CTS
CONNECTION TECHNOLOGY SYSTEMS

IES-3110
Managed Industrial Gigabit Ethernet Switch

Network Management User's Manual

Version 1.0

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

Version	Firmware	Modification	Date
0.90	0.99.04	The initial version	20161007
0.90	0.99.0C	Add Rapid Spanning Tree(Section 3.4.5), Trap Destination(Section 3.3.6), Trap Configuration(Section 3.3.7), IGMP(Section 3.4.7), Ring Detection(Section 3.4.8)	20170109
0.90	0.99.0F	Add Time Range (Section 3.3.5), SNMPv3 USM User (Section 3.3.7), Broadcast Storm Control (Section 3.4.2), LACP Port Configuration (Section 3.4.6.3), Mirroring Configuration (Section 3.4.9), Loop Detection (Section 3.4.12), DHCP Snooping (Section 3.4.15) Revise MAC Quotient (Section 3.4.6.1)	20170217
0.90	0.99.0K		20170712
1.0	1.00.0P	**Add:** 2.5.4 Archive Command 2.5.7 Fast-redundancy Command 2.5.21 Security Command 3.4.8 802.1X Configuration 3.4.9 Static MAC Table Configuration 3.4.16 Fast Redundancy 3.5.13 Fast Redundancy Status 3.6.6 Auto-Backup Configuration **Revise:** 2.5.11 MAC Command 2.5.12 Management Command 2.5.16 SNMP Server Command 2.5.17 Spanning Tree Command 2.5.18 Switch Command 3.3.2 System Service Configuration 3.3.3 RS232/Telnet/Console Configuration 3.3.8 Trap Configuration 3.4.1 Switch Configuration 3.4.5 QoS Priority Configuration Appendix B: FreeRADIUS Readme	20221018

Table of Content

1. OVERVIEW

Thank you for choosing the Managed Industrial Gigabit Ethernet Switches. The Managed Industrial Gigabit Ethernet Switches are designed to meet the massive needs for Gigabit Ethernet network deployments and aim at Industrial 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 and 802.3x standards. The built-in management module allows users to configure this Managed Industrial Gigabit Ethernet Switch and monitor the operation status locally or remotely through network.

Besides, redundant power supplies are offered on the Managed Industrial 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).

1.1 Management Preparations

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

1.1.1 Connecting the Managed Industrial Switch

It is extremely important that proper cables are used with correct pin arrangements when connecting the Managed Industrial 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 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 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.

1.1.2 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.

1.2 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.
STATUS	System Status	Orange	System is booting up.
		Green	System is working normally.
		Green Blinking	When a USB is inserted, the Status LED indicator will blink 3 times in green.
			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.
RM	Role	Off	The role of switch is slave.
		Green	The role of switch is master.
R	Function	Off	Ring Detection is disabled.
		Green	Ring Detection is enabled.
LINK/ACT 1~10	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.

2. 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

2.1 Remote Console Management-Telnet

You can use Command Line Interface to manage the Managed Industrial Gigabit Ethernet Switch via Telnet session. For first-time users, you must first assign a unique IP address to the Managed Industrial 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 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 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 Gigabit Ethernet Switch via Telnet session again.

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

2.2 Navigating CLI

After you successfully access to the Managed Industrial 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 Gigabit Ethernet Switch. If you would like to configure advanced features of the Managed Industrial 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 Gigabit Ethernet Switch.

Command Mode	Access Method	Prompt Displayed	Exit Method
User Mode	Login username & password	Switch>	logout
Privileged Mode	From User Mode, enter the *enable* command	Switch#	disable, exit, logout
Configuration Mode	From Privileged Mode, enter the *config* or *configure* command	Switch(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.*

2.2.1 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

2.2.2 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.

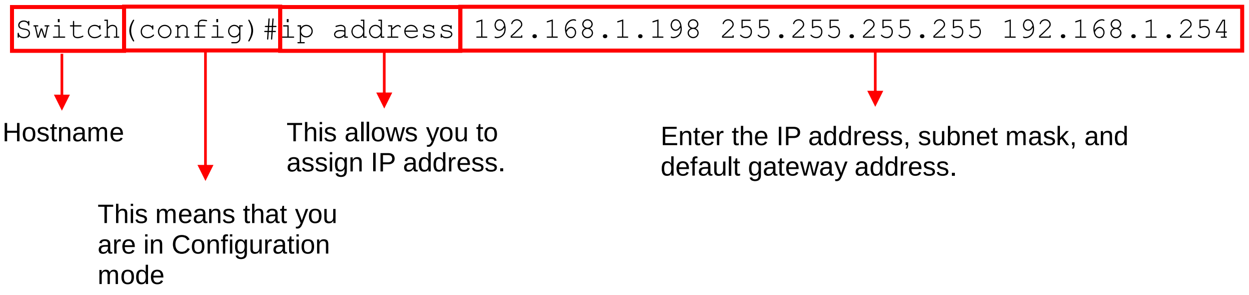
Unfinished command followed by ?	Enter an unfinished command or keyword and press “?” key to complete the command and get command syntax help.
	
