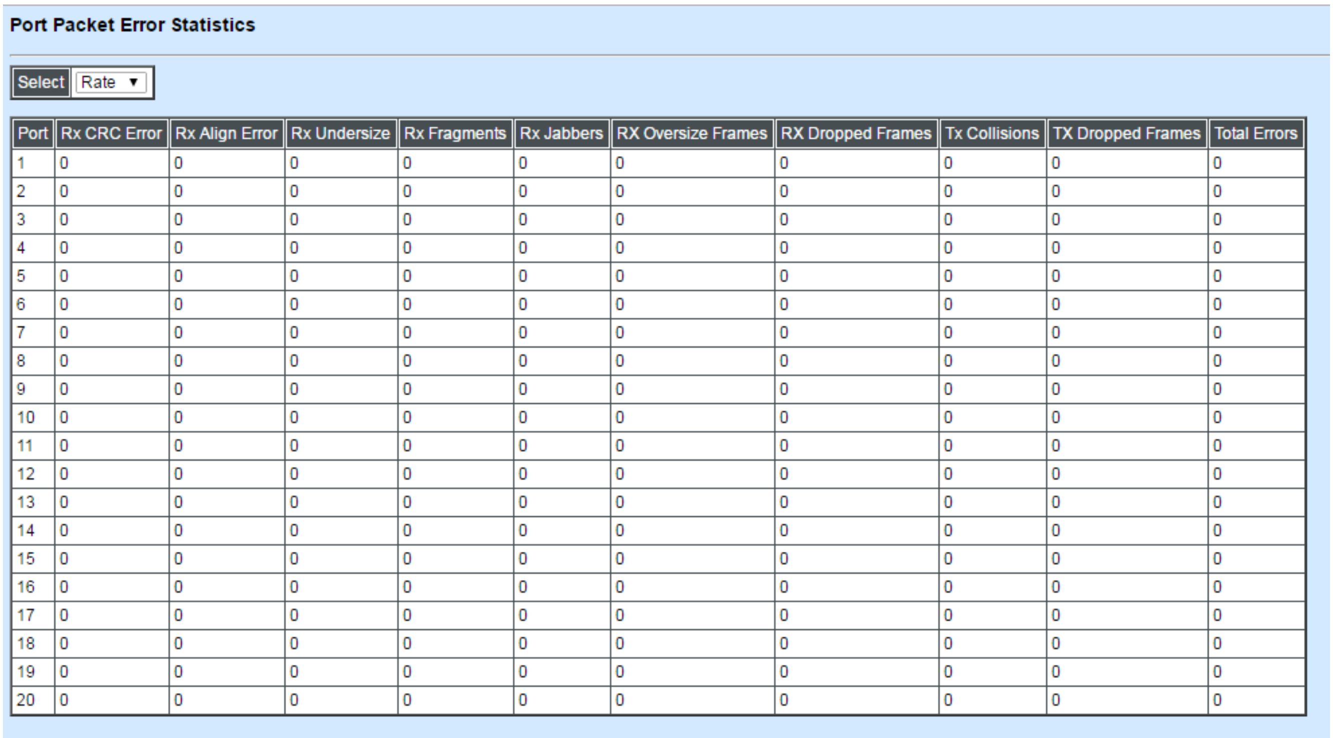
Bytes Sent: The total bytes sent from the current port.

Frames Sent: The total frames sent from the current port.

Total Bytes: The total bytes received and sent from the current port.

7.5.2.3 Port Packet Error Statistics (Rate)

The following screen page appears if you choose **Port Packet Error Rates** and then select **Port Packet Error Statistics (Rate)**.



Port Packet Error Statistics

Select: Rate

Port	Rx CRC Error	Rx Align Error	Rx Undersize	Rx Fragments	Rx Jabbers	RX Oversize Frames	RX Dropped Frames	Tx Collisions	TX Dropped Frames	Total Errors
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0

Rx CRC Error: CRC Error frames received.

Rx Align Error: Align Error frames received.

Rx Undersize: Undersize frames received.

RX Fragments: Fragments frames received.

Rx Oversized Frames: Oversize frames received.

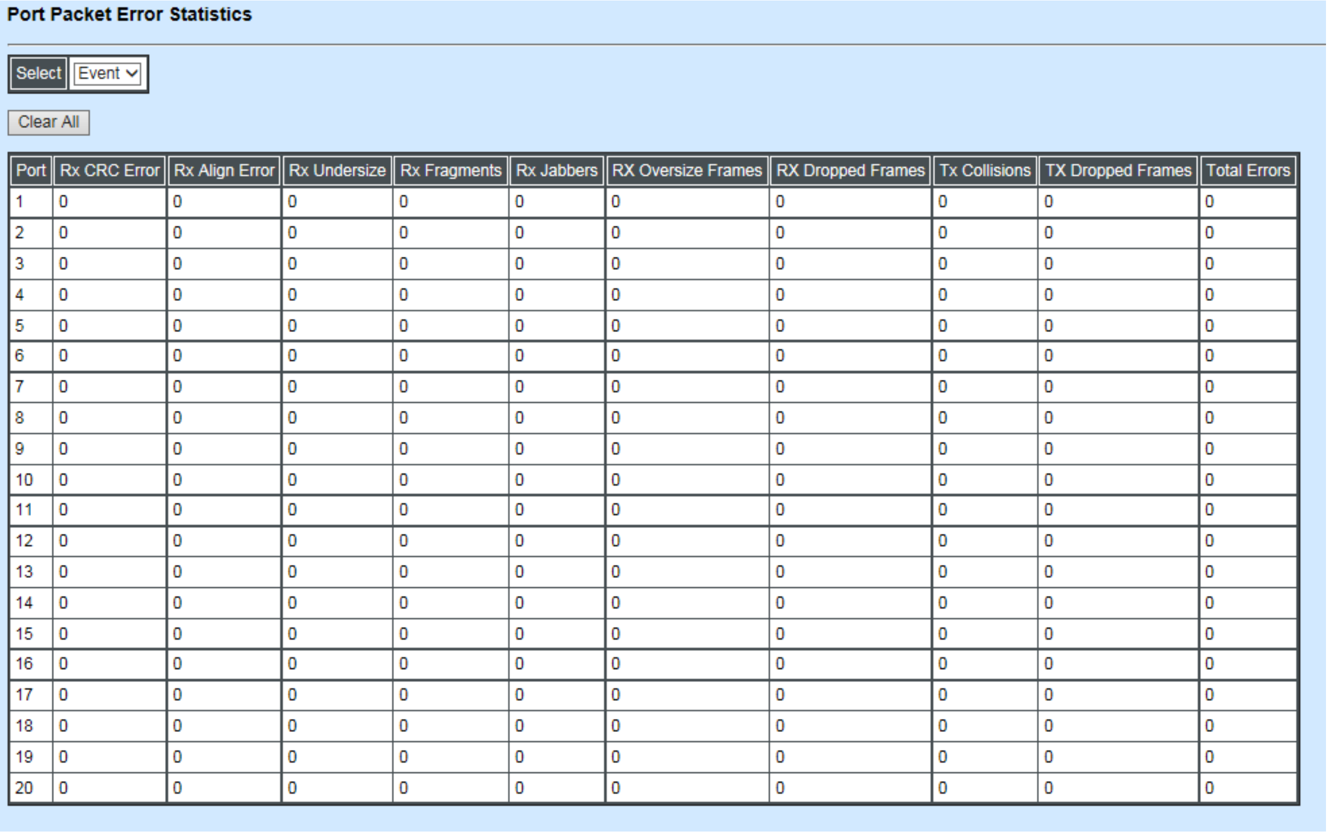
Rx Dropped Frames: Drop frames received.

Tx Collisions: Each port’s Collision frames.

Tx Dropped Frames: Drop frames sent.

Total Errors: Total error frames received.

7.5.2.4 Port Packet Error Statistics (Event)



Port Packet Error Statistics

Port	Rx CRC Error	Rx Align Error	Rx Undersize	Rx Fragments	Rx Jabbers	RX Oversize Frames	RX Dropped Frames	Tx Collisions	TX Dropped Frames	Total Errors
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0

Rx CRC Error: CRC Error frames received.

Rx Align Error: Align Error frames received.

Rx Undersize: Undersize frames received.

RX Fragments: Fragments frames received.

Rx Oversized Frames: Oversize frames received.

Rx Dropped Frames: Drop frames received.

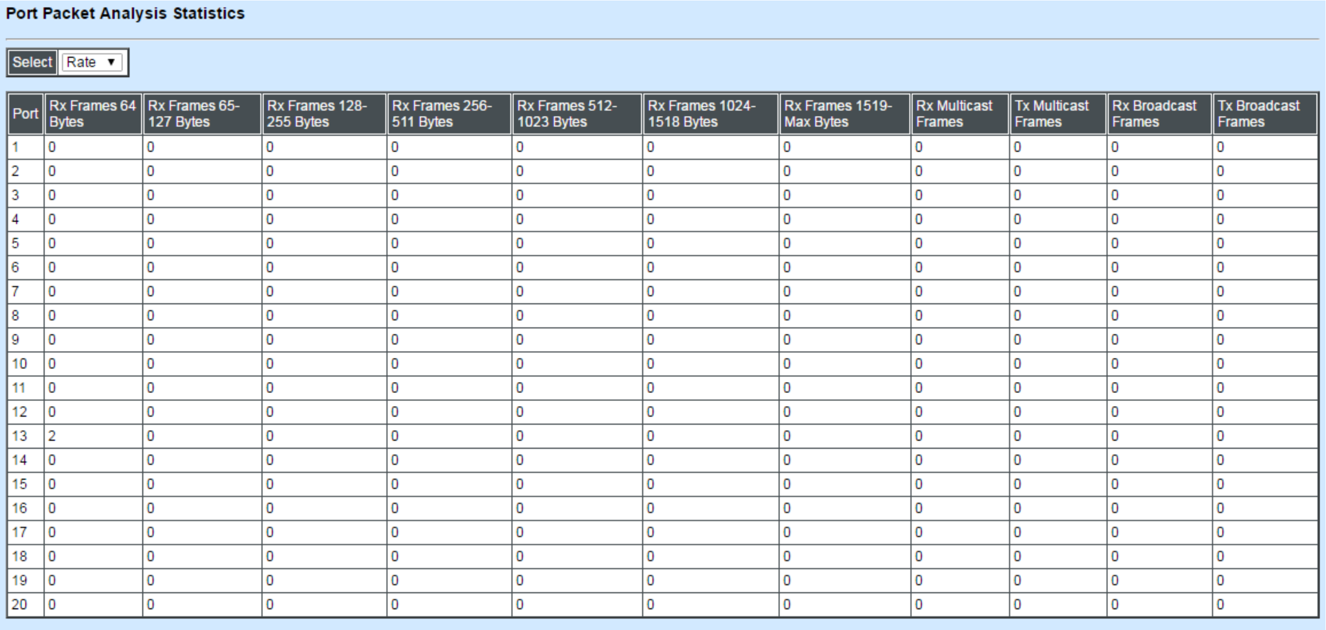
Tx Collisions: Each port’s Collision frames.

Tx Dropped Frames: Drop frames sent.

Total Errors: Total error frames received.

7.5.2.5 Port Packet Analysis Statistics (Rate)

The following screen page appears if you choose **Port Counters Rates** and then select **Port Packet Analysis Statistics (Rate)**.



Port Packet Analysis Statistics

Select Rate ▾

Port	Rx Frames 64 Bytes	Rx Frames 65-127 Bytes	Rx Frames 128-255 Bytes	Rx Frames 256-511 Bytes	Rx Frames 512-1023 Bytes	Rx Frames 1024-1518 Bytes	Rx Frames 1519-Max Bytes	Rx Multicast Frames	Tx Multicast Frames	Rx Broadcast Frames	Tx Broadcast Frames
1	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0
13	2	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0

RX Frames 64 Bytes: 64 bytes frames received.

RX Frames 65-127 Bytes: 65-127 bytes frames received.

RX Frames 128-255 Bytes: 128-255 bytes frames received.

RX Frames 256-511 Bytes: 256-511 bytes frames received.

RX Frames 512-1023 Bytes: 512-1023 bytes frames received.

RX Frames 1024-10240 Bytes: 1024-10240 bytes frames received.

RX Multicast Frames: Good multicast frames received.

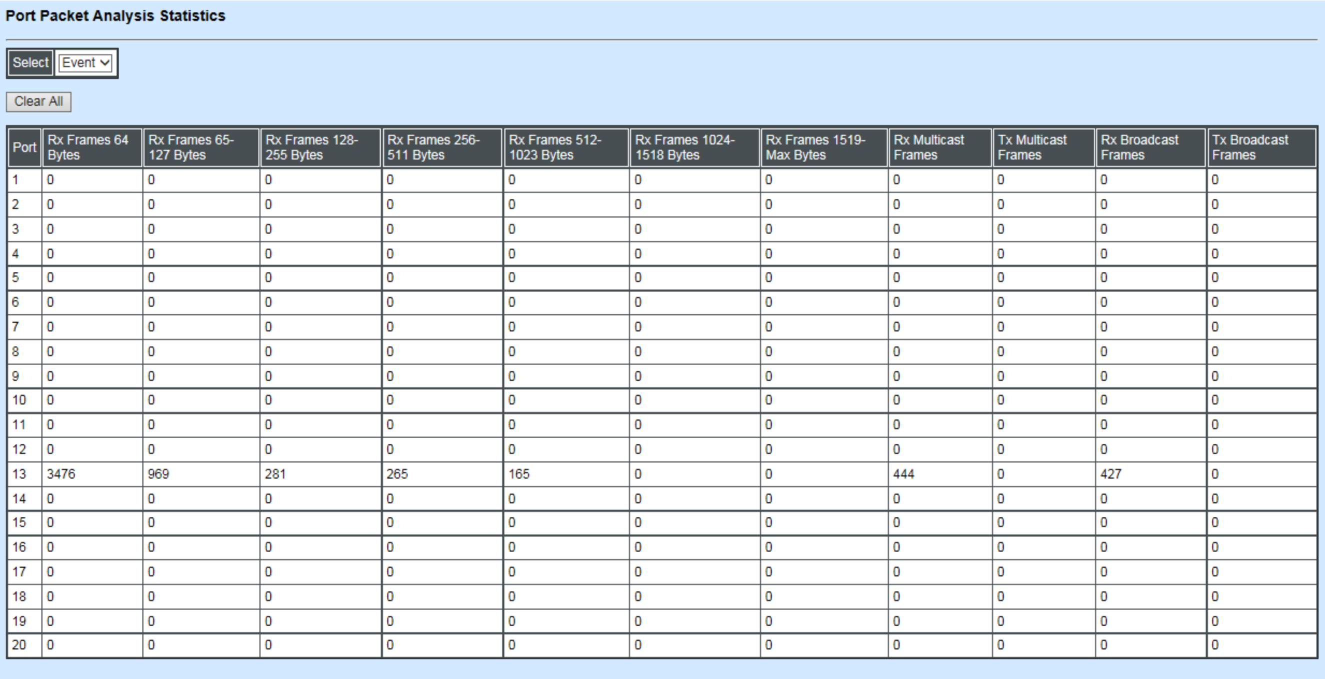
TX Multicast Frames: Good multicast packets sent.

RX Broadcast Frames: Good broadcast frames received.

TX Broadcast Frames: Good broadcast packets sent.

7.5.2.6 Port Packet Analysis Statistics (Event)

The following screen page appears if you choose **Port Counters Rates** and then select **Port Packet Analysis Statistics (Event)**.



Port Packet Analysis Statistics

Port	Rx Frames 64 Bytes	Rx Frames 65-127 Bytes	Rx Frames 128-255 Bytes	Rx Frames 256-511 Bytes	Rx Frames 512-1023 Bytes	Rx Frames 1024-1518 Bytes	Rx Frames 1519-Max Bytes	Rx Multicast Frames	Tx Multicast Frames	Rx Broadcast Frames	Tx Broadcast Frames
1	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0
13	3476	969	281	265	165	0	0	444	0	427	0
14	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0

RX Frames 64 Bytes: 64 bytes frames received.

RX Frames 65-127 Bytes: 65-127 bytes frames received.

RX Frames 128-255 Bytes: 128-255 bytes frames received.

RX Frames 256-511 Bytes: 256-511 bytes frames received.

RX Frames 512-1023 Bytes: 512-1023 bytes frames received.

RX Frames 1024-10240 Bytes: 1024-10240 bytes frames received.

RX Multicast Frames: Good multicast frames received.

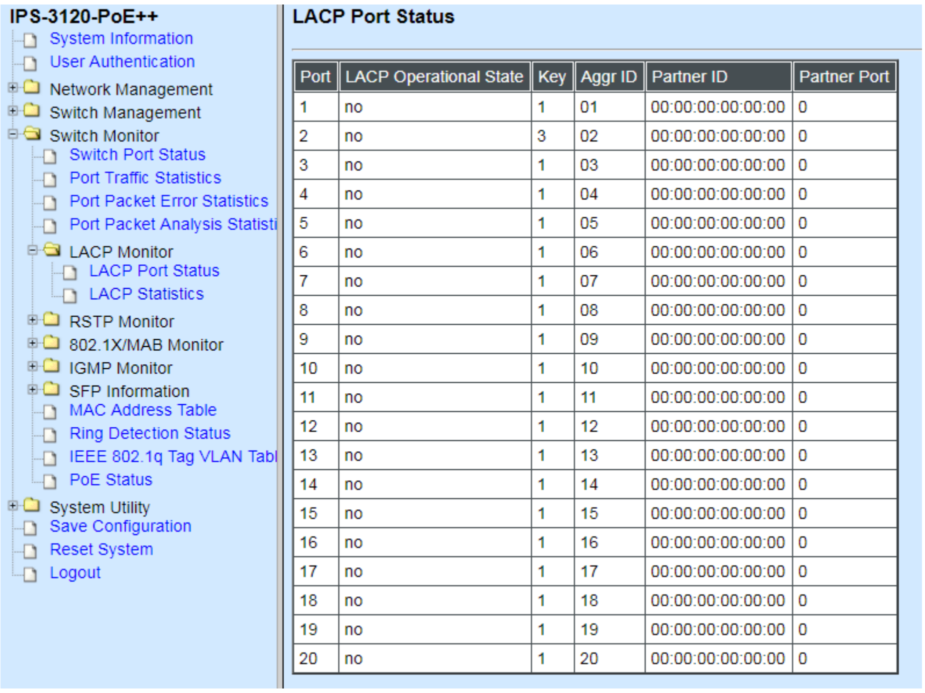
TX Multicast Frames: Good multicast packets sent.