	Examples:
	`Switch#h?`
	`help        Show available commands`
	`history     Show history commands`

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.

2.2.3 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 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 means that you are in Configuration mode

This allows you to assign IP address.

Enter the IP address, subnet mask, and default gateway address.

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`

2.2.4 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 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 Gigabit Ethernet Switch for use after you gain access again to the device.

2.3 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 Gigabit Ethernet Switch.
enable	Enter Privileged mode.

2.4 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 Gigabit Ethernet Switch.
reload	Restart the Managed Industrial Gigabit Ethernet Switch.
write	Save the current configurations to Flash.
configure	Enter Global Configuration mode
show	Display the system information.

2.4.1 Copy-cfg Command

Use the “copy-cfg” command to restore the Managed Industrial 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 Gigabit Ethernet Switch back to default settings:**

Command / Example
Switch# copy-cfg from default

NOTE: *There are two ways to set the Managed Industrial 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 Gigabit 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		

2.4.2 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	[A.B.C.D]	Enter the IP address of your TFTP server.

upgrade tftp [A.B.C.D] [file_name]	[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		

2.4.3 Reload Command

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

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

2.4.4 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 Gigabit Ethernet Switch.

Command / Example
Switch# write

2.4.5 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)#

2.5 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
archive	Manage archive configuration files.
channel-group	Link Aggregation/LACP global configuration commands
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.
fast-redundancy	Set up Fast Ring v2 and Chain configuration for fast network recovery.
ip	Global IP configuration commands
lldp	LLDP global configuration mode
loop-detection	Configure loop-detection to prevent loop between switch ports by locking them.
mac	Global MAC configuration commands
management	Manage the interface configuration.
mirror	Set up target port for mirroring.
ntp	Set up required configurations for Network Time Protocol.
qos	Set up the priority of packets within the Managed Industrial Switch.
security	Set up storm control settings.
snmp-server	Create a new SNMP community and trap destination and specify the trap types.
spanning-tree	Set up RSTP status of each port and aggregated ports.
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.
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.

2.5.1 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 "Loop Detection", "QoS", "VLAN" and "Security" commands. For detailed usages, please refer to Loop Detection, QoS, VLAN and Security sections below.

2.5.2 No Command

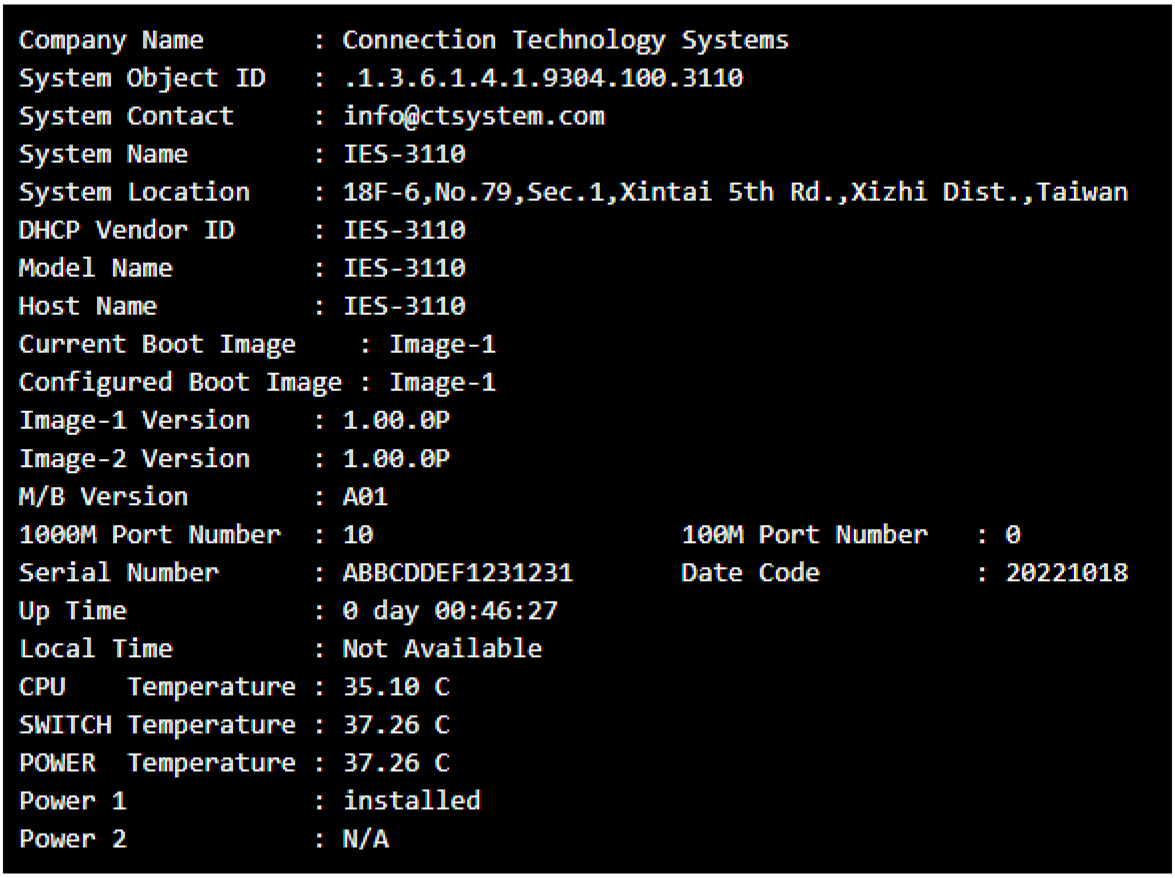
Most commands that you enter in Configuration mode can be negated by "no" command following the same or original command. The purpose of "no" command is to disable a function, remove a command, or configure the setting back to the default value. In each sub-section below, the use of no command to fulfill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