RX Broadcast Frames: Good broadcast frames received.

TX Broadcast Frames: Good broadcast packets sent.

7.5.3 LACP Monitor

Click the **LACP Monitor** folder and then the two options will appears.

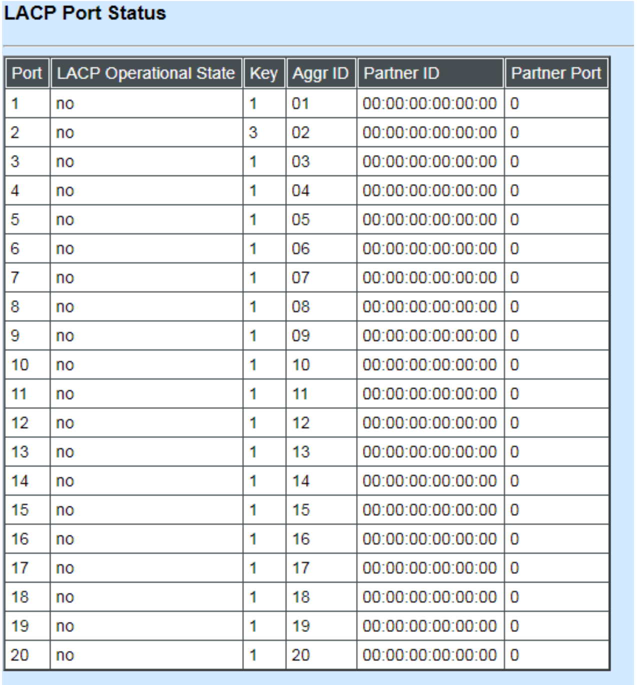


LACP Port Status

Port	LACP Operational State	Key	Aggr ID	Partner ID	Partner Port
1	no	1	01	00:00:00:00:00:00	0
2	no	3	02	00:00:00:00:00:00	0
3	no	1	03	00:00:00:00:00:00	0
4	no	1	04	00:00:00:00:00:00	0
5	no	1	05	00:00:00:00:00:00	0
6	no	1	06	00:00:00:00:00:00	0
7	no	1	07	00:00:00:00:00:00	0
8	no	1	08	00:00:00:00:00:00	0
9	no	1	09	00:00:00:00:00:00	0
10	no	1	10	00:00:00:00:00:00	0
11	no	1	11	00:00:00:00:00:00	0
12	no	1	12	00:00:00:00:00:00	0
13	no	1	13	00:00:00:00:00:00	0
14	no	1	14	00:00:00:00:00:00	0
15	no	1	15	00:00:00:00:00:00	0
16	no	1	16	00:00:00:00:00:00	0
17	no	1	17	00:00:00:00:00:00	0
18	no	1	18	00:00:00:00:00:00	0
19	no	1	19	00:00:00:00:00:00	0
20	no	1	20	00:00:00:00:00:00	0

7.5.3.1 LACP Port Status

LACP Port Status allows users to view a list of all LACP ports' information. Select **LACP Port Status** from the **LACP monitor** menu and then the following screen page appears.



LACP Port Status

Port	LACP Operational State	Key	Aggr ID	Partner ID	Partner Port
1	no	1	01	00:00:00:00:00:00	0
2	no	3	02	00:00:00:00:00:00	0
3	no	1	03	00:00:00:00:00:00	0
4	no	1	04	00:00:00:00:00:00	0
5	no	1	05	00:00:00:00:00:00	0
6	no	1	06	00:00:00:00:00:00	0
7	no	1	07	00:00:00:00:00:00	0
8	no	1	08	00:00:00:00:00:00	0
9	no	1	09	00:00:00:00:00:00	0
10	no	1	10	00:00:00:00:00:00	0
11	no	1	11	00:00:00:00:00:00	0
12	no	1	12	00:00:00:00:00:00	0
13	no	1	13	00:00:00:00:00:00	0
14	no	1	14	00:00:00:00:00:00	0
15	no	1	15	00:00:00:00:00:00	0
16	no	1	16	00:00:00:00:00:00	0
17	no	1	17	00:00:00:00:00:00	0
18	no	1	18	00:00:00:00:00:00	0
19	no	1	19	00:00:00:00:00:00	0
20	no	1	20	00:00:00:00:00:00	0

In this page, you can find the following information about LACP port status:

Port Number: The number of the port.

LACP Operational State: Current operational state of LACP

Key: The current operational key for the LACP group.

Aggr ID: The ID of the LACP group.

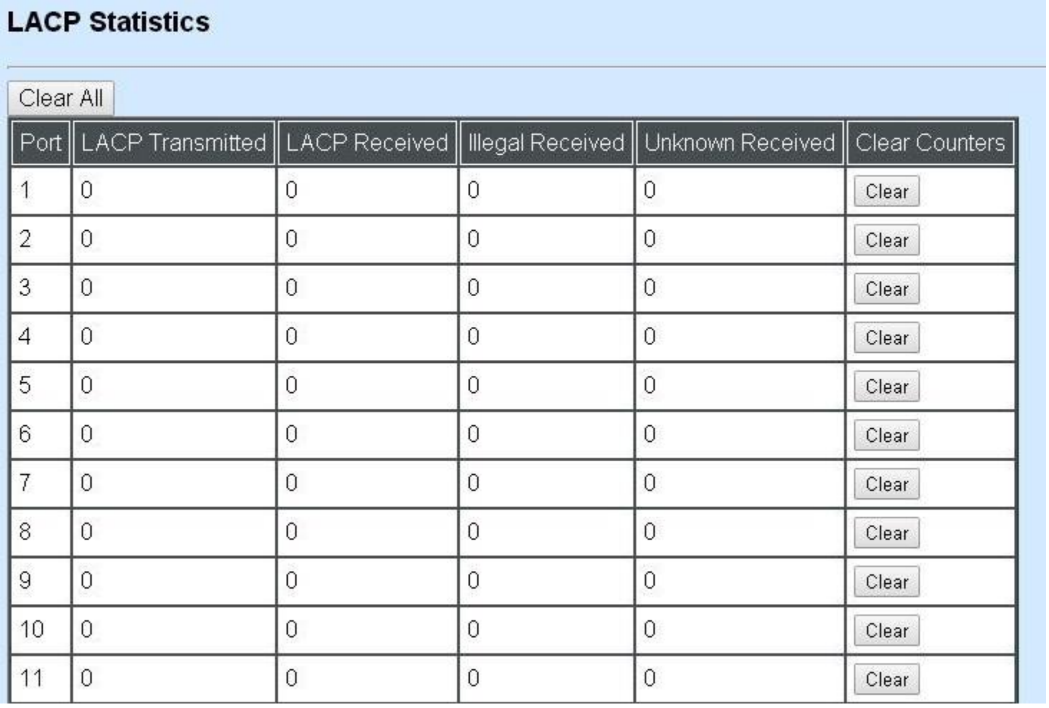
In LACP mode, link aggregation control protocol data unit (LACPDU) is used for exchanging information among LACP-enabled devices. After LACP is enabled on a port, the port sends LACPDUs to notify the remote system of its system LACP priority, system MAC address, port LACP priority, port number and operational key. Upon receipt of an LACPDU, the remote system compares the received information with the information received on other ports to determine the ports that can operate as selected ports. This allows the two systems to reach an agreement on the states of the related ports when aggregating ports, link aggregation control automatically assigns each port an operational key based on its rate, duplex mode and other basic configurations. In an LACP aggregation group, all ports share the same operational key; in a manual or static LACP aggregation, the selected ports share the same operational key.

Partner ID: The ID (MAC address) of the partner port

Partner Port: The corresponding port numbers that connect to the partner switch in LACP mode.

7.5.3.2 LACP Statistics

In order to view the real-time LACP statistics status of the Managed Switch, select **LACP Statistics** from the **LACP Monitor** menu and then the following screen page appears.



LACP Statistics

Clear All

Port	LACP Transmitted	LACP Received	Illegal Received	Unknown Received	Clear Counters
1	0	0	0	0	Clear
2	0	0	0	0	Clear
3	0	0	0	0	Clear
4	0	0	0	0	Clear
5	0	0	0	0	Clear
6	0	0	0	0	Clear
7	0	0	0	0	Clear
8	0	0	0	0	Clear
9	0	0	0	0	Clear
10	0	0	0	0	Clear
11	0	0	0	0	Clear

Port: LACP packets (LACPDU) transmitted or received from current port.

LACP Transmitted: Packets transmitted from current port.

LACP Received: Packets received form current port.

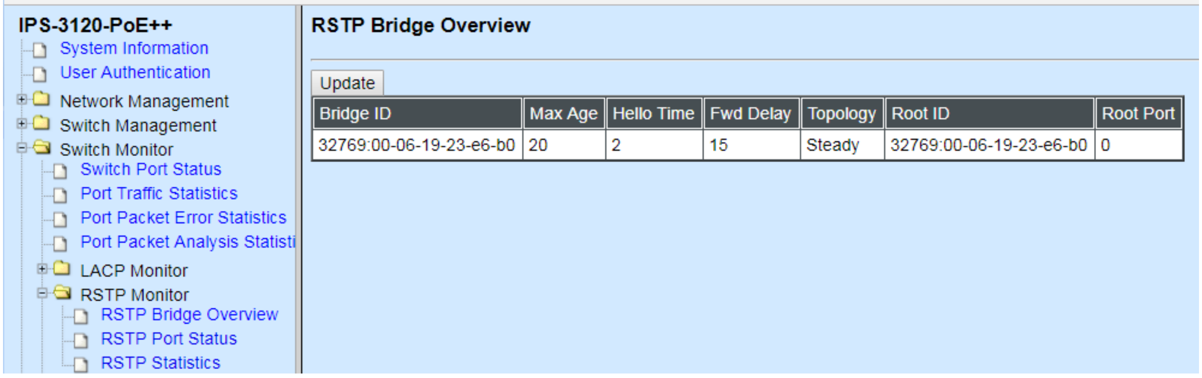
Illegal Received: Illegal packets received from current port.

Unknown Received: Unknown packets received from current port.

Clear Counter: Clear the statistics of the current port.

7.5.4 RSTP Monitor

Click the **RSTP Monitor** folder and then three options appear.

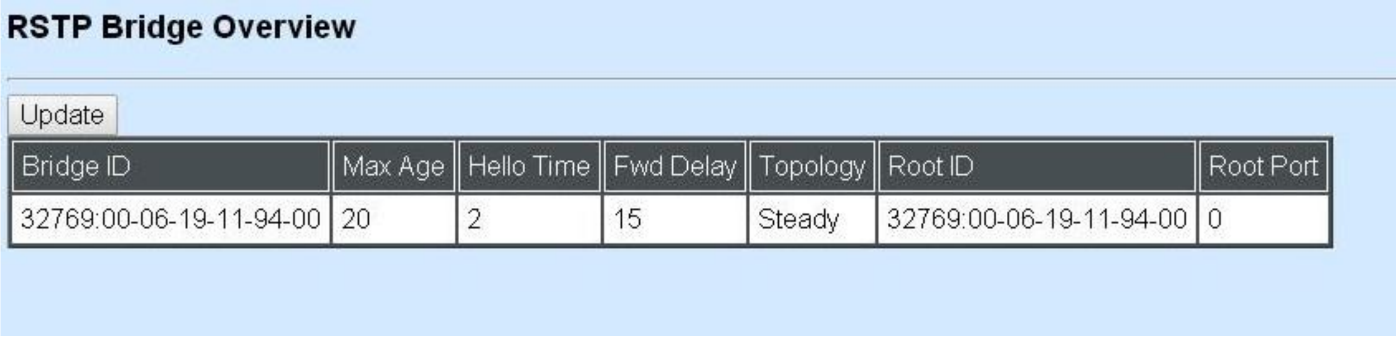


RSTP Bridge Overview

Bridge ID	Max Age	Hello Time	Fwd Delay	Topology	Root ID	Root Port
32769:00-06-19-23-e6-b0	20	2	15	Steady	32769:00-06-19-23-e6-b0	0

7.5.4.1 RSTP Bridge Overview

RSTP Bridge Overview allows users to view a list of all RSTP VLANs' brief information, such as Bridge ID, topology status and Root ID. Select **RSTP Bridge Overview** from the **RSTP Monitor** menu and then the following screen page appears.



RSTP Bridge Overview

Bridge ID	Max Age	Hello Time	Fwd Delay	Topology	Root ID	Root Port
32769:00-06-19-11-94-00	20	2	15	Steady	32769:00-06-19-11-94-00	0

In this page, you can find the following information about RSTP bridge:

Update: Update the current status.

Bridge ID: RSTP Bridge ID of the Managed Switch

Max Age: Max Age setting of the Managed Switch.

Hello Time: Hello Time setting of the Managed Switch.

Forward Delay: The Managed Switch's setting of Forward Delay Time.

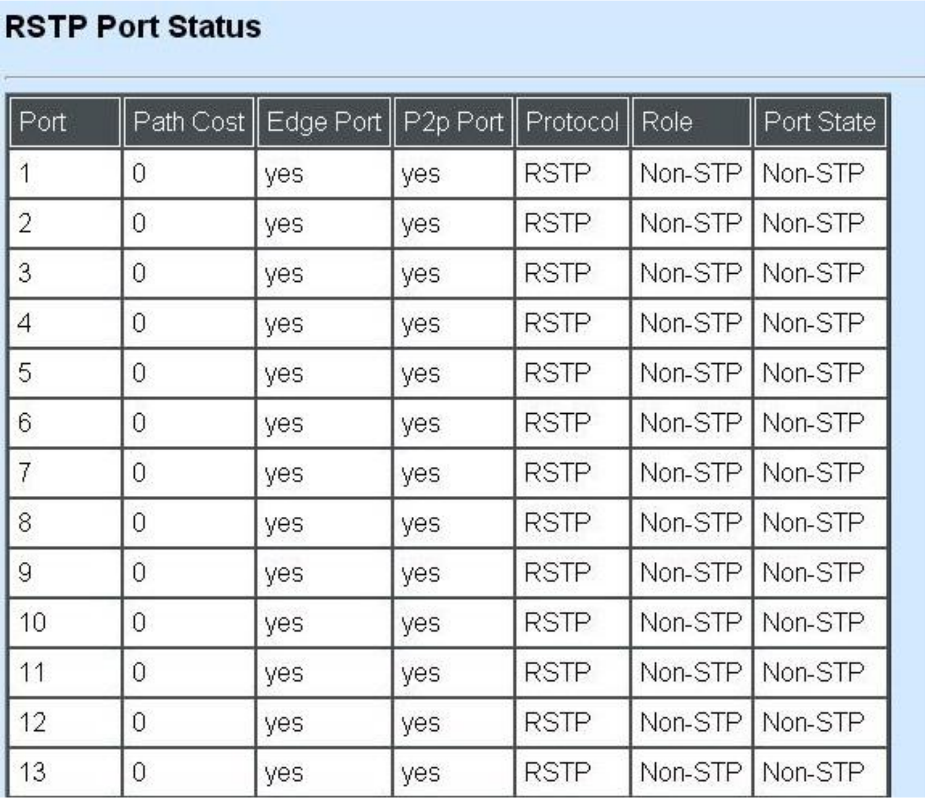
Topology: The state of the topology.

Root ID: Display this Managed Switch's Root ID.

Root port: Display this Managed Switch's Root Port Number.

7.5.4.2 RSTP Port Status

RSTP Port Status allows users to view a list of all RSTP ports' information. Select **RSTP Port Status** from the **RSTP Monitor** menu and then the following screen page appears.



RSTP Port Status

Port	Path Cost	Edge Port	P2p Port	Protocol	Role	Port State
1	0	yes	yes	RSTP	Non-STP	Non-STP
2	0	yes	yes	RSTP	Non-STP	Non-STP
3	0	yes	yes	RSTP	Non-STP	Non-STP
4	0	yes	yes	RSTP	Non-STP	Non-STP
5	0	yes	yes	RSTP	Non-STP	Non-STP
6	0	yes	yes	RSTP	Non-STP	Non-STP
7	0	yes	yes	RSTP	Non-STP	Non-STP
8	0	yes	yes	RSTP	Non-STP	Non-STP
9	0	yes	yes	RSTP	Non-STP	Non-STP
10	0	yes	yes	RSTP	Non-STP	Non-STP
11	0	yes	yes	RSTP	Non-STP	Non-STP
12	0	yes	yes	RSTP	Non-STP	Non-STP
13	0	yes	yes	RSTP	Non-STP	Non-STP

In this page, you can find the following information about RSTP status:

Port Number: The number of the port.

Path Cost: The Path Cost of the port.

Edge Port: "Yes" is displayed if the port is the Edge port connecting to an end station and does not receive BPDU.

P2p Port: "Yes" is displayed if the port link is connected to another STP device.

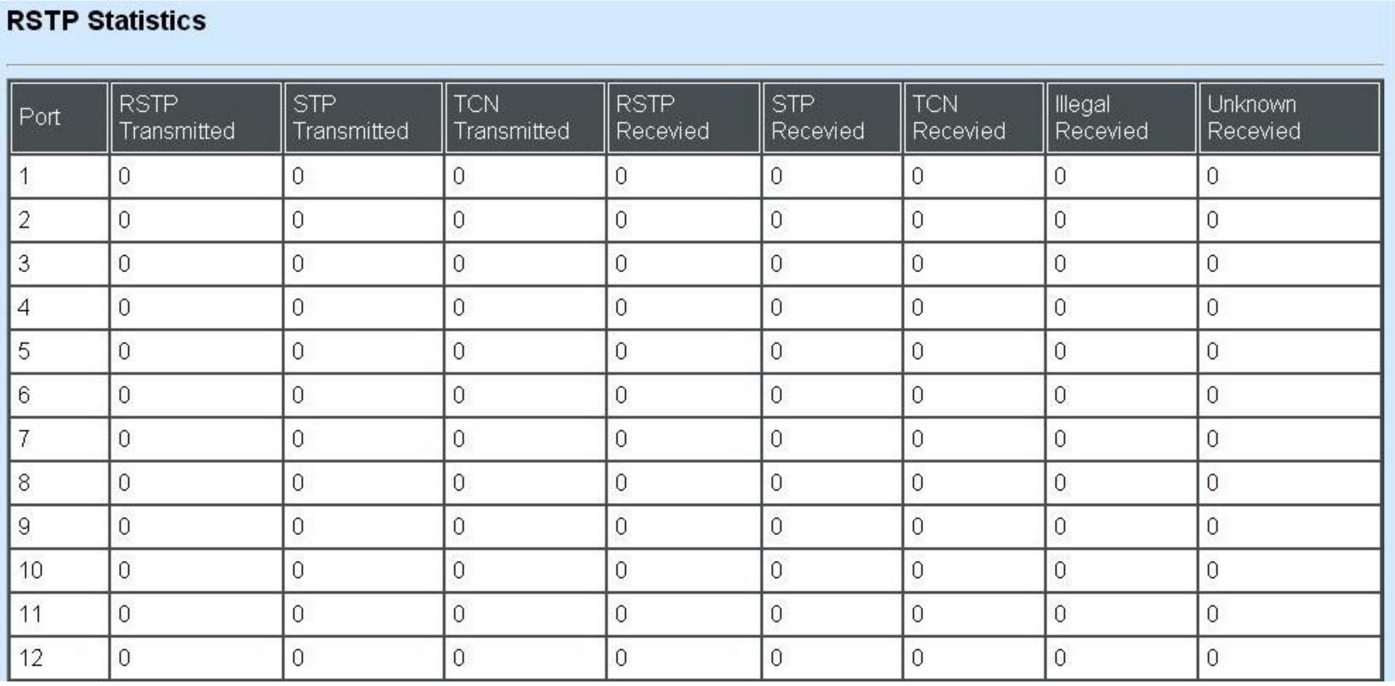
Protocol: Display RSTP or STP.

Role: Display the Role of the port (non-STP, forwarding or blocked).

Port State: Display the state of the port (non-STP, forwarding or blocked).

7.5.4.3 RSTP Statistics

In order to view the real-time RSTP statistics status of the Managed Switch, select **RSTP Statistics** from the **RSTP Monitor** menu and then the following screen page appears.



RSTP Statistics

Port	RSTP Transmitted	STP Transmitted	TCN Transmitted	RSTP Recevied	STP Recevied	TCN Recevied	Illegal Recevied	Unknown Recevied
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0

Port Number: The number of the port.

RSTP Transmitted: The total transmitted RSTP packets from current port.

STP Transmitted: The total transmitted STP packets from current port.

TCN Transmitted: The total transmitted TCN (Topology Change Notification) packets from current port.

RSTP Received: The total received RSTP packets from current port.

STP Received: The total received STP packets from current port.

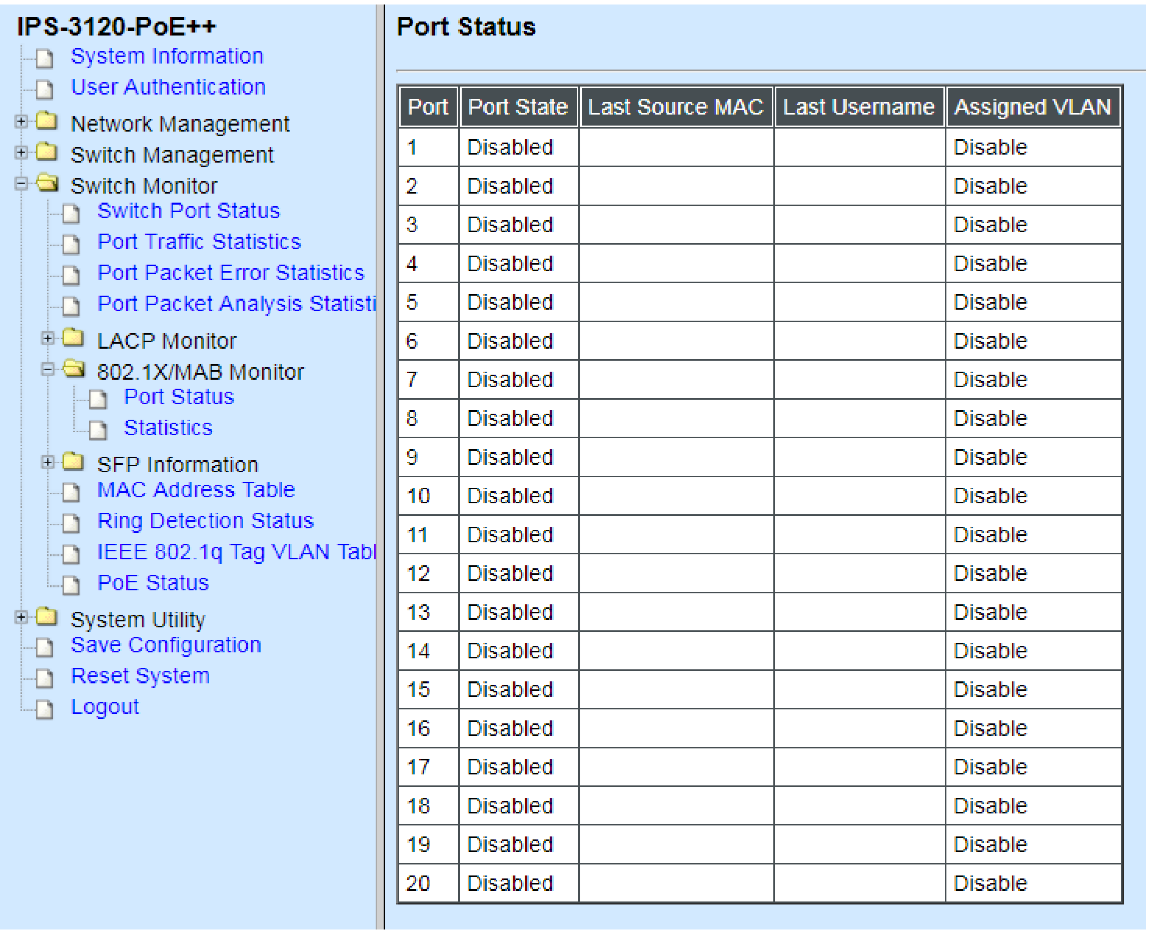
TCN Received: The total received TCN packets from current port.

Illegal Received: The total received illegal packets from current port.

Unknown Received: The total received unknown packets from current port.

7.5.5 802.1X/MAB Monitor

Click the **802.1X/MAB Monitor** folder and then two options appear.

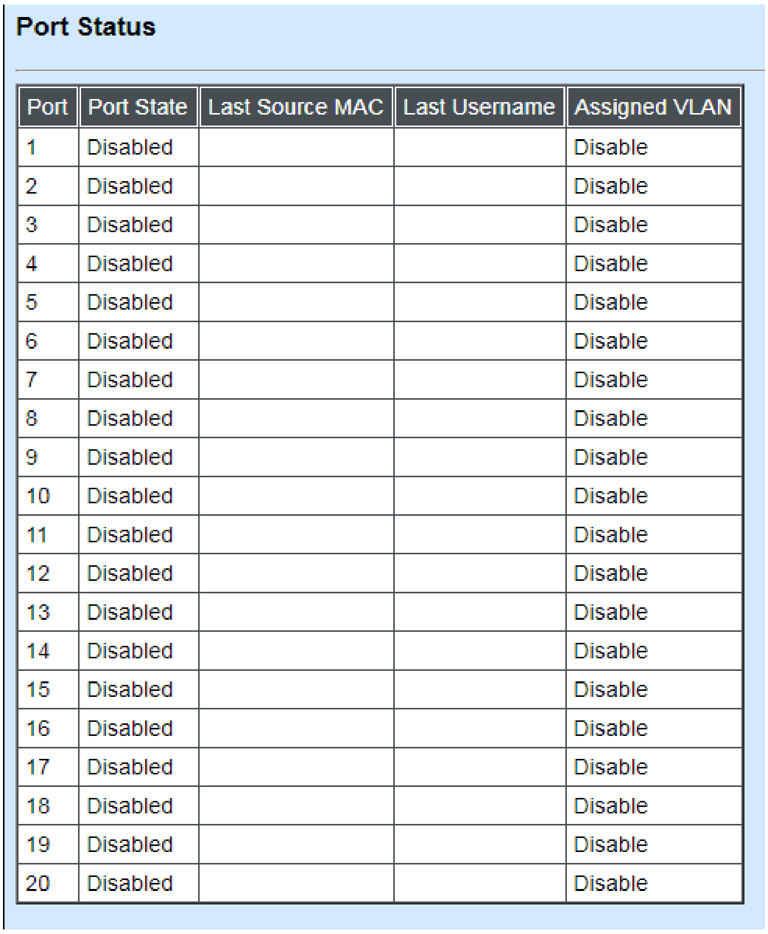


Port Status

Port	Port State	Last Source MAC	Last Username	Assigned VLAN
1	Disabled			Disable
2	Disabled			Disable
3	Disabled			Disable
4	Disabled			Disable
5	Disabled			Disable
6	Disabled			Disable
7	Disabled			Disable
8	Disabled			Disable
9	Disabled			Disable
10	Disabled			Disable
11	Disabled			Disable
12	Disabled			Disable
13	Disabled			Disable
14	Disabled			Disable
15	Disabled			Disable
16	Disabled			Disable
17	Disabled			Disable
18	Disabled			Disable
19	Disabled			Disable
20	Disabled			Disable

7.5.5.1 Port Status

802.1X Port Status allows users to view a list of all 802.1x ports' information. Select **port status** from the **802.1X/MAB Monitor** menu and then the following screen page appears.



Port Status

Port	Port State	Last Source MAC	Last Username	Assigned VLAN
1	Disabled			Disable
2	Disabled			Disable
3	Disabled			Disable
4	Disabled			Disable
5	Disabled			Disable
6	Disabled			Disable
7	Disabled			Disable
8	Disabled			Disable
9	Disabled			Disable
10	Disabled			Disable
11	Disabled			Disable
12	Disabled			Disable
13	Disabled			Disable
14	Disabled			Disable
15	Disabled			Disable
16	Disabled			Disable
17	Disabled			Disable
18	Disabled			Disable
19	Disabled			Disable
20	Disabled			Disable

In this page, you can find the following information about 802.1X ports:

Port: The number of the port.

State: Display the number of the port 802.1x link state LinkDown or LinkUp.

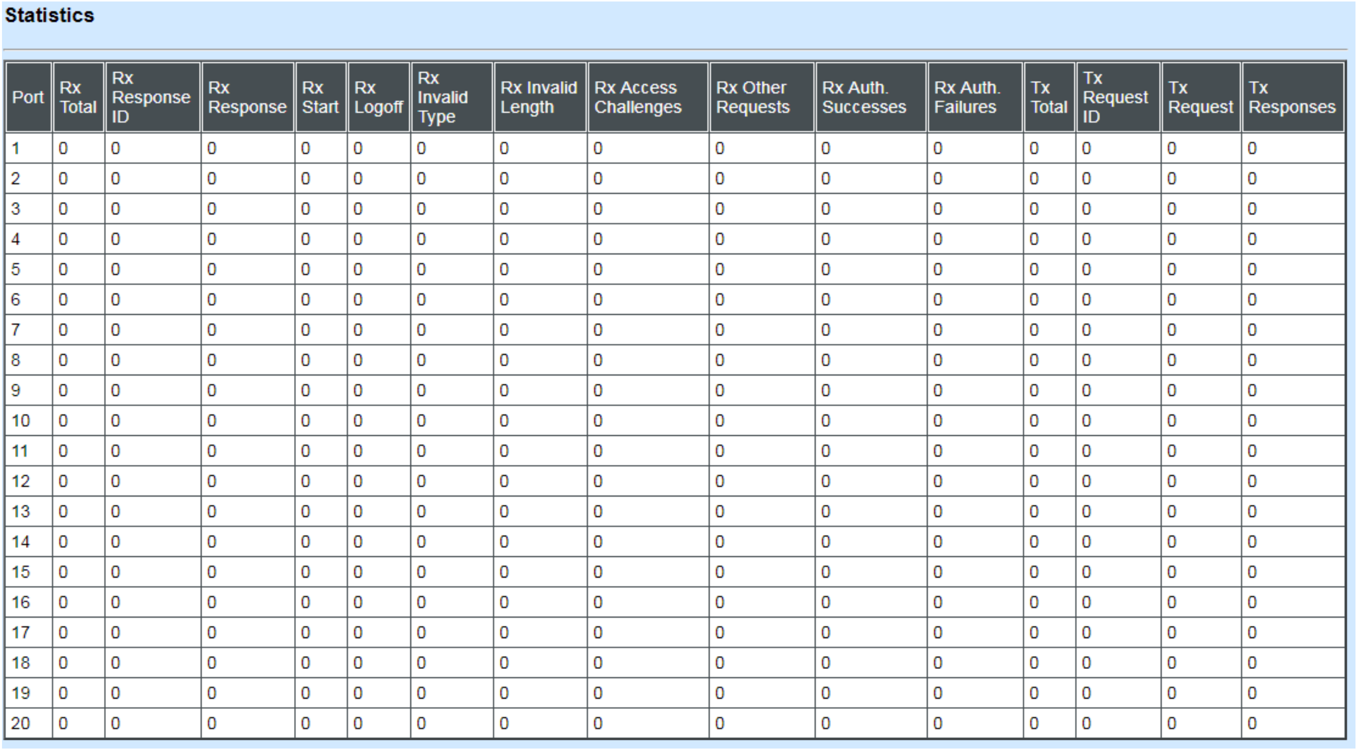
Last Source: Display the number of the port’s Last Source.

Last ID: Display the number of the port’s Last ID.

Assigned VLAN: Display the value of the port’s Assigned VLAN.

7.5.5.2 Statistics

In order to view the real-time 802.1X port statistics status of the Managed Switch, select **Statistics** from the **802.1x Monitor** menu and then the following screen page shows up.

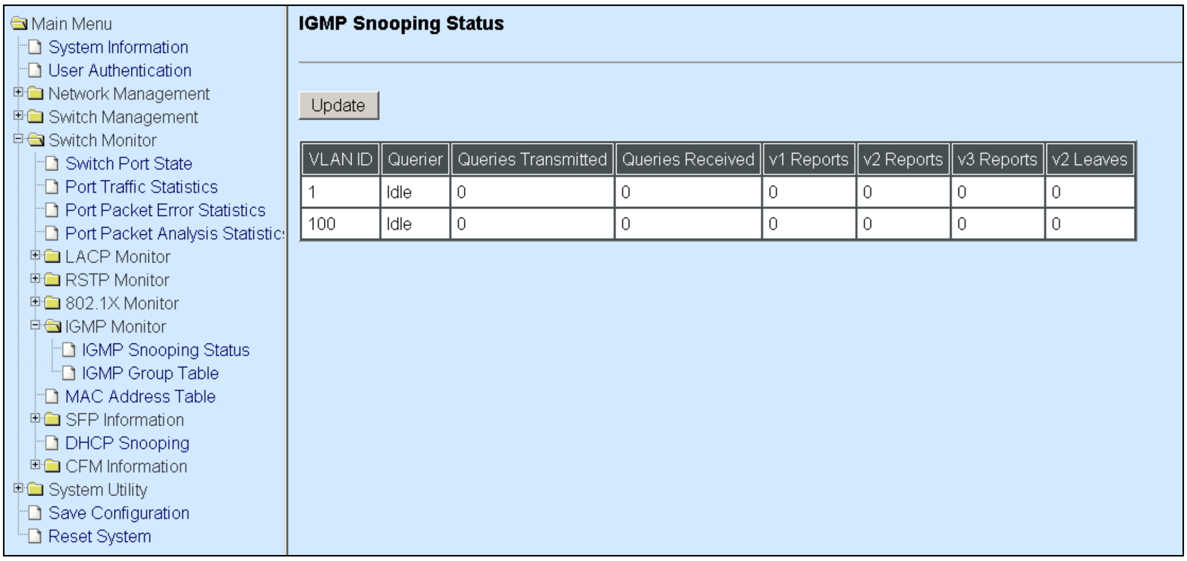


Statistics

Port	Rx Total	Rx Response ID	Rx Response	Rx Start	Rx Logoff	Rx Invalid Type	Rx Invalid Length	Rx Access Challenges	Rx Other Requests	Rx Auth. Successes	Rx Auth. Failures	Tx Total	Tx Request ID	Tx Request	Tx Responses
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

7.5.6 IGMP/MLD Monitor

Click the **IGMP/MLD Monitor** folder and then the following screen page appears.