2.5.3 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:

1. Displaying system information

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



```
Company Name        : Connection Technology Systems
System Object ID    : .1.3.6.1.4.1.9304.100.3110
System Contact      : info@ctsystem.com
System Name         : IES-3110
System Location     : 18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan
DHCP Vendor ID      : IES-3110
Model Name          : IES-3110
Host Name           : IES-3110
Current Boot Image    : Image-1
Configured Boot Image : Image-1
Image-1 Version     : 1.00.0P
Image-2 Version     : 1.00.0P
M/B Version         : A01
1000M Port Number   : 10                    100M Port Number   : 0
Serial Number       : ABBCDDEF1231231       Date Code          : 20221018
Up Time             : 0 day 00:46:27
Local Time          : Not Available
CPU    Temperature  : 35.10 C
SWITCH Temperature  : 37.26 C
POWER  Temperature  : 37.26 C
Power 1             : installed
Power 2             : N/A
```

Company Name: Display a company name for this Managed Industrial 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 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 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 Managed Industrial 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

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

Date Code: Displays the Managed Industrial 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.

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.

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.

2.5.4 Archive Command

Command	Parameter	Description
Switch(config)# archive auto-backup		Enable the auto-backup configuration files function.
Switch(config)# archive auto-backup path ftp [A.B.C.D] [file_directory] [user_name] [password]	[A.B.C.D]	Specify the IP address of the FTP server.
	[file_directory]	Specify the file directory of the FTP server to save the start-up configuration files.
	[user_name]	Specify the user name to login the FTP server.
	[password]	Specify the password for FTP server's authentication.
Switch(config)# archive auto-backup path tftp [A.B.C.D] [file_directory]	[A.B.C.D]	Specify the IP address of the TFTP server.
	[file_directory]	Specify the file directory of the TFTP server to save the start-up configuration files.
Switch(config)# archive auto-backup time [0-23]	[0-23]	Specify the time to begin the automatic backup of the start-up configuration files everyday.
No command		
Switch(config)# no archive auto-backup		Disable the auto-backup function.
Switch(config)# no archive auto-backup path		Remove TFTP / FTP server settings.
Switch(config)# no archive auto-backup time		Reset the Auto-backup time back to the default (0 o'clock).
Show command		**Description**
Switch# show archive auto-backup		Display the auto-backup configuration.
Switch(config)# show archive auto-backup		Display the auto-backup configuration.

2.5.5 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. Configuring MAC Quotient

Command	Parameter	Description
Switch(config)# channel-group type mac-quotient		Enable distributing packets according to the MAC address.
No command		
Switch(config)# no channel-group type mac-quotient		Disable distributing packets according to the MAC address.

Here is how it works.

1. Identifying MAC

It checks the last three bits of Source MAC and Dst. MAC and XOR algorithm distributes them.

XOR Algorithm:

0 & 0 = 0

0 & 1 = 1

1 & 0 = 1

1 & 1 = 0

Three bits results in eight combinations (0~7), it is used to determine which packet should be sent to.

Example:

Source MAC 11:22:33:44:55:66

⇧ The last digit 6 occupies 4 bits (Use the last three bits ⇨ 0100)

Dst. MAC   33:44:55:66:77:88

⇧ The last digit 8 occupies 4 bits (Use the last three bits ⇨ 1000)

XOR Algorithm:

Src. MAC – 1 1 0

Dst. MAC – 0 0 0

Result – 1 1 0 = 6

2. MAC Quotient Distribution

Example 1:

Assume that 2 ports are aggregated

8(bit)/2(port) = 4 (Integer) ⇨ each port is evenly distributed 4 types of bit

8(bit)/2(port) = 0 (Remainder) ⇨ The first ports will be distributed extra bits, if any

If enabled:

Port 1 will get 4 bits ⇨ 0, 1, 2, 3

Port 2 will get 4 bits ⇨ 4, 5, 6, 7

Example 2:

Assume that 3 ports are aggregated

8(bit)/2(port) = 2 (Integer) ⇨ each port is distributed 2 types of bit at least

8(bit)/2(port) = 2 (Remainder) ⇨ The first two ports will be additionally gotten 1 bit respectively

If enabled:

Port 1 will get 3 bits ⇨ 0, 1, 2

Port 2 will get 3 bits ⇨ 3, 4, 5

Port 3 will get 2 bits ⇨ 6, 7

Example 3:

Assume that 6 ports are aggregated

8(bit)/6(port) = 1 (Integer) ⇨ each port is distributed 1 type of bit at least

8(bit)/6(port) = 2 (Remainder) ⇨ The first two ports will be additionally gotten 1 bit respectively

If enabled:

Port 1 will get 2 bits ⇨ 0, 1

Port 2 will get 2 bits ⇨ 2, 3

Port 3 will get 1 bit ⇨ 4

Port 4 will get 1 bit ⇨ 5

Port 5 will get 1 bit ⇨ 6

Port 6 will get 1 bit ⇨ 7

3. Disabling MAC Quotient

If MAC Quotient is disabled, 8 types of bit are distributed in order.

Example 1

Assume that 2 ports are aggregated

Port 1 will get 4 bits ⇨ 0, 2, 4, 6

Port 2 will get 4 bits ⇨ 1, 3, 5, 7

Example 2

Assume that 3 ports are aggregated

Port 1 will get 3 bits ⇨ 0, 3, 6

Port 2 will get 3 bits ⇨ 1, 4, 7

Port 3 will get 2 bits ⇨ 2, 5

3. 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 active		Set the selected interfaces to active LACP type.

2.5.6 Dot1X Command

The IEEE 802.1X/MAB 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.

Dot1x Command	Parameter	Description
Switch(config)# dot1x		Enable IEEE 802.1X/MAB 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		Enable radius-assigned vlan of the system.
Switch(config)# dot1x reauthentication		Enable auto reauthentication function of the system.
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 IPv4 address of RADIUS authentication server.
No command		
Switch(config)# no dot1x		Disable IEEE 802.1X/MAB function.
Switch(config)# no dot1x radius-assigned vlan		Disable radius-assigned vlan of the system.
Switch(config)# no dot1x reauthentication		Disable auto reauthentication function of the system.
Switch(config)# no dot1x secret		Remove the configured shared secret.
Switch(config)# no dot1x server		Remove the configured IPv4 address of RADIUS authentication server.
Show command		
Switch(config)# show dot1x		Show 802.1X/MAB system configuration.
Switch(config)# show dot1x interface		Show each interface’s 802.1X/MAB configuration.
Switch(config)# show dot1x interface [port_list]	[port_list]	Show the specified interfaces’ 802.1X/MAB configuration.
Switch(config)# show dot1x statistics		Show each port’s 802.1X/MAB statistics.
Switch(config)# show dot1x statistics clear		Clear all the interfaces’ 802.1X/MAB statistics.
Switch(config)# show dot1x statistics [port_list]	[port_list]	Show the specified interfaces’ 802.1X/MAB statistics.

Switch(config)# show dot1x statistics [port_list] clear	[port_list]	Clear the specified interfaces' 802.1X/MAB statistics.
Switch(config)# show dot1x status		Show all ports' 802.1X/MAB status.
Switch(config)# show dot1x status [port_list]	[port_list]	Show the specified interfaces' 802.1X/MAB status.
Examples of Dot1x command		
Switch(config)# dot1x		Enable IEEE 802.1X/MAB function.
Switch(config)# dot1x reauthentication		Enable auto reauthentication function of the system.
Switch(config)# dot1x secret agagabcxyz		Set the shared secret as "agagabcxyz".
Switch(config)# dot1x server 192.168.1.10		Set the RADIUS authentication server's IP address as 192.168.1.10.

Use "Interface" command to configure a group of ports' IEEE 802.1X/MAB settings.