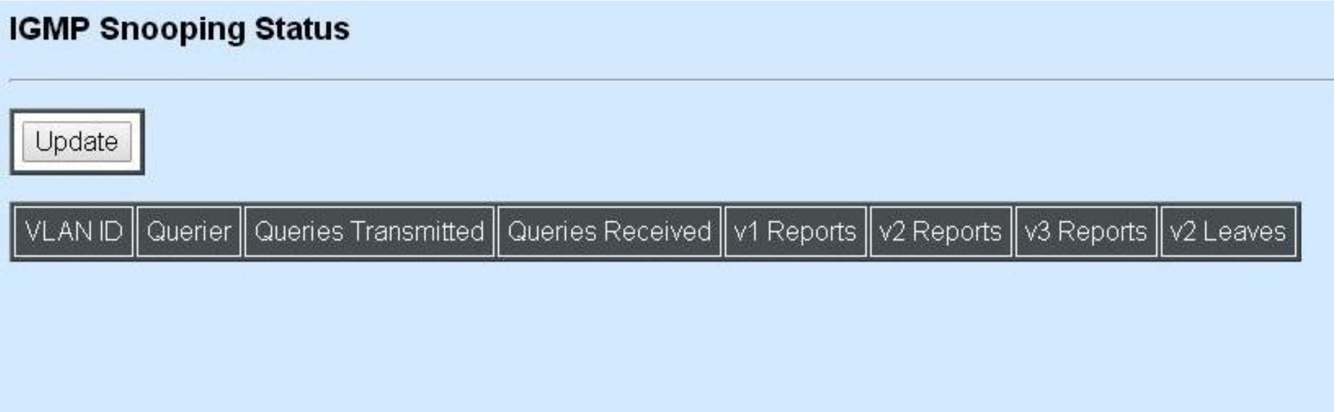


IGMP Snooping Status

VLAN ID	Querier	Queries Transmitted	Queries Received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
1	Idle	0	0	0	0	0	0
100	Idle	0	0	0	0	0	0

7.5.6.1 IGMP Snooping Status

IGMP Snooping Status allows users to view a list of IGMP queries' information in VLAN(s) such as VLAN ID, Querier and Queries Transmitted/Received packets. Select **IGMP Snooping Status** from the **IGMP Monitor** menu and then the following screen page appears.



IGMP Snooping Status

VLAN ID	Querier	Queries Transmitted	Queries Received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves

Update: Click “Update” to update the table.

VLAN ID: VID of the specific VLAN

The IGMP querier periodically sends IGMP general queries to all hosts and routers (224.0.0.1) on the local subnet to find out whether active multicast group members exist on the subnet.

Upon receiving an IGMP general query, the Managed Switch forwards it through all ports in the VLAN except the receiving port.

Querier: The state of IGMP querier in the VLAN.

Queries Transmitted: The total IGMP general queries transmitted will be sent to IGMP hosts.

Queries Received: The total received IGMP general queries from IGMP querier.

v1 Reports: IGMP Version 1 reports.

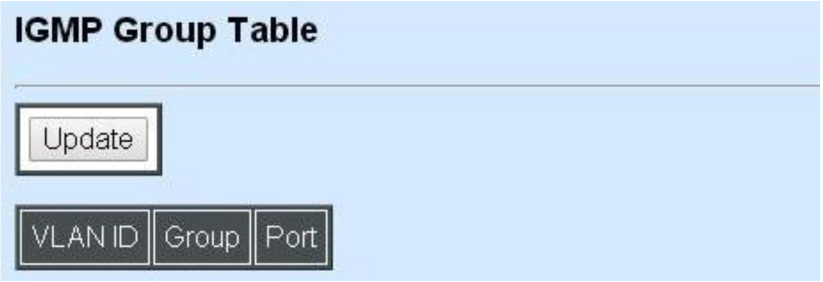
v2 Reports: IGMP Version 2 reports.

v3 Reports: IGMP Version 3 reports.

v2 Leaves: IGMP Version 2 leaves.

7.5.6.2 IGMP Group Table

In order to view the real-time IGMP multicast group status of the Managed Switch, select **IGMP Group Table** from the **IGMP monitor** menu and then the following screen page appears.



IGMP Group Table

VLAN ID	Group	Port

Update: Click “Update” to update the table.

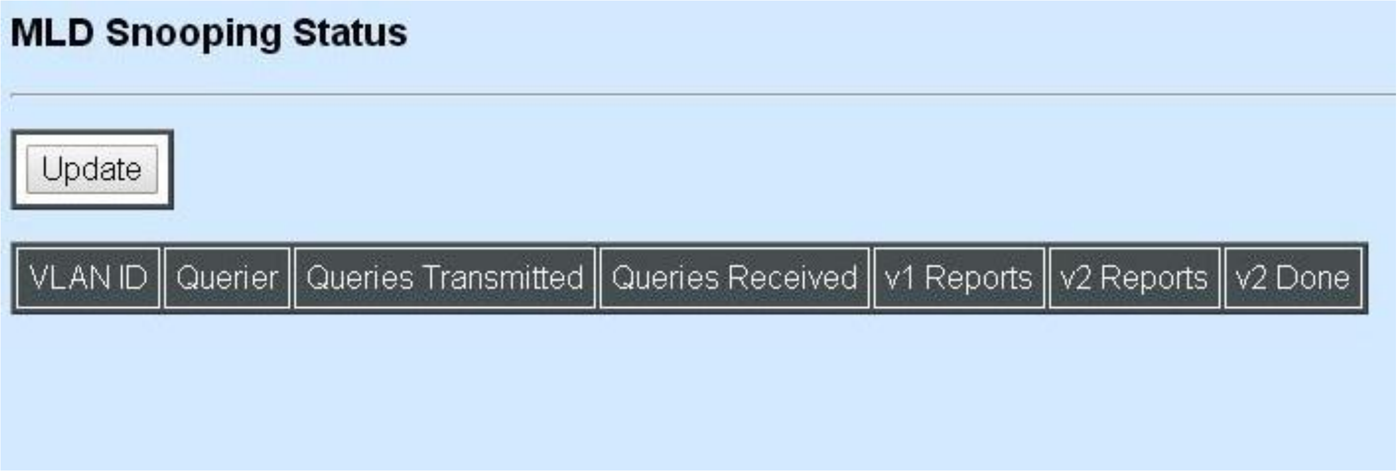
VLAN ID: VID of the specific VLAN

Group: The multicast IP address of IGMP querier.

Port: The port(s) grouped in the specific multicast group.

7.5.6.3 MLD Snooping Status

MLD Snooping Status allows users to view a list of IGMP queries’ information in VLAN(s) such as VLAN ID, Querier and Queries Transmitted/Received packets. Select **MLD Snooping Status** from the **IGMP/MLD Monitor** menu and then the following screen page appears.



MLD Snooping Status

VLAN ID	Querier	Queries Transmitted	Queries Received	v1 Reports	v2 Reports	v2 Done

Update: Click “Update” to update the table.

VLAN ID: VID of the specific VLAN

Queries Transmitted: The total IGMP general queries transmitted will be sent to IGMP hosts.

Queries Received: The total received IGMP general queries from IGMP querier.

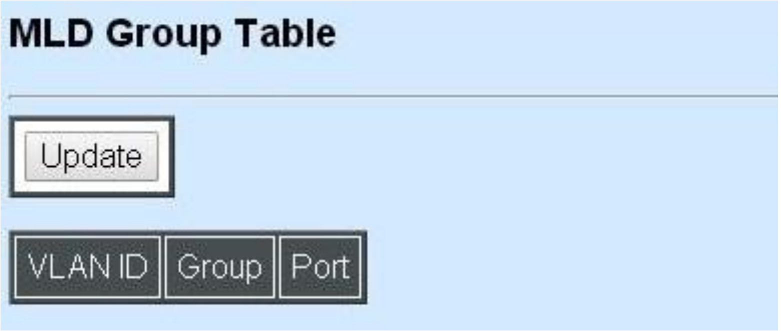
v1 Reports: IGMP Version 1 reports.

v2 Reports: IGMP Version 2 reports.

v2 Done: IGMP Version 2 dones

7.5.6.4 MLD Group Table

In order to view the real-time IGMP multicast group status of the Managed Switch, select **MLD Group Table** from the **IGMP/MLD monitor** menu and then the following screen page appears.



MLD Group Table

Update

VLAN ID	Group	Port

Update: Click “Update” to update the table.

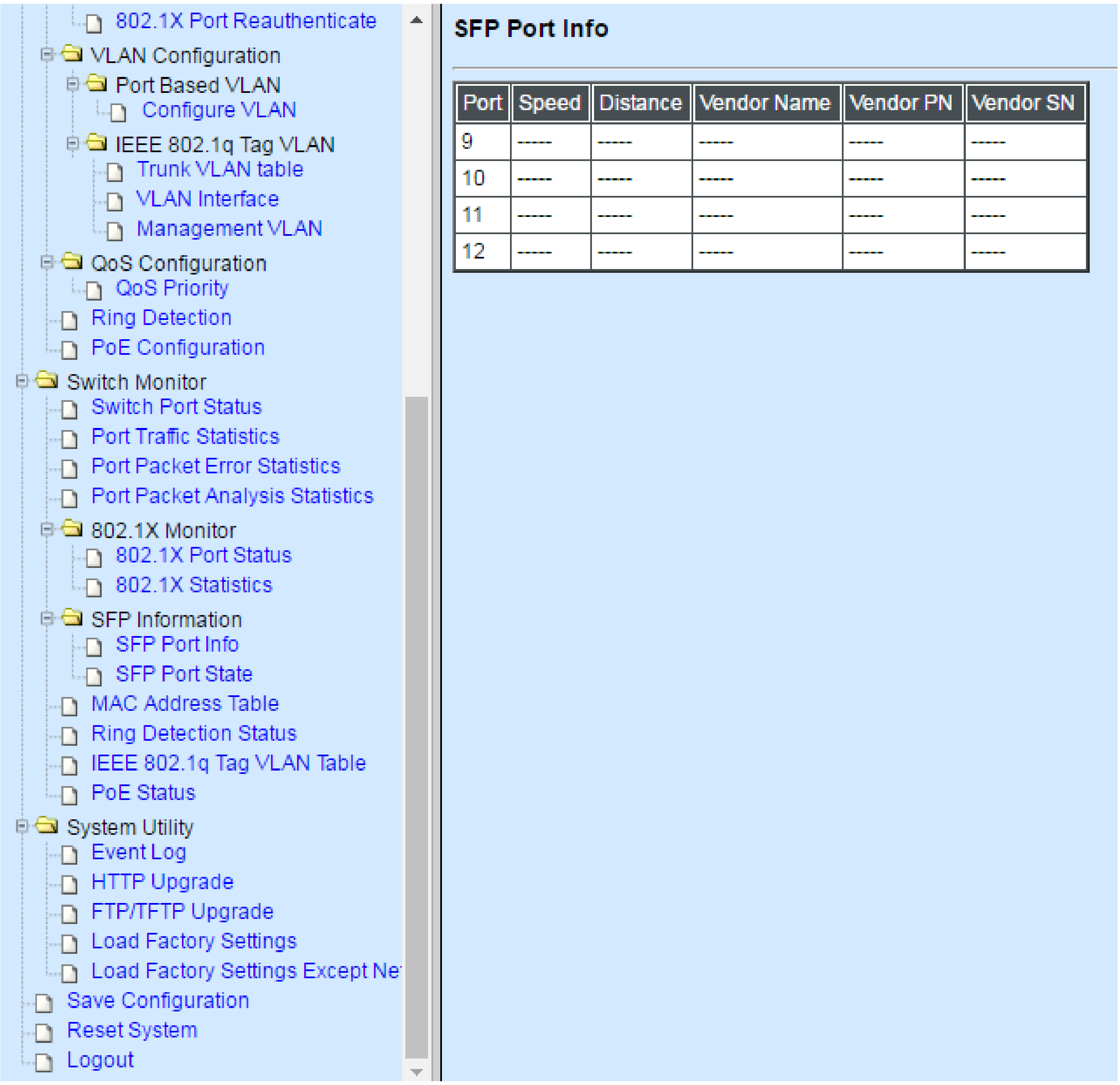
VLAN ID: VID of the specific VLAN

Group: The multicast IP address of IGMP querier.

Port: The port(s) grouped in the specific multicast group.

7.5.7 SFP Information

Click **SFP Information** folder from **Switch Monitor** menu and then two options appear.



SFP Port Info

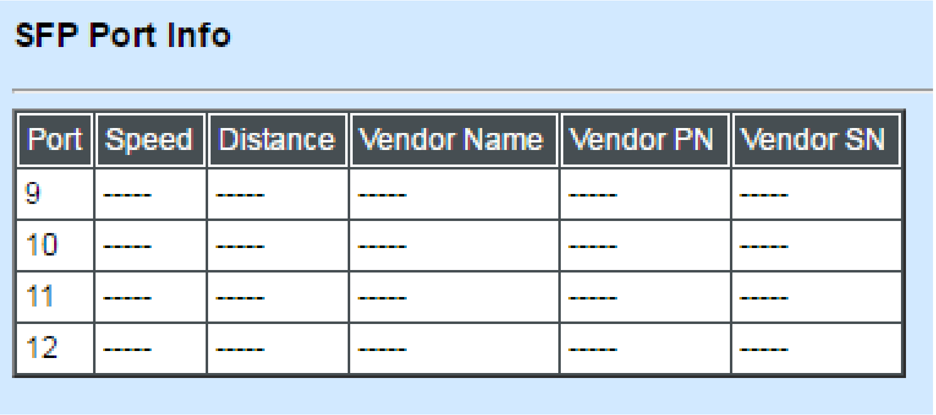
Port	Speed	Distance	Vendor Name	Vendor PN	Vendor SN
9	------	------	------	------	------
10	------	------	------	------	------
11	------	------	------	------	------
12	------	------	------	------	------

SFP Port Info: It shows the information of Speed, Distance, Vendor Name, Vendor PN, and Vendor SN of the SFP Port.

SFP Port State: It shows the state of Temperature, Voltage, TX Bias, TX Power, and RX Power of the SFP Port.

7.5.7.1 SFP Port Info

The following screen page appears if you choose **SFP Information** and then select **SFP Port Info**.


SFP Port Info

Port	Speed	Distance	Vendor Name	Vendor PN	Vendor SN
9	------	------	------	------	------
10	------	------	------	------	------
11	------	------	------	------	------
12	------	------	------	------	------

Port: The port number of the slide-in SFP module.

Speed: The transmitting speed of the slide-in SFP module.

Distance: The transmitting distance of the slide-in SFP module.

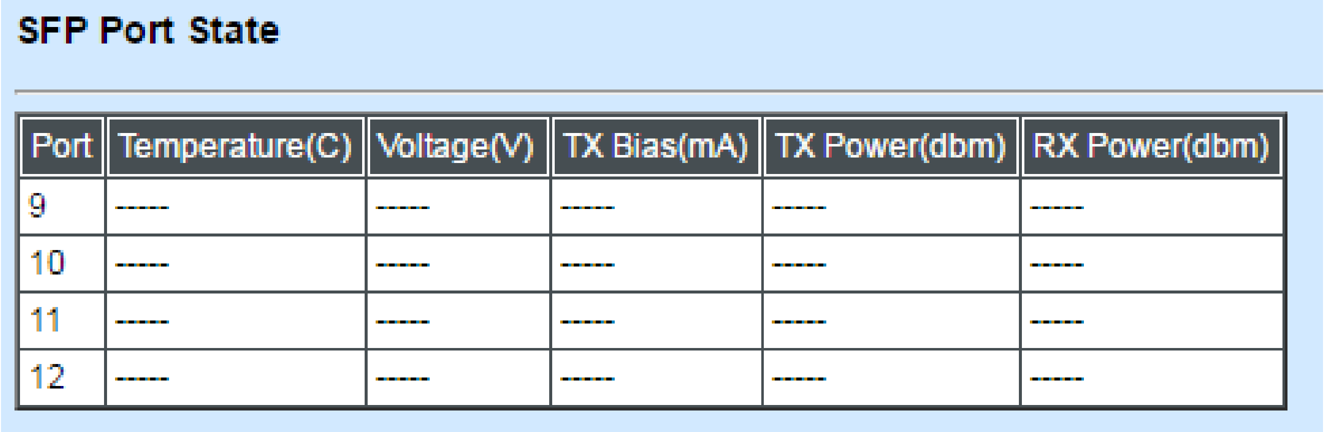
Vendor Name: The vendor name of the slide-in SFP module.

Vendor PN: The vendor part number of the slide-in SFP module.

Vendor SN: The vendor serial number of the slide-in SFP module.

7.5.7.2 SFP Port State

The following screen page appears if you choose **SFP Information** and then select **SFP Port State**.


SFP Port State

Port	Temperature(C)	Voltage(V)	TX Bias(mA)	TX Power(dbm)	RX Power(dbm)
9	------	------	------	------	------
10	------	------	------	------	------
11	------	------	------	------	------
12	------	------	------	------	------

Port: The port number of the slide-in SFP module.

Temperature (C): The operation temperature of the slide-in SFP module.

Voltage (V): The operation voltage of the slide-in SFP module.

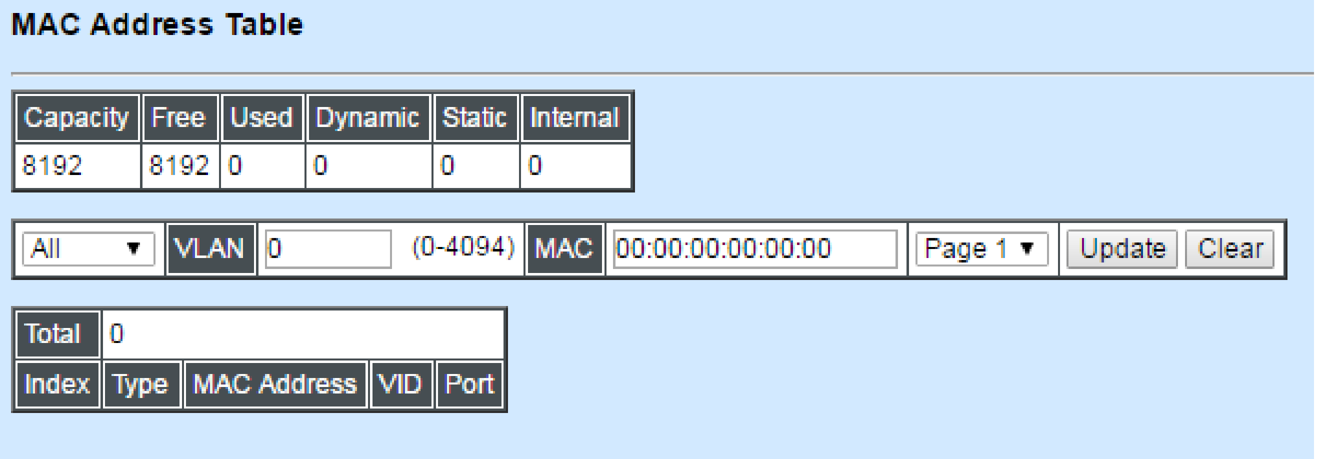
TX Bias (mA): The operation current of the slide-in SFP module.

TX Power (dbm): The optical transmission power of the slide-in SFP module.

RX Power (dbm): The optical receiver power of the slide-in SFP module.

7.5.8 MAC Address Table

MAC Address Table displays MAC addresses learned after the system reset.



MAC Address Table

Capacity	Free	Used	Dynamic	Static	Internal
8192	8192	0	0	0	0

All ▼ VLAN 0 (0-4094) MAC 00:00:00:00:00:00 Page 1 ▼

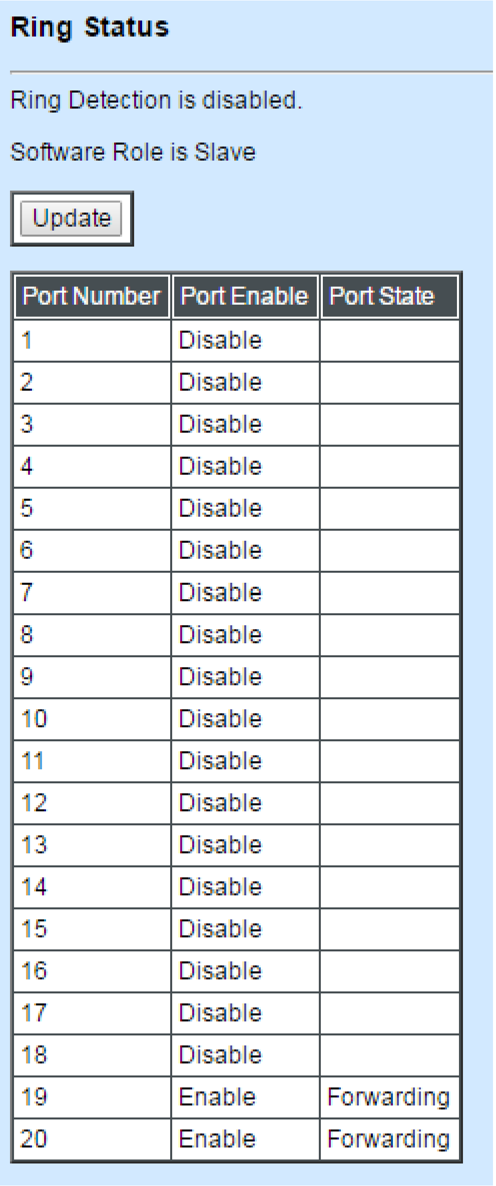
Total	0			
Index	Type	MAC Address	VID	Port

The table above shows the MAC addresses learned from each port of the Managed Industrial PoE Switch.

Click **Top** to show the first page (the first twenty entries) of the MAC Address Table.

Click **Next** to show the next page of the MAC Address Table.

7.5.9 Ring Detection Status



Ring Detection is disabled.

Software Role is Slave

Port Number	Port Enable	Port State
1	Disable	
2	Disable	
3	Disable	
4	Disable	
5	Disable	
6	Disable	
7	Disable	
8	Disable	
9	Disable	
10	Disable	
11	Disable	
12	Disable	
13	Disable	
14	Disable	
15	Disable	
16	Disable	
17	Disable	
18	Disable	
19	Enable	Forwarding
20	Enable	Forwarding

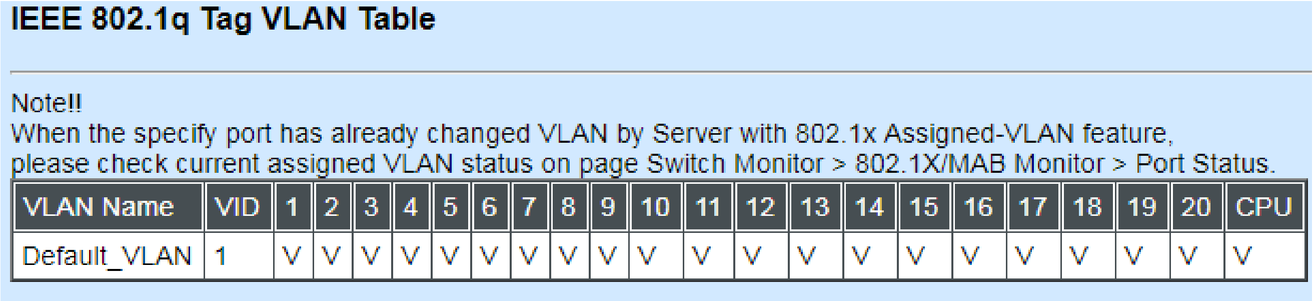
Port Enable: The status of whether Ring Detection on ports is enabled or disabled.

Port State: The status of whether the port is blocking or forwarding.

Blocking: It indicates a port is temporarily blocked and stop sending packet until link down occurs.
Forwarding: It indicates a port keeps sending packets.

7.5.10 IEEE 802.1q Tag VLAN Table

Select **IEEE 802.1q Tag VLAN Table** from the **Switch Monitor** menu and then the following screen page appears.



IEEE 802.1q Tag VLAN Table

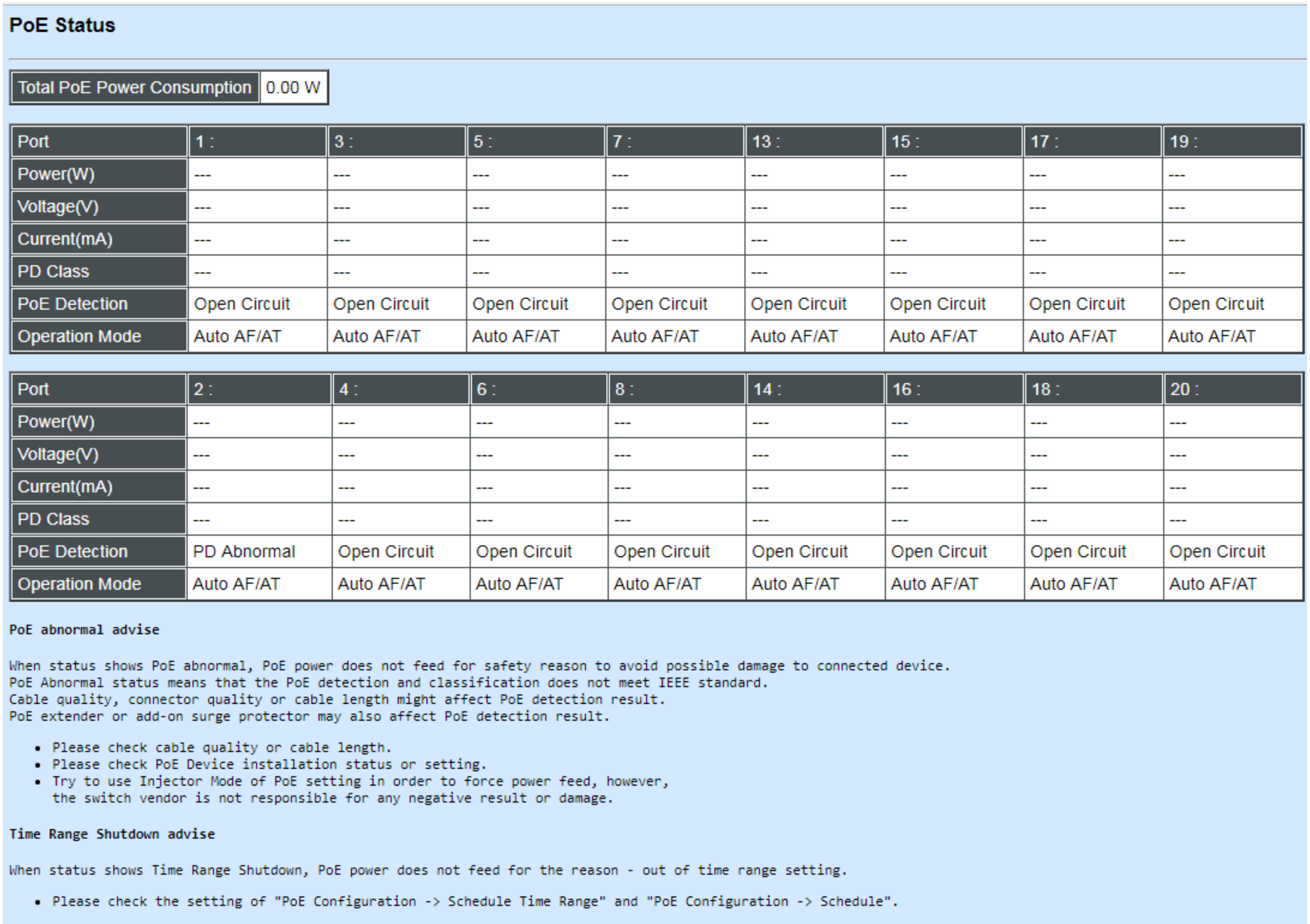
Note!!
When the specify port has already changed VLAN by Server with 802.1x Assigned-VLAN feature,
please check current assigned VLAN status on page Switch Monitor > 802.1X/MAB Monitor > Port Status.

VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	CPU
Default_VLAN	1	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V

VLAN Name: View-only filed that shows the VLAN group name.

VID: View-only filed that shows the VID.

7.5.11 PoE Status



PoE Status

Total PoE Power Consumption	0.00 W

Port	1 :	3 :	5 :	7 :	13 :	15 :	17 :	19 :
Power(W)	---	---	---	---	---	---	---	---
Voltage(V)	---	---	---	---	---	---	---	---
Current(mA)	---	---	---	---	---	---	---	---
PD Class	---	---	---	---	---	---	---	---
PoE Detection	Open Circuit	Open Circuit	Open Circuit	Open Circuit	Open Circuit	Open Circuit	Open Circuit	Open Circuit
Operation Mode	Auto AF/AT	Auto AF/AT	Auto AF/AT	Auto AF/AT	Auto AF/AT	Auto AF/AT	Auto AF/AT	Auto AF/AT

Port	2 :	4 :	6 :	8 :	14 :	16 :	18 :	20 :
Power(W)	---	---	---	---	---	---	---	---
Voltage(V)	---	---	---	---	---	---	---	---
Current(mA)	---	---	---	---	---	---	---	---
PD Class	---	---	---	---	---	---	---	---
PoE Detection	PD Abnormal	Open Circuit	Open Circuit	Open Circuit	Open Circuit	Open Circuit	Open Circuit	Open Circuit
Operation Mode	Auto AF/AT	Auto AF/AT	Auto AF/AT	Auto AF/AT	Auto AF/AT	Auto AF/AT	Auto AF/AT	Auto AF/AT

PoE abnormal advise

When status shows PoE abnormal, PoE power does not feed for safety reason to avoid possible damage to connected device.
PoE Abnormal status means that the PoE detection and classification does not meet IEEE standard.
Cable quality, connector quality or cable length might affect PoE detection result.
PoE extender or add-on surge protector may also affect PoE detection result.

- Please check cable quality or cable length.
- Please check PoE Device installation status or setting.
- Try to use Injector Mode of PoE setting in order to force power feed, however, the switch vendor is not responsible for any negative result or damage.

Time Range Shutdown advise

When status shows Time Range Shutdown, PoE power does not feed for the reason - out of time range setting.

- Please check the setting of "PoE Configuration -> Schedule Time Range" and "PoE Configuration -> Schedule".

Total PoE Power Consumption: Shows current total power used in watt and in percentage on the switch.

Port: The number of each port.

Power (W): Current power in watt used on a port.

Voltage (V): Current voltage used on a port.

Current (mA): Current used in milliampere on a port at present.

PD Class: Shows the current connected Powered Device Class.

PoE Detection: Shows the current status of PoE operation. A list of detection definition is shown below.

PoE Detection	Definition
Good	The PD is in good PoE operation.
Open Circuit	The PD is disconnected with the switch.
PD Abnormal	The PD has some technical difficulties with the switch. Please refer to the notification below.

Note:
PoE abnormal advise
When status shows PoE abnormal, PoE power does not feed for safety reason to avoid possible damage to connected device.
PoE Abnormal status means that the PoE detection and classification does not meet IEEE standard.
Cable quality, connector quality or cable length might affect PoE detection result.
PoE extender or add-on surge protector may also affect PoE detection result.

- Please check cable quality or cable length.
- Please check PoE Device installation status or setting.
- Try to use Injector Mode of PoE setting in order to force power feed, however, the switch vendor is not responsible for any negative result or damage.

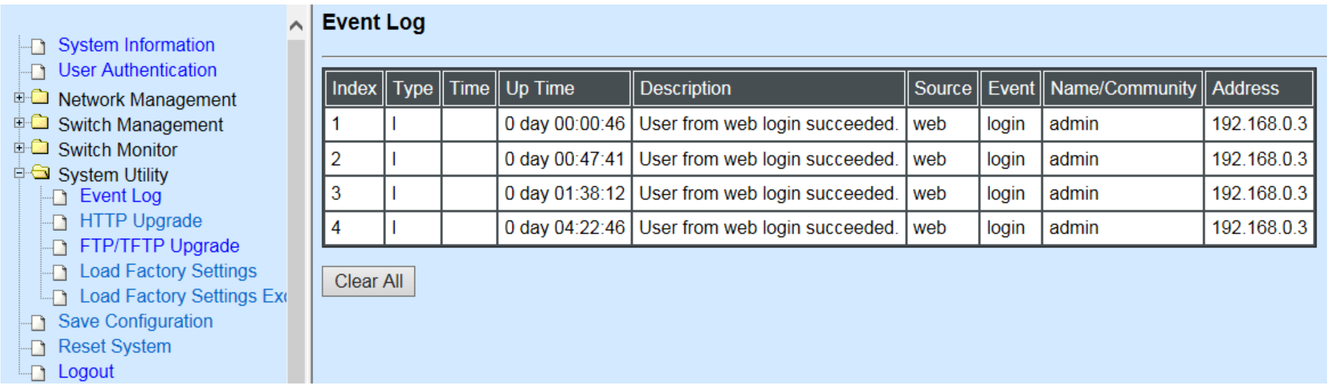
Time Range Shutdown advise
When status shows Time Range Shutdown, PoE power does not feed for the reason - out of time range setting.

- Please check the setting of “PoE Configuration -> Schedule Time Range” and “PoE Configuration -> Schedule”

Operation Mode: Shows the current operation mode used. Shutdown mode refers to disable PoE on a port permanently. Injector-30Watt mode refers to enable PoE on a port permanently. Auto AF/AT mode refers to flexibly enable PoE on a port the connected device at the other end. Under Auto AF/AT mode, it automatically detects the connected device if the device supports PoE feature. If not, it won’t give the connected device power.

7.6 System Utility

Select the folder **System Utility** from the left column and then the following screen page appears.



Event Log

Index	Type	Time	Up Time	Description	Source	Event	Name/Community	Address
1	I		0 day 00:00:46	User from web login succeeded.	web	login	admin	192.168.0.3
2	I		0 day 00:47:41	User from web login succeeded.	web	login	admin	192.168.0.3
3	I		0 day 01:38:12	User from web login succeeded.	web	login	admin	192.168.0.3
4	I		0 day 04:22:46	User from web login succeeded.	web	login	admin	192.168.0.3

1. **Event Log:** Event log can keep a record of system's log events such as system warm start, cold start, link up/down, user login/logout, etc.

2. **HTTP Upgrade:** Users may save or restore the configuration and update the firmware by HTTP.

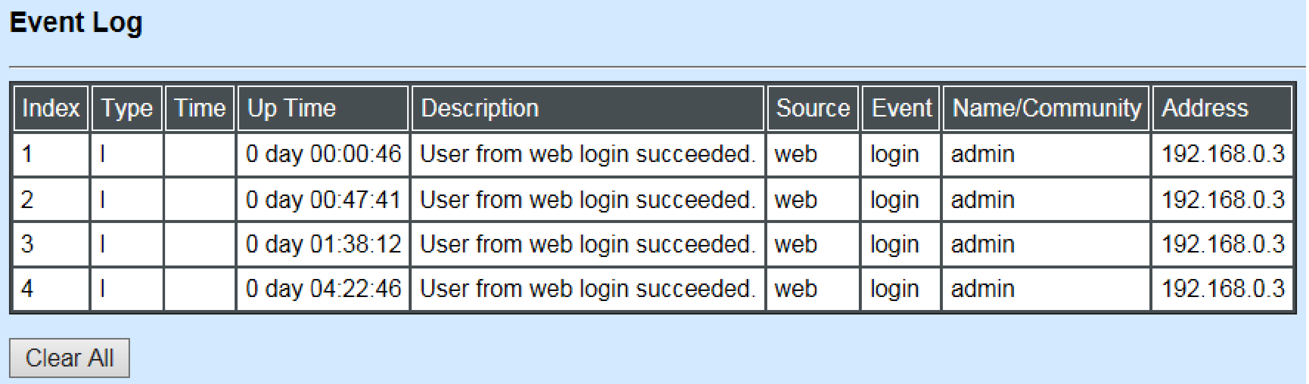
3. **FTP/TFTP Upgrade:** The Managed Industrial PoE Switch has both built-in TFTP and FTP clients. Users may save or restore the configuration and update the firmware by FTP/TFTP.