Dot1x & 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)# dot1x mab		Enable MAC authentication bypass.
Switch(config-if-PORT-PORT)# dot1x max-req [1-10]	[1-10]	Configure EAP-request/identity retry times from switch to client before restarting the authentication process.
Switch(config-if-PORT-PORT)# dot1x port-control [auto | unauthorized]	[auto | unauthorized]	Specify the 802.1X/MAB port type "auto", "authorized" or "unauthorized" to the selected ports. **"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, both 802.1X-aware and 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-if-PORT-PORT)# dot1x radius-assigned vlan		Enable radius-assigned vlan of the specified port.
Switch(config-if-PORT-PORT)# dot1x reauthenticate		Re-authenticate the selected interfaces right now.
Switch(config-if-PORT-PORT)# dot1x reauthentication		Enable the selected ports' auto reauthentication function.
Switch(config-if-PORT-PORT)# dot1x timeout eap-timeout [1-255]	[1-255]	Specify EAP authentication timeout 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.
Switch(config-if-PORT-PORT)# dot1x timeout reauth-period [1-65535]	[1-65535]	Specify a period of reauthentication time that a client authenticates with the authentication server. The allowable value is between 1 and 65535 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 mab		Disable MAC authentication bypass.
Switch(config-if-PORT-PORT)# no dot1x max-req		Reset EAP-request/identity retry times back to the default. (2 times)
Switch(config-if-PORT-PORT)# no dot1x port-control		Reset the selected interfaces' 802.1X/MAB port type back to the default (authorized state).
Switch(config-if-PORT-PORT)# no dot1x radius-assigned vlan		Disable radius-assigned vlan of the specified port(s).
Switch(config-if-PORT-PORT)# no dot1x reauthentication		Disable the selected ports' auto reauthentication function.
Switch(config-if-PORT-PORT)# no dot1x timeout eap-timeout		Reset EAP authentication timeout value back to the default. (30 seconds).
Switch(config-if-PORT-PORT)# no dot1x timeout reauth-period		Reset EAP reauthentication period back to the default. (3600 seconds).
Examples of Dot1x & interface command		
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 up the selected ports to "auto" state.

Switch(config-if-1-3)# dot1x reauthenticate	Re-authenticate the selected interfaces immediately.

2.5.7 Fast-redundancy Command

Besides RSTP and Ring Detection, the employment of fast redundancy on your network will help protect mission-critical links against failures, avoids the occurrence of network loops, and keeps network downtime to a minimum to assure the reliability of the network. With these network redundancy, it allows the user to set up redundant loops in a network to provide a backup data transmission route in the event of the disconnection or damage of the cables. By means of this important feature in the network recovery applications, you can be totally free from any loss resulting from the time spent in locating the cable that fails to connect.

Fast redundancy provides **Fast Ring v2** and **Chain** two redundancy protocols, which allows you to configure 2 rings, 2 chains, or 1 ring & 1 chain at most for a switch.

Please note that all switches on the same ring or chain must be the ones with the same brand and configured using the same redundancy protocol when configuring a redundant ring or chain. You are not allowed to use switches with different brands or mix the Ring Detection, Fast Ring v2 and Chain protocols within the same ring or chain.

In the following table, it lists the difference among forementioned redundancy protocols for your evaluation when employing network redundancy on your network.

	Ring Detection	Fast Ring v2	Chain	RSTP
Topology	Ring	Ring	Ring	Ring
Recovery Time	<30 ms	<50 ms	<1 second (for copper ports) <50 ms (for fiber ports)	Up to 5 seconds

Fast Redundancy Command	Parameter	Description
Switch(config)# fast-redundancy id [group_id]	[1-2]	Create a fast redundancy group and assign it to an id number.
Switch(config-fr-ID)# description [description]	[description]	Enter a brief description for the specified fast redundancy group. Up to 35 alphanumeric characters can be accepted.
Switch(config-fr-ID)# enable		Enable the specified group of fast redundancy. **Note:**

		The port setting must be done beforehand to successfully enable the fast redundancy group.
Switch(config-fr-ID)# protocol [chain]	[chain]	Apply the Chain protocol on the specified group of fast redundancy.
Switch(config-fr-ID-chain)# chain-port1 interface [port_number] role [role] chain-port2 [disable]	[port_number]	Specify a single port to serve as the 1st interface of the Chain protocol. **Note:** **Each port can only be assigned to one single interface in the entire configuration of the fast redundancy.**
	[head | tail]	Assign a role to the 1st interface of the Chain protocol.
	[disable]	Disable the 2nd interface of the Chain protocol. Only when the role of the 1st interface of the Chain protocol is specified as either head or tail can the 2nd interface be disabled.
Switch(config-fr-ID-chain)# chain-port1 interface [port_number] role [role] chain-port2 interface [port_number] role [role]	[port_number]	Specify a single port to serve as the 1st interface of the Chain protocol. **Note:** **Each port can only be assigned to one single interface in the entire configuration of the fast redundancy.**
	[head | member | tail]	Assign a role to the 1st interface of the Chain protocol.
	[port_number]	Specify a single port to serve as the 2nd interface of the Chain protocol. **Note:** **Each port can only be assigned to one single interface in the entire configuration of the fast redundancy.**
	[member]	Assign a role to the 2nd interface of the Chain protocol. Only member is allowed.
Switch(config-fr-ID)# protocol [fast-ringv2] role [role]	[fast-ringv2]	Apply the Fast Ring v2 protocol on the specified group of fast redundancy.
	[master | slave]	Specify the role of the Managed Switch.