4. **Load Factory Settings:** Load Factory Setting will set the configuration of the Managed Industrial PoE Switch back to the factory default settings. The IP and Gateway addresses will be set to the factory default as well.

5. **Load Factory Settings Except Network Configuration:** Selecting this function will also restore the configuration of the Managed Industrial PoE Switch to its original factory default settings. However, this will not reset the IP and Gateway addresses to the factory default.

7.6.1 Event Log

Event Log keeps a record of user login and logout timestamp information. Select **Event Log** from the **System Utility** menu and then the following screen page appears.



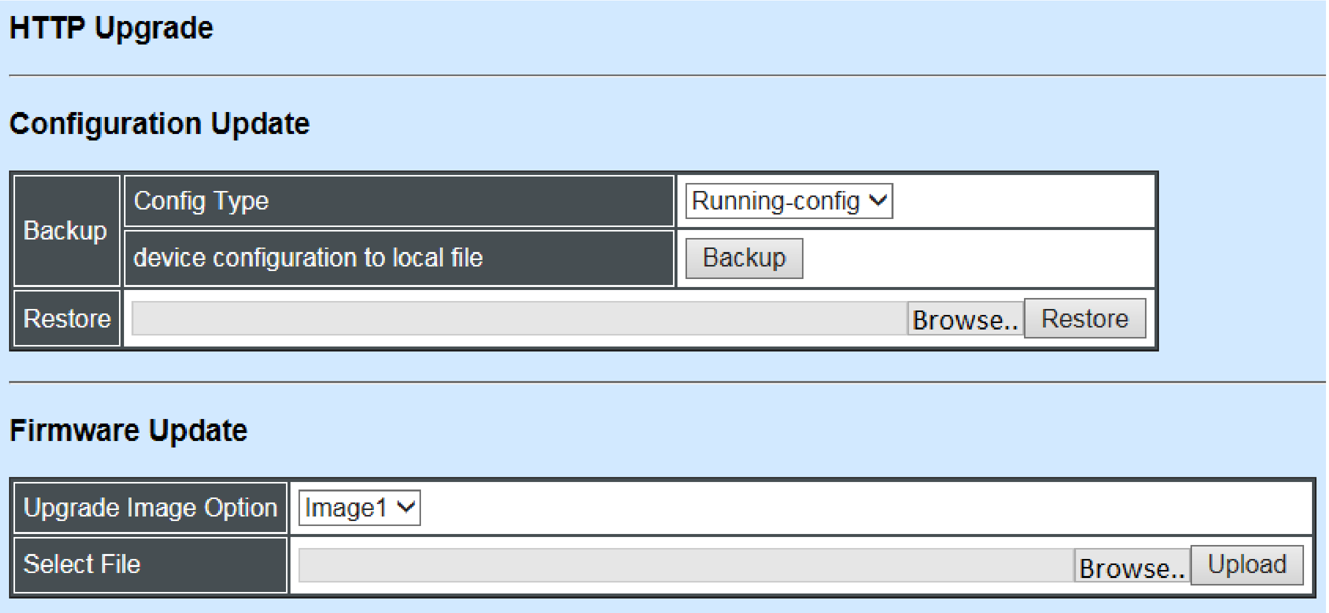
Event Log

Index	Type	Time	Up Time	Description	Source	Event	Name/Community	Address
1	I		0 day 00:00:46	User from web login succeeded.	web	login	admin	192.168.0.3
2	I		0 day 00:47:41	User from web login succeeded.	web	login	admin	192.168.0.3
3	I		0 day 01:38:12	User from web login succeeded.	web	login	admin	192.168.0.3
4	I		0 day 04:22:46	User from web login succeeded.	web	login	admin	192.168.0.3

Click **Clear All** to clear all Event Log records.

7.6.2 HTTP Upgrade

Click the option **HTTP Upgrade** from the **System Utility** menu and then the following screen page appears.



HTTP Upgrade

Configuration Update

Backup	Config Type	Running-config
	device configuration to local file	Backup
Restore	Browse.. Restore	

Firmware Update

Upgrade Image Option	Image1
Select File	Browse.. Upload

Configuration Update

Config Type: There are three configuration types: Running-config, Default-config and Start-up-config

Running-config: Back up the configuration you're processing.

Default-config: Back up the factory setting.

Start-up-config: Back up the last saved configuration.

Device Configuration to Local File: Click **Backup** and define the route where you intend to save the configuration.

Restore: Click **Browse**, select the designated file and then click **Restore**.

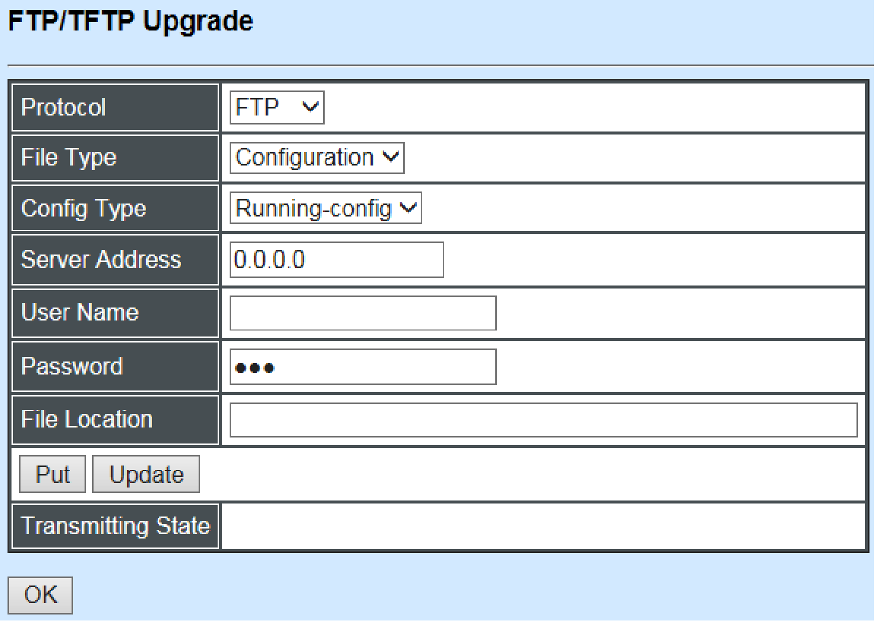
Firmware Update

Upgrade Image Option: Choose the image you want to upgrade.

Select File: Click **Browse**, select the designated file and then click **Upload**.

7.6.3 FTP/TFTP Upgrade

Click the option **FTP/TFTP Upgrade** from the **System Utility** menu and then the following screen page appears.



FTP/TFTP Upgrade

Protocol	FTP
File Type	Configuration
Config Type	Running-config
Server Address	0.0.0.0
User Name	
Password	●●●
File Location	
Put Update	
Transmitting State	

OK

Protocol: Select the preferred protocol, either FTP or TFTP.

File Type: Select the file type to process, either Configuration or Firmware.

Config Type: Three options for Config Type are available while the File Type is Configuration: Running-config, Default-config and Start-up-config.

Upgrade Image Option: While the File Type is Firmware, select Image1 or Image2 to update the firmware.

Server Address: Enter the specific IP address of the File Server.

User Name: Enter the specific username to access the File Server. (Leave it blank while using TFTP)

Password: Enter the specific password to access the File Server. (Leave it blank while using TFTP)

File Location: Enter the specific path and filename within the File Server.

Put: Click **Put** to start the upload procedure and transmit the file to the server.

Update: Click **Update** to instruct the Managed Industrial PoE Switch to update the firmware or configuration from the File Server. After a successful update, a message will pop up. The Managed Industrial PoE Switch will need a reset to make changes effective.

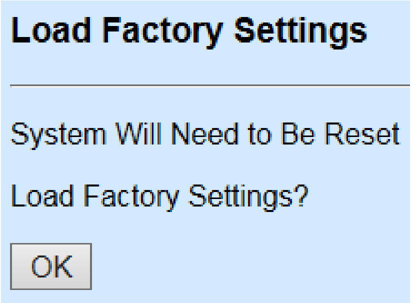
Transmitting State: This field displays the uploading or updating status.

OK: Click **OK** to update the firmware or configuration from the File Server.

7.6.4 Load Factory Settings

Load Factory Settings will set all configurations of the Managed Industrial PoE Switch back to the factory default settings, including the IP and Gateway address. This function is useful when network administrators would like to re-configure the system. A system reset is required to make all changes effective after Load Factory Settings.

Select **Load Factory Settings** from the **System Utility** menu and then the following screen page appears.



Load Factory Settings

System Will Need to Be Reset

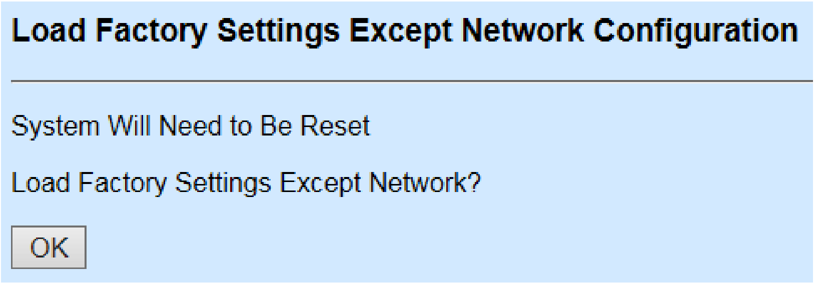
Load Factory Settings?

Click the **"OK"** button to restore the Managed Industrial PoE Switch back to the defaults.

7.6.5 Load Factory Settings Except Network Configuration

Load Factory Settings Except Network Configuration will set all configurations of the Managed Industrial PoE Switch back to the factory default settings. However, IP and Gateway addresses will not restore to the factory default. **Load Factory Settings Except Network Configuration** is very useful when network administrators need to re-configure the system "REMOTELY", because conventional Factory Reset will bring network settings back to default and lose all remote network connections.

Select **Load Factory Setting Except Network Configuration** from the **System Utility** menu, then the following screen page shows up.



Load Factory Settings Except Network Configuration

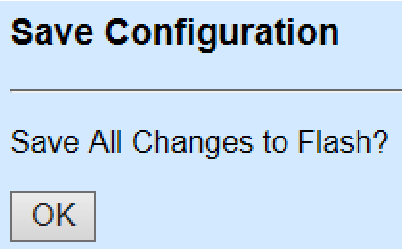
System Will Need to Be Reset

Load Factory Settings Except Network?

Click the **"OK"** button to restore the Managed Industrial PoE Switch back to the defaults excluding network configurations.

7.7 Save Configuration

To keep the existing configurations permanently, users need to save the configurations first before resetting the Managed Industrial PoE Switch. Select **Save Configuration** from the **Main Menu** and then the following screen page appears.



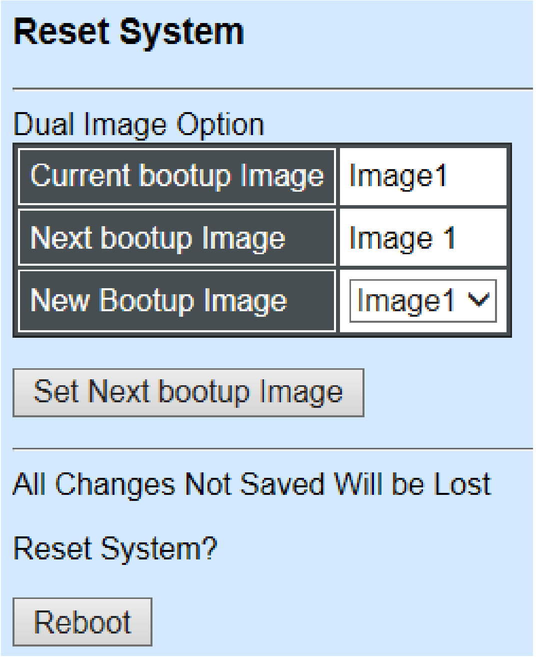
Save Configuration

Save All Changes to Flash?

Click the **“OK”** button to save changes or running configurations to Flash.

7.8 Reset System

After any configuration changes, **Reset System** can make changes effective. Select **Reset System** from the **Main menu** and then the following screen page appears.



Reset System

Dual Image Option

Current bootup Image	Image1
Next bootup Image	Image 1
New Bootup Image	Image1

All Changes Not Saved Will be Lost

Reset System?

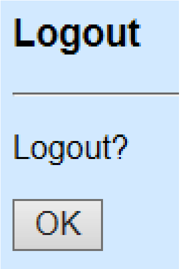
The Managed Industrial PoE Switch supports Dual Image for boot-up, please select the next boot-up image before restarting.

Click the **“Set Next bootup Image”** button to set the designated image for booting up.

Click the **“Reboot”** button to restart the Managed Industrial PoE Switch.

7.9 Logout

Select **Logout** from the **Main menu** and then the following screen page appears.



Logout

Logout?

Click the **“OK”** button to logout the Managed Industrial PoE Switch.

APPENDIX A: DHCP Auto-Provisioning Setup

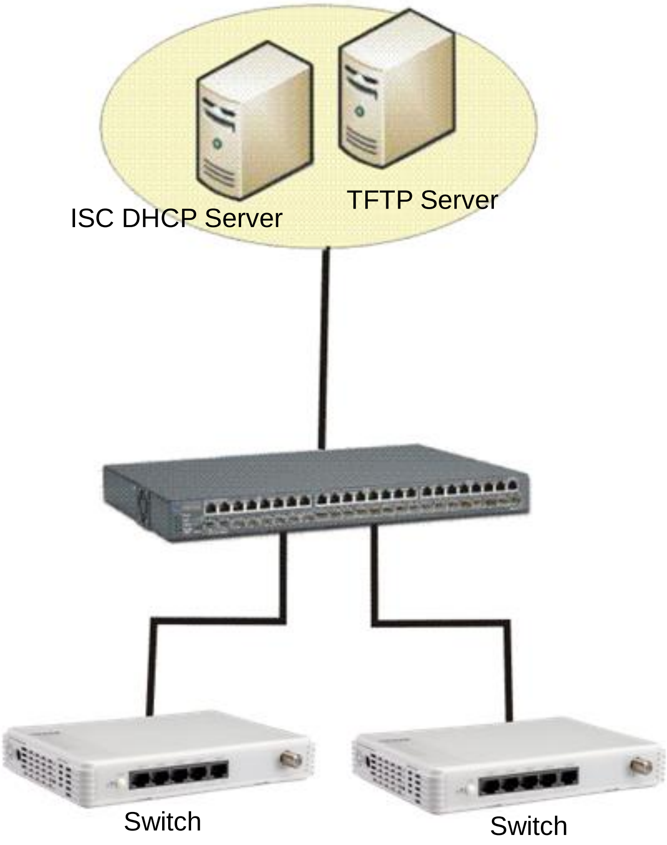
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the Managed Industrial PoE Switch that you purchased supports DHCP Auto-provisioning. Setup procedures and auto-provisioning process are described below for your reference.

A. Setup Procedures

Follow the steps below to set up Auto Provisioning server, modify dhcpd.conf file and generate a copy of configuration file.

Step 1. Set Up Environment

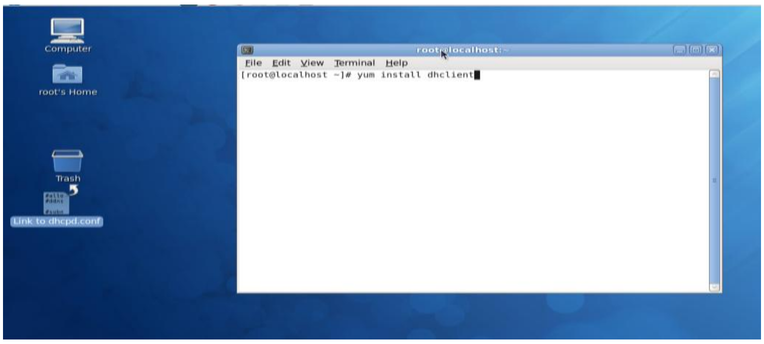
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Topology Example

Step 2. Set Up Auto Provision Server

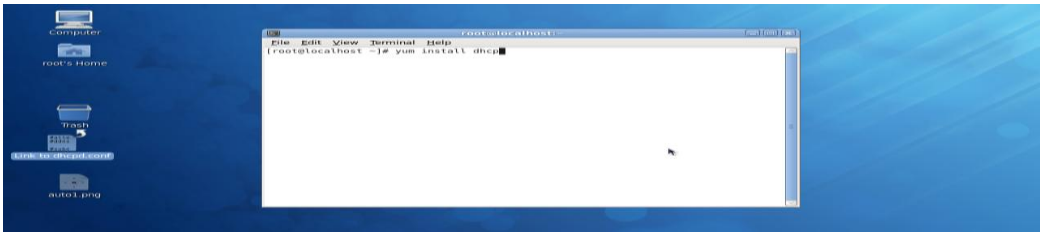
- **Update DHCP client**



```
[root@localhost ~]# yum install dhclient
```

Linux Fedora 12 supports "yum" function by default. First of all, update DHCP client function by issuing "yum install dhclient" command.