Switch(config-fr-ID-ringv2-ROLE)# ring-port1 interface [port_number] ring-port2 interface [port_number]	[port_number]	Specify a single port to serve as the 1st interface of the Fast Ring v2 protocol. **Note:** **Each port can only be assigned to one single interface in the entire configuration of the fast redundancy.**
	[port_number]	Specify a single port to serve as the 2nd interface of the Fast Ring v2 protocol. **Note:** **Each port can only be assigned to one single interface in the entire configuration of the fast redundancy.**
No Command		
Switch(config)# no fast-redundancy id [group_id]	[1-2]	Remove the specified fast redundancy group.
Switch(config-fr-ID)# no description		Remove the configured description for the specified fast redundancy group.
Switch(config-fr-ID)# no enable		Disable the specified group of fast redundancy.
Show Command		
Switch(config)# show fast-redundancy all		Show the current configuration, the topology change status, and the statistics of the entire fast redundancy function.
Switch(config)# show fast-redundancy id [group_id]	[1-2]	Show the current configuration of the specified fast redundancy group and the topology change status.
Switch(config)# show fast-redundancy id [group_id] statistics	[1-2]	Show the current configuration and the statistics of the specified fast redundancy group.
Switch(config)# show fast-redundancy id [group_id] statistics clear	[1-2]	Clear the statistics of the specified fast redundancy group.
Switch(config)# show fast-redundancy topology		Show the fast redundancy topology change status.
Switch(config)# show fast-redundancy topology clear		Clear the record of the fast redundancy topology change status.
Examples of Fast Redundancy Command		
Switch(config)# fast-redundancy id 1		Create a fast redundancy group and specify its ID to 1.

Switch(config-fr-1)# description 18F_office	Add a brief description “18F_office” to the fast redundancy group.
Switch(config-fr-1)# enable	Enable the fast redundancy group.
Switch(config-fr-1)# protocol chain	Apply the Chain protocol on the fast redundancy group.
Switch(config-fr-1-chain)# chain-port1 interface 10 role head chain-port2 disable	Specify the 10th port of the Managed Switch as the 1st interface and disable the 2nd interface of the chain protocol. And assign the 1st interface as the role of head.
Switch(config-fr-1-chain)# chain-port1 interface 6 role head chain-port2 interface 7 role member	Specify the 6th port of the Managed Switch as the 1st interface and the 7th port as the 2nd interface of the chain protocol, and assign the 1st interface as head, and the 2nd interface as member.
Switch(config-fr-1)# protocol fast-ringv2 role master	Apply the Fast Ring v2 protocol on the fast redundancy group, and specify the role of the Managed Switch as master.
Switch(config-fr-1-ringv2-master)# ring-port1 interface 5 ring-port2 interface 6	Specify the 5th port as the 1st interface of the Fast Ring v2 protocol, and the 6th port as the 2nd interface.

2.5.8 IP Command

1. To set up or remove the IP address of the Managed Industrial 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 Gigabit 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 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 snooping globally.

IGMP, Internet Group Management Protocol, 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 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.

Command / Example	Parameter	Description
Switch(config)# ip igmp snooping		Enable IGMP snooping function.
Switch(config)# ip igmp snooping aging-time [1-3000] 1/10 secs	[1-3000] 1/10 secs	Specify the IGMP querier aging time. If the switch does not receive join packets from the end device within the specified time, the entry associated with this end device will be removed from the IGMP table. The default setting is “1200” 1/10 seconds.
No command		

Switch(config)# no ip igmp snooping	Disable IGMP snooping function.
Switch(config)# no ip igmp snooping aging time	Remove IGMP querier aging time setting.
Show command	
Switch(config)# show ip igmp snooping	Show current IGMP snooping status including immediate leave function.
Switch(config)# show ip igmp snooping groups	Show IGMP group table. When IGMP Snooping is enabled, the Switch is able to read multicast group IP and the corresponding MAC address from IGMP packets that enter the device.

4. Enable or disable IGMP snooping immediate-leave function.

This works only when IGMP Snooping is enabled. When Immediate Leave is enabled, the Switch immediately removes the port when it detects IGMPv1 & IGMPv2 leave message on that port.

Command	Description
Switch(config)# ip igmp snooping immediate-leave	Enable IGMP immediate leave function.
No command	
Switch(config)# no ip igmp snooping immediate-leave	Disable IGMP immediate leave function.
Show command	
Switch(config)# show ip igmp snooping	Show current IGMP snooping status including immediate leave function.
Switch(config)# show ip igmp snooping groups	Show IGMP group table.

5. Configure multicast router ports.

Command	Parameter	Description
Switch(config)# ip igmp snooping mcast-router [port_list]	[port_list]	Specify multicast router ports.

6. Configure IGMP Snooping for specific VLAN

Command	Parameter	Description
Switch(config)# ip igmp snooping vlan [1-4094]	[1-4094]	Enable IGMP snooping for specific VLAN.
Switch(config)# ip igmp snooping vlan [1-4094] query		Enable querier for specific VLAN.
No Command		**Description**
Switch(config)# ip igmp snooping vlan [1-4094]	[1-4094]	Disable IGMP snooping for specific VLAN.
Switch(config)# ip igmp		Disable querier for specific VLAN.

snooping vlan [1-4094] query		
Show command		
Switch(config)# show ip igmp snooping		Show current IGMP snooping status.
Switch(config)# show ip igmp snooping groups		Show IGMP group table.