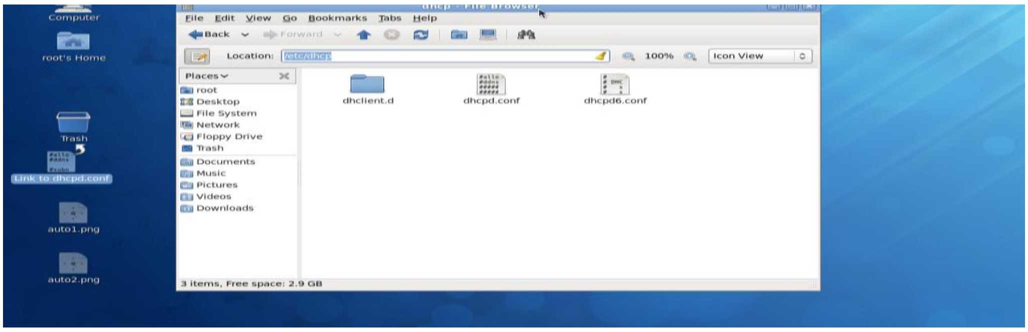
- **Install DHCP server**



```
[root@localhost ~]# yum install dhcp
```

Issue "yum install dhcp" command to install DHCP server.

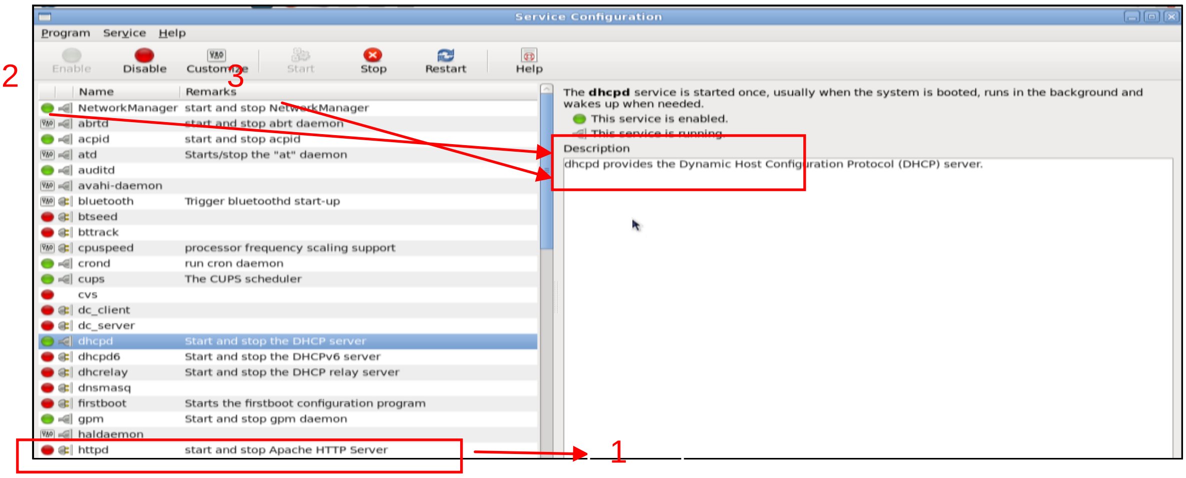
- **Copy dhcpd.conf to /etc/dhcp/ directory**



Copy dhcpd.conf file provided by the vendor to /etc/dhcp/ directory.

Please note that each vendor has its own way to define auto-provisioning. Make sure to use the file provided by the vendor.

Enable and run DHCP service



Name	Remarks
NetworkManager	start and stop NetworkManager
abrtd	start and stop abrt daemon
acpid	start and stop acpid
atd	Starts/stop the "at" daemon
auditd	
avahi-daemon	
bluetooth	Trigger bluetoothd start-up
btseed	
bttrack	
cpuspeed	processor frequency scaling support
crond	run cron daemon
cups	The CUPS scheduler
cvs	
dc_client	
dc_server	
dhcpd	Start and stop the DHCP server
dhcpd6	Start and stop the DHCPv6 server
dhcrelay	Start and stop the DHCP relay server
dnsmasq	
firstboot	Starts the firstboot configuration program
gpm	Start and stop gpm daemon
haldaemon	
httpd	start and stop Apache HTTP Server

The **dhcpd** service is started once, usually when the system is booted, runs in the background and wakes up when needed.

This service is enabled.

This service is running.

Description

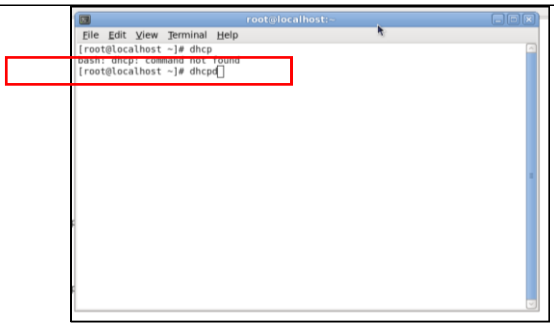
dhcpd provides the Dynamic Host Configuration Protocol (DHCP) server.

1. Choose dhcpd.

2. Enable DHCP service.

3. Start running DHCP service.

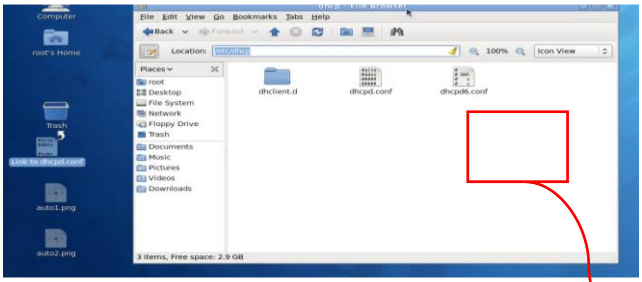
***NOTE:** DHCP service can also be enabled using CLI. Issue "dhcpd" command to enable DHCP service.*

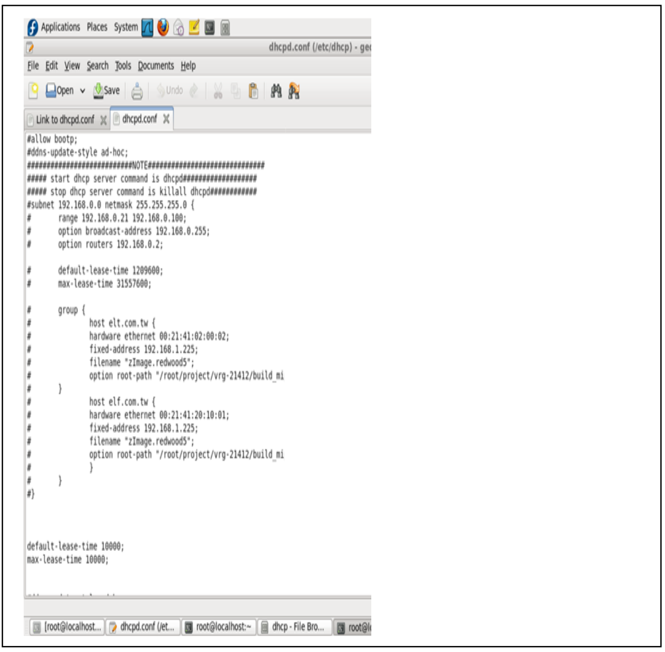


```
[root@localhost ~]# dhcp
bash: dhcp: command not found
[root@localhost ~]# dhcpd
```

Step 3. Modify dhcpd.conf File

Open dhcpd.conf file in /etc/dhcp/ directory



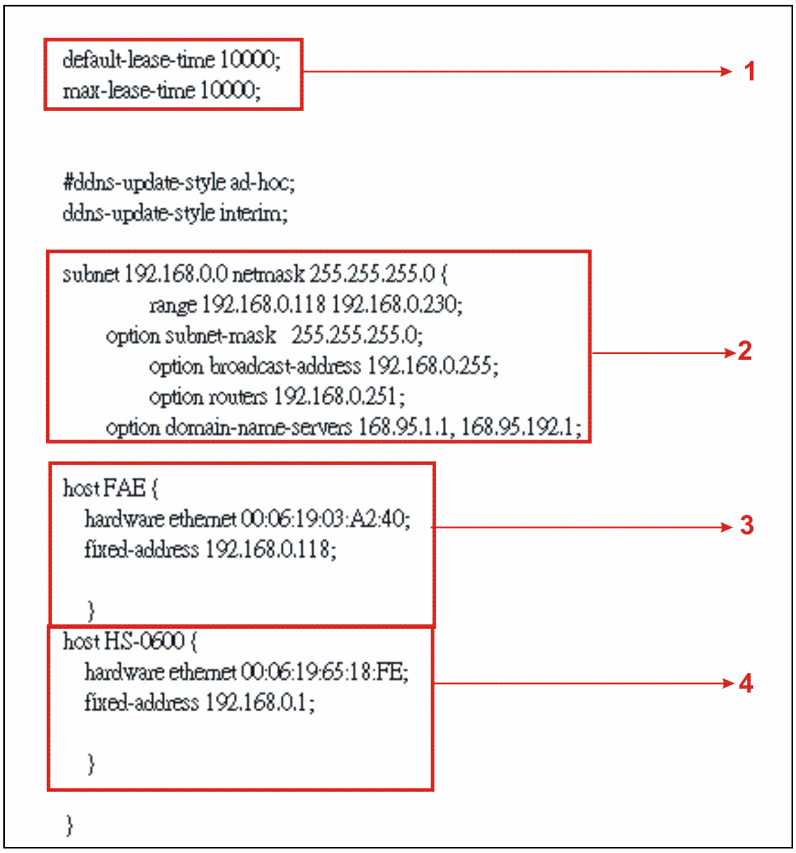


```
#allow bootp;
#ddns-update-style ad-hoc;
###########################NOTE##############################
##### start dhcp server command is dhcpd###################
##### stop dhcp server command is killall dhcpd############
#subnet 192.168.0.0 netmask 255.255.255.0 {
#       range 192.168.0.21 192.168.0.100;
#       option broadcast-address 192.168.0.255;
#       option routers 192.168.0.2;

#       default-lease-time 1209600;
#       max-lease-time 31557600;

#       group {
#               host elt.com.tw {
#               hardware ethernet 00:21:41:02:00:02;
#               fixed-address 192.168.1.225;
#               filename "zImage.redwood5";
#               option root-path "/root/project/vrg-21412/build_mi
#       }
#               host elf.com.tw {
#               hardware ethernet 00:21:41:20:10:01;
#               fixed-address 192.168.1.225;
#               filename "zImage.redwood5";
#               option root-path "/root/project/vrg-21412/build_mi
#               }
#       }
#}



default-lease-time 10000;
max-lease-time 10000;
```

Double-click dhcpd.conf placed in /etc/dhcp/ di

Modify dhcpd.conf file

The following marked areas in dhcpd.conf file can be modified with values that work with your networking environment.



```
default-lease-time 10000;
max-lease-time 10000;


#ddns-update-style ad-hoc;
ddns-update-style interim;

subnet 192.168.0.0 netmask 255.255.255.0 {
            range 192.168.0.118 192.168.0.230;
      option subnet-mask   255.255.255.0;
            option broadcast-address 192.168.0.255;
            option routers 192.168.0.251;
      option domain-name-servers 168.95.1.1, 168.95.192.1;

host FAE {
   hardware ethernet 00:06:19:03:A2:40;
   fixed-address 192.168.0.118;

   }
host HS-0600 {
   hardware ethernet 00:06:19:65:18:FE;
   fixed-address 192.168.0.1;

   }

}
```

1. Define DHCP default and maximum lease time in seconds.

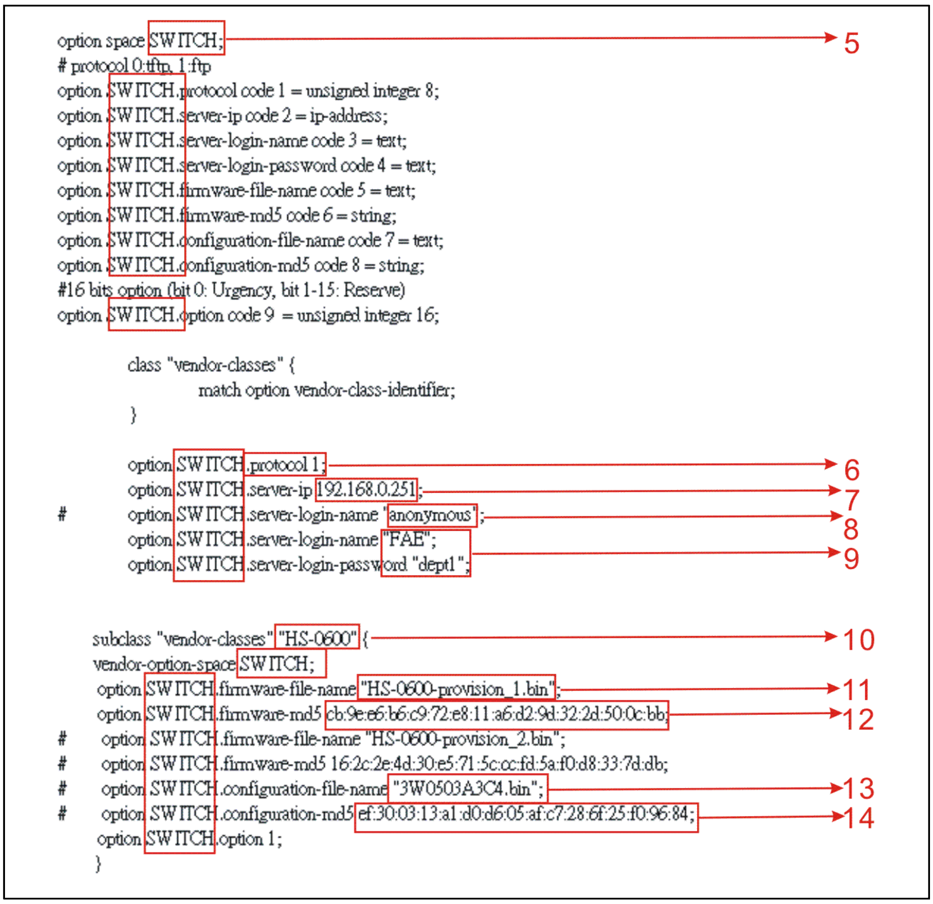
   Default lease time: If a client does not request a specific IP lease time, the server will assign a default lease time value.

   Maximum lease time: This is the maximum length of time that the server will lease for.

2. Define subnet, subnet mask, IP range, broadcast address, router address and DNS server address.

3. Map a host’s MAC address to a fixed IP address.

4. Map a host’s MAC address to a fixed IP address. Use the same format to create multiple MAC-to-IP address bindings.



```
option space SWITCH;
# protocol 0:tftp, 1:ftp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
option SWITCH.server-login-password code 4 = text;
option SWITCH.firmware-file-name code 5 = text;
option SWITCH.firmware-md5 code 6 = string;
option SWITCH.configuration-file-name code 7 = text;
option SWITCH.configuration-md5 code 8 = string;
#16 bits option (bit 0: Urgency, bit 1-15: Reserve)
option SWITCH.option code 9  = unsigned integer 16;

         class "vendor-classes" {
                  match option vendor-class-identifier;
         }

         option SWITCH.protocol 1;
         option SWITCH.server-ip 192.168.0.251;
#        option SWITCH.server-login-name "anonymous";
         option SWITCH.server-login-name "FAE";
         option SWITCH.server-login-password "dept1";


     subclass "vendor-classes" "HS-0600" {
     vendor-option-space SWITCH;
      option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
      option SWITCH.firmware-md5 cb:9e:e6:b6:c9:72:e8:11:a6:d2:9d:32:2d:50:0c:bb;
#      option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
#      option SWITCH.firmware-md5 16:2c:2e:4d:30:e5:71:5c:cc:fd:5a:f0:d8:33:7d:db;
#      option SWITCH.configuration-file-name "3W0503A3C4.bin";
#      option SWITCH.configuration-md5 ef:30:03:13:a1:d0:d6:05:af:c7:28:6f:25:f0:96:84;
      option SWITCH.option 1;
      }
```

This value is configurable and can be defined by users.

Specify the protocol used (Protocol 1: FTP; Protocol 0: TFTP).

Specify the FTP or TFTP IP address.

Login TFTP server anonymously (TFTP does not require a login name and password).

Specify FTP Server login name and password.

Specify the product model name.

Specify the firmware filename.

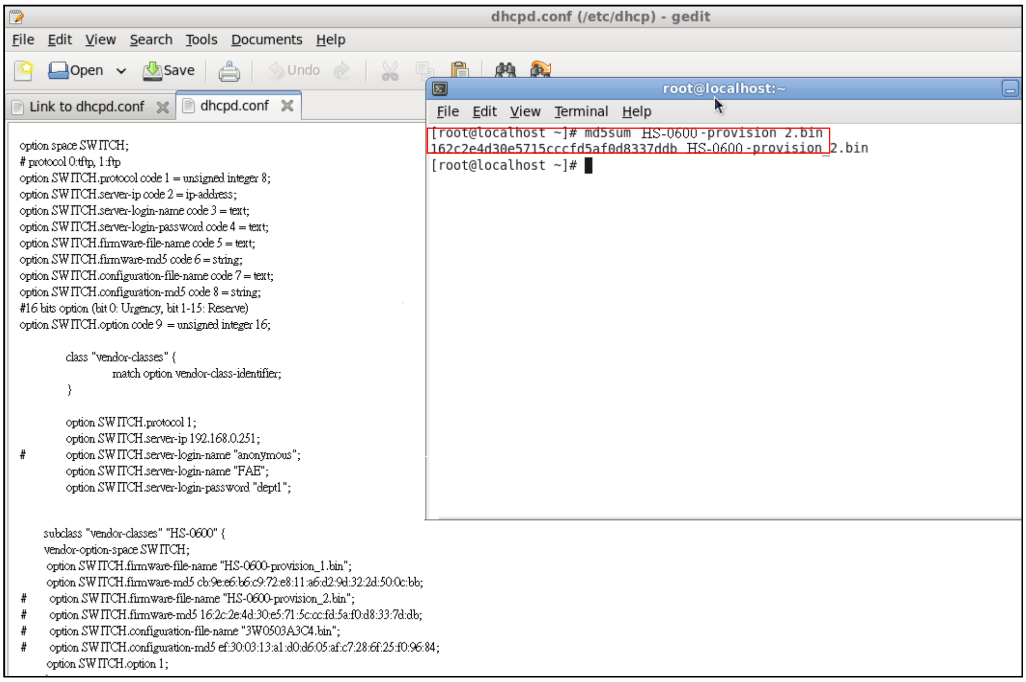
Specify the MD5 for firmware image.