2.5.9 LLDP Command

LLDP stands for Link Layer Discovery Protocol and runs over data link layer. It is used for network devices to send information about themselves to other directly connected devices on the network. By using LLDP, two devices running different network layer protocols can learn information about each other. A set of attributes are used to discover neighbor devices. These attributes contains type, length, and value descriptions and are referred to TLVs. Details such as port description, system name, system description, system capabilities, and management address can be sent and received on this Managed Switch. Use Spacebar to select "ON" if you want to receive and send the TLV.

Command	Parameter	Description
Switch(config)# lldp hold-time [1-3600]	[1-3600]	Specify the amount of time in seconds. A receiving device will keep the information sent by your device for a period of time you specify here before discarding it. The allowable hold-time value is between 1 and 3600 seconds.
Switch(config)# lldp initiated-delay [0-300]	[0-300]	Specify a period of time the Managed Switch will wait before the initial LLDP packet is sent. The allowable initiated-delay value is between 0 and 300 seconds.
Switch(config)# lldp interval [1-180]	[1-180]	Specify the time interval for updated LLDP packets to be sent. The allowable interval value is between 1 and 180 seconds.
Switch(config)# lldp packets [1-16]	[1-16]	Specify the amount of packets that are sent in each discovery. The allowable packet value is between 1 and 16 seconds.
Switch(config)# lldp tlv-select capability		Enable Capability attribute to be sent.
Switch(config)# lldp tlv-select management-address		Enable Management Address attribute to be sent.
Switch(config)# lldp tlv-select port-description		Enable Port Description attribute to be sent.
Switch(config)# lldp tlv-select system-description		Enable System Description attribute to be sent.
Switch(config)# lldp tlv-select system-name		Enable System Name attribute to be sent.
No command		

Switch(config)# no lldp hold-time	Reset the hold-time value back to the default setting.
Switch(config)# no lldp initiated-delay	Reset the initiated-delay value back to the default setting.
Switch(config)# no lldp interval	Reset the interval value back to the default setting.
Switch(config)# no lldp packets	Reset the packets-to-be-sent value back to the default setting.
Switch(config)# no lldp tlv-select capability	Disable Capability attribute to be sent.
Switch(config)# no lldp tlv-select management-address	Disable Management Address attribute to be sent.
Switch(config)# no lldp tlv-select port-description	Disable Port Description attribute to be sent.
Switch(config)# no lldp tlv-select system-description	Disable System Description attribute to be sent.
Switch(config)# no lldp tlv-select system-name	Disable System Name attribute to be sent.
Show command	
Switch(config)# show lldp	Show or verify LLDP settings.
Switch(config)# show lldp interface	Show or verify each interface's LLDP port state.
Switch(config)# show lldp interface [port_list]	Show or verify the selected interfaces' LLDP port state.
Switch(config)# show lldp status	Show current LLDP status.
LLDP command example	**Description**
Switch(config)# lldp hold-time 60	Set the hold-time value to 60 seconds.
Switch(config)# lldp initiated-delay 60	Set the initiated-delay value to 60 seconds
Switch(config)# lldp interval 10	Set the updated LLDP packets to be sent in very 10 seconds.
Switch(config)# lldp packets 2	Set the number of packets to be sent in each discovery to 2.
Switch(config)# lldp tlv-select capability	Enable Capability attribute to be sent.
Switch(config)# lldp tlv-select management-address	Enable Management Address attribute to be sent.
Switch(config)# lldp tlv-select port-description	Enable Port Description attribute to be sent.
Switch(config)# lldp tlv-select system-description	Enable System Description to be sent.
Switch(config)# lldp tlv-select system-name	Enable System Name to be sent.

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

LLDP & 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)# lldp		Enable LLDP on the selected interfaces.
No command		
Switch(config-if-PORT-PORT)# no lldp		Disable LLDP on the selected interfaces.
Show command		
Switch(config)# show lldp		Show or verify LLDP configurations.

2.5.10 Loop Detection Command

In a real network, it is possible the people misconnect the network cable to incur loop condition. In a worst case, the network is out of service thereafter. This section gives a guide to configure the Loop Detection function of the system to prevent the system from loop.

After a proper setting of Loop Detection function, the system detects loop condition by periodically sending loop detection packet. Once the system receives the loop detection packet from itself, it is claimed that it detects loop condition. Then, the system takes the following 3 actions

1. It blocks the relevant port to prevent broadcast storms. In other words, the system stops forwarding all the traffic via the looped port. However, the system will process the loop detection packet received on the looped port.
2. It slowly blinks the LED of looped port in orange.
3. It periodically sends loop detection packet to detect the existence of loop condition.