Specify the configuration filename.

Specify the MD5 for configuration file.

NOTE 1: *The text beginning with a pound sign (#) will be ignored by the DHCP server. For example, in the figure shown above, firmware-file-name “HS-0600-provision_2.bin” and firmware-md5 (line 5 & 6 from the bottom) will be ignored. If you want DHCP server to process these two lines, remove pound signs in the initial of each line.*

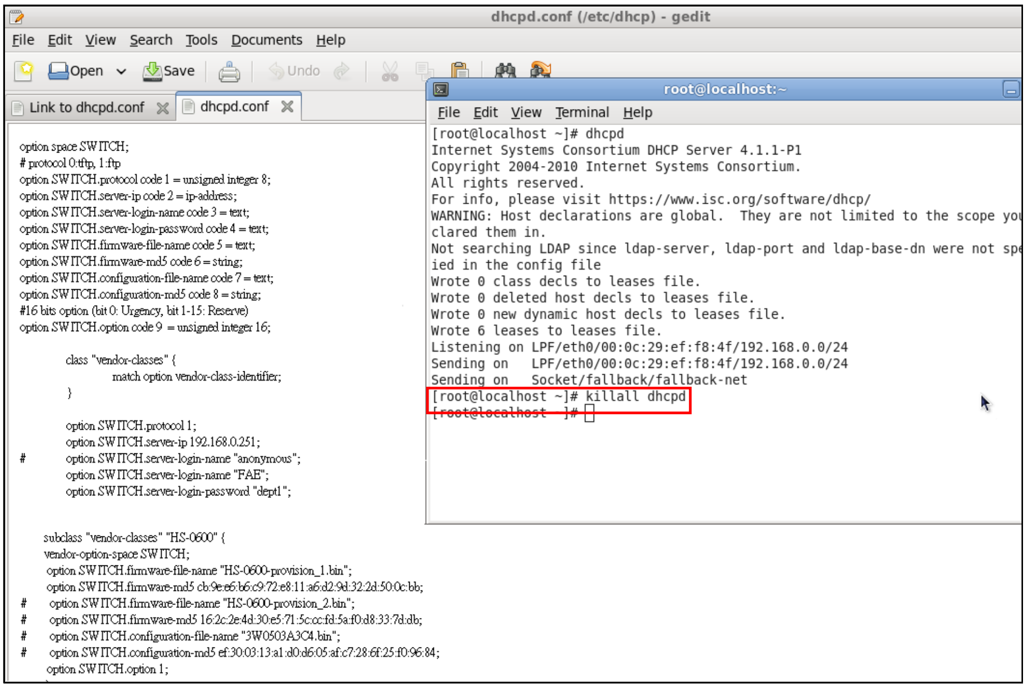
***NOTE 2:** You can use either free software program or Linux default md5sum function to get MD5 checksum for firmware image and configuration file.*


dhcpd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
Link to dhcpd.conf
dhcpd.conf
root@localhost:~
File Edit View Terminal Help

```
option space SWITCH;
# protocol 0:tftp, 1:ftp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
option SWITCH.server-login-password code 4 = text;
option SWITCH.firmware-file-name code 5 = text;
option SWITCH.firmware-md5 code 6 = string;
option SWITCH.configuration-file-name code 7 = text;
option SWITCH.configuration-md5 code 8 = string;
#16 bits option (bit 0: Urgency, bit 1-15: Reserve)
option SWITCH.option code 9  = unsigned integer 16;

        class "vendor-classes" {
                match option vendor-class-identifier;
        }

        option SWITCH.protocol 1;
        option SWITCH.server-ip 192.168.0.251;
#       option SWITCH.server-login-name "anonymous";
        option SWITCH.server-login-name "FAE";
        option SWITCH.server-login-password "dept1";


    subclass "vendor-classes" "HS-0600" {
    vendor-option-space SWITCH;
     option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
     option SWITCH.firmware-md5 cb:9e:e6:b6:c9:72:e8:11:a6:d2:9d:32:2d:50:0c:bb;
#     option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
#     option SWITCH.firmware-md5 16:2c:2e:4d:30:e5:71:5c:cc:fd:5a:f0:d8:33:7d:db;
#     option SWITCH.configuration-file-name "3W0503A3C4.bin";
#     option SWITCH.configuration-md5 ef:30:03:13:a1:d0:d6:05:af:c7:28:6f:25:f0:96:84;
     option SWITCH.option 1;
```

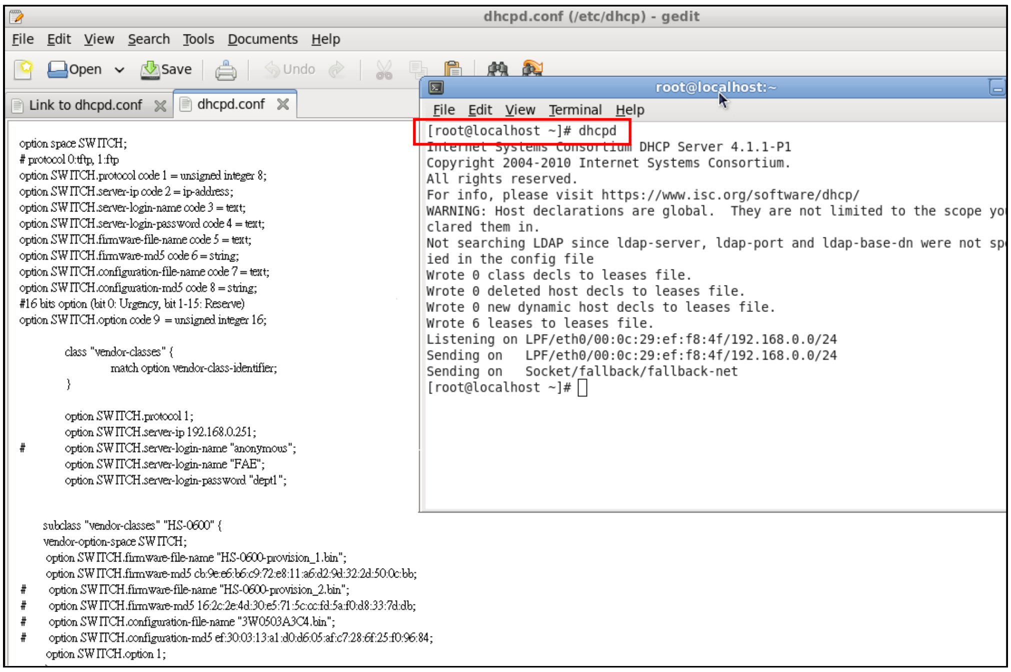
```
[root@localhost ~]# md5sum HS-0600-provision 2.bin
162c2e4d30e5715cccfd5af0d8337ddb HS-0600-provision_2.bin
[root@localhost ~]#
```

Restart DHCP service


dhcpd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
Link to dhcpd.conf
dhcpd.conf
root@localhost:~
File Edit View Terminal Help

```
option space SWITCH;
# protocol 0:tftp, 1:ftp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
option SWITCH.server-login-password code 4 = text;
option SWITCH.firmware-file-name code 5 = text;
option SWITCH.firmware-md5 code 6 = string;
option SWITCH.configuration-file-name code 7 = text;
option SWITCH.configuration-md5 code 8 = string;
#16 bits option (bit 0: Urgency, bit 1-15: Reserve)
option SWITCH.option code 9  = unsigned integer 16;

        class "vendor-classes" {
                match option vendor-class-identifier;
        }

        option SWITCH.protocol 1;
        option SWITCH.server-ip 192.168.0.251;
#       option SWITCH.server-login-name "anonymous";
        option SWITCH.server-login-name "FAE";
        option SWITCH.server-login-password "dept1";


    subclass "vendor-classes" "HS-0600" {
    vendor-option-space SWITCH;
     option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
     option SWITCH.firmware-md5 cb:9e:e6:b6:c9:72:e8:11:a6:d2:9d:32:2d:50:0c:bb;
#     option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
#     option SWITCH.firmware-md5 16:2c:2e:4d:30:e5:71:5c:cc:fd:5a:f0:d8:33:7d:db;
#     option SWITCH.configuration-file-name "3W0503A3C4.bin";
#     option SWITCH.configuration-md5 ef:30:03:13:a1:d0:d6:05:af:c7:28:6f:25:f0:96:84;
     option SWITCH.option 1;
```

```
[root@localhost ~]# dhcpd
Internet Systems Consortium DHCP Server 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
WARNING: Host declarations are global.  They are not limited to the scope you
clared them in.
Not searching LDAP since ldap-server, ldap-port and ldap-base-dn were not spe
ied in the config file
Wrote 0 class decls to leases file.
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 6 leases to leases file.
Listening on LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on   LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on   Socket/fallback/fallback-net
[root@localhost ~]# killall dhcpd
[root@localhost ~]#
```


dhcpd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
Link to dhcpd.conf
dhcpd.conf
root@localhost:~
File Edit View Terminal Help

```
option space SWITCH;
# protocol 0:tftp, 1:ftp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
option SWITCH.server-login-password code 4 = text;
option SWITCH.firmware-file-name code 5 = text;
option SWITCH.firmware-md5 code 6 = string;
option SWITCH.configuration-file-name code 7 = text;
option SWITCH.configuration-md5 code 8 = string;
#16 bits option (bit 0: Urgency, bit 1-15: Reserve)
option SWITCH.option code 9  = unsigned integer 16;

        class "vendor-classes" {
                match option vendor-class-identifier;
        }

        option SWITCH.protocol 1;
        option SWITCH.server-ip 192.168.0.251;
#       option SWITCH.server-login-name "anonymous";
        option SWITCH.server-login-name "FAE";
        option SWITCH.server-login-password "dept1";


    subclass "vendor-classes" "HS-0600" {
    vendor-option-space SWITCH;
     option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
     option SWITCH.firmware-md5 cb:9e:e6:b6:c9:72:e8:11:a6:d2:9d:32:2d:50:0c:bb;
#     option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
#     option SWITCH.firmware-md5 16:2c:2e:4d:30:e5:71:5c:cc:fd:5a:f0:d8:33:7d:db;
#     option SWITCH.configuration-file-name "3W0503A3C4.bin";
#     option SWITCH.configuration-md5 ef:30:03:13:a1:d0:d6:05:af:c7:28:6f:25:f0:96:84;
     option SWITCH.option 1;
```

```
[root@localhost ~]# dhcpd
Internet Systems Consortium DHCP Server 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
WARNING: Host declarations are global.  They are not limited to the scope yo
clared them in.
Not searching LDAP since ldap-server, ldap-port and ldap-base-dn were not sp
ied in the config file
Wrote 0 class decls to leases file.
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 6 leases to leases file.
Listening on LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on   LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on   Socket/fallback/fallback-net
[root@localhost ~]# 
```

Every time you modify dhcpd.conf file, DHCP service must be restarted. Issue “killall dhcpd” command to disable DHCP service and then issue “dhcpd” command to enable DHCP service.

Step 4. Backup a Configuration File

Before preparing a configuration file in TFTP/FTP Server, make sure the device generating the configuration file is set to **“Get IP address from DHCP”** assignment. DHCP Auto-provisioning is running under DHCP mode, so if the configuration file is uploaded by the network type other than DHCP mode, the downloaded configuration file has no chance to be equal to DHCP when provisioning, and it results in MD5 never matching and causes the device to reboot endlessly.

In order to have your Managed Industrial PoE Switch retrieve the correct configuration image in TFTP/FTP Server, please make sure the filename of your configuration file is defined exactly the same as the one specified in **dhcpd.conf**. For example, if the configuration image’s filename specified in dhcpd.conf is “metafile”, the configuration image filename should be named to “metafile” as well.

Step 5. Place a Copy of Firmware and Configuration File in TFTP/FTP

The TFTP/FTP File server should include the following items:

1. Firmware image (This file is provided by the vendor.)

2. Configuration file (This file is generally created by users.)

3. User account for your device (For FTP server only.)

B. Auto-Provisioning Process

This switching device is setting-free (through auto-upgrade and configuration) and its upgrade procedures are as follows:

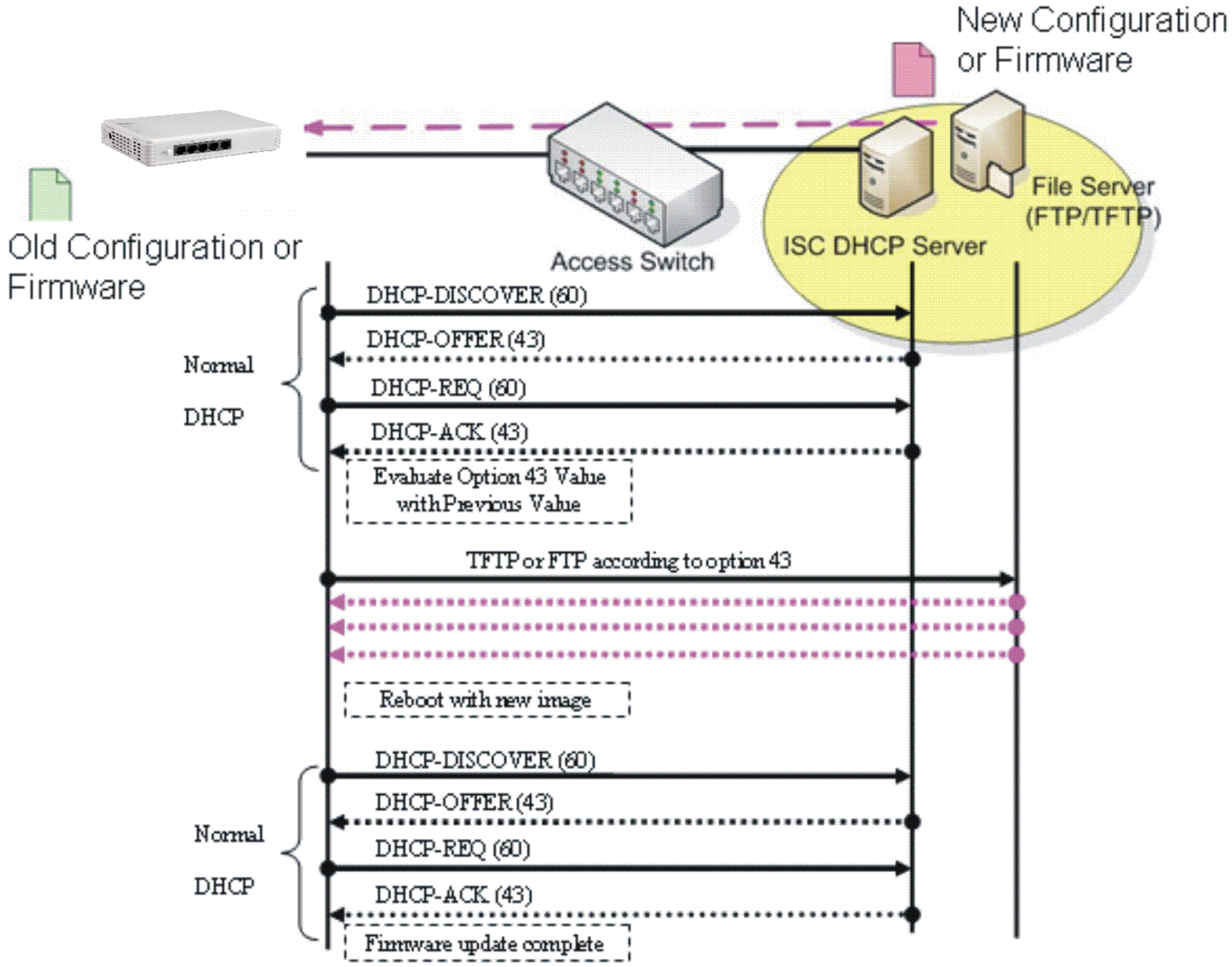
1. ISC DHCP server will recognize the device when it receives an IP address request sent by the device, and it will tell the device how to get a new firmware or configuration.

2. The device will compare the firmware and configuration MD5 code form of DHCP option every time it communicates with DHCP server.

3. If MD5 code is different, the device will then upgrade the firmware or configuration. However, it will not be activated immediately.

4. If the Urgency Bit is set, the device will be reset to activate the new firmware or configuration immediately.

5. The device will retry for 3 times if the file is incorrect, and then it gives up until getting another DHCP ACK packet again.



APPENDIX B: Free RADIUS readme

The advanced RADIUS Server Set up for **RADIUS Authentication** is described as below.

When free RADIUS client is enabled on the device, the server side needs to put this file "**dictionary.sample**" under the directory **/raddb**, and modify these three files **-** "**users**", "**clients.conf**" and "**dictionary**", which are on the disc shipped with this product.

In the file "**users**":

Set up the user name, password, and other attributes.

In the file "**clients.conf**":

Set the valid range of RADIUS client IP address.

In the file "**dictionary**":

Add this following line -

```
$INCLUDE dictionary.sample
```

***Note:** Please use any text editing software (e.g. Notepad) to carry out the file editing works.*