When the system does not receives any loop detection packet from itself for a period of configured **Looped port unlock-interval**. The system claims the loop condition disappears. Then, the system takes the following 3 actions

1. It un-blocks the relevant port. In other words, the system normally forwards all the traffic via the relevant port.
2. It stops slowly blinking the LED of looped port in orange.
3. It periodically sends loop detection packet to detect the existence of loop condition.

***Note:** Under loop condition, the LED of looped port continues to slowly blink orange even the connected network cable is unplugged out of looped port.*

Command	Parameter	Description
Switch(config)# loop-detection		Enable Loop Detection function.
Switch(config)# loop-detection all-vlan		Check All VLAN box to enable loop detection on all trunk-VLAN-vid configured in VLAN Command (Section 2.6.23) ***NOTE:** When All VLAN check-box is checked, it invalidates the configured "Specific VLAN".*
Switch(config)# loop-detection interval [1-180]	[0-180]	This is the time interval (in seconds) that the device will periodically send

		loop detection packets to detect the presence of looped network. The valid range is from 1 to 180 seconds. The default setting is 1 seconds.
Switch(config)# loop-detection unlock-interval [1-1440]	[1-1440]	This is the time interval for the system to detect the existence of loop condition. System un-blocks the looped port if it does not receive any loop-detection packet during the configured unlock-interval. The unlock-interval can be set from 1 to 1440 minutes. The default setting is 1440 minutes. ***Note:*** *1. Be aware that Looped port unlock-interval converted into seconds should be greater than or equal to Detection Interval seconds multiplied by 10. The ‘10’ is a magic number which is for the system to claims the loop detection disappears when the system does not receive the loop-detection packet from itself at least 10 times. In general, it can be summarized by a formula below:* ***60* “Looped port unlock-interval” ≧ 10* “Detection Interval“*** *2. When a port is detected as a looped port, the system keeps the looped port in blocking status until loop situation is gone. In other words, the system stops forwarding all the traffic via the looped port. However, the system will process the loop-detection packet received on the looped port.*
Switch(config)# loop-detection vlan-id [1-4094]	[1-4094]	Set up loop detection on specified VLAN. The maximum number of VLAN ID is up to 4 sets. ***NOTE:*** *The configured “Specific VLAN” takes effect when All VLAN check-box is unchecked.*
No command		
Switch(config)# no loop-detection		Disable Loop Detection function.
Switch(config)# no loop-detection all-vlan		Disable loop detection on all trunk-VLAN-vid.

Switch(config)# no loop-detection interval		Reset Loop Detection time interval to default setting.
Switch(config)# no loop-detection unlock-interval		Reset Loop Detection unlock time interval to default setting.
Switch(config)# no loop-detection vlan-id		Disable loop detection on a specified VLAN.
Show command		
Switch(config)# show loop-detection		Show Loop Detection settings.
Switch(config)# show loop-detection status		Show Loop Detection status of all ports.
Switch(config)# show loop-detection status [port_list]	[port_list]	Show Loop Detection status of the ports.
Loop Detection command example		
Switch(config)# loop-detection interval 60		Set the Loop Detection time interval to 60 seconds.
Switch(config)# loop-detection unlock-interval 120		Set the Loop Detection unlock time interval to 120 minutes.
Switch(config)# loop-detection vlan-id 100		Set the Loop Detection VLAN ID to 100.

Use “Interface” command to configure a group of ports’ Loop Detection settings.

Dot1x & 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)# loop-detection		Enable Loop Detection function on the specific ports.
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 loop-detection		Disable Loop Detection function on the specific ports.

2.5.11 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-	[4-900]	Enter the aging time for the MAC address

table aging-time [4-900]		table. The available number is from 4 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 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.
Switch(config)# show mac address-table vlan-id [1-4094]	[1-4094]	Show the MAC status of specified VLAN ID.
Switch(config)# show mac static-mac		Show the static MAC address table.
MAC command example		
Switch(config)# mac address-table aging-time 600		Set the MAC address table aging time to 600 seconds.

Use “Interface” command to configure a group of ports’ MAC Table settings.

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

2.5.12 Management Command

Management Command	Parameter	Description
Switch(config)# management console timeout [1-1440]	[1-1440]	To disconnect the Managed Switch when console management is inactive for a certain period of time. The allowable value is from 1 to 1440 (seconds).

Switch(config)# management console timeout [1-1440] min	[1-1440]	To disconnect the Managed Switch when console management is inactive for a certain period of time. The allowable value is from 1 to 1440 (minutes).
Switch(config)# management ssh		Enable SSH management. To manage the Managed Switch via SSH.
Switch(config)# management telnet		Enable Telnet Management. To manage the Managed Switch via Telnet.
Switch(config)# management telnet port [1-65535]	[1-65535]	When telnet is enabled, you can set up the port number that allows telnet access. The default port number is set to 23. However, you can also identify a port number between 1 and 65535.
Switch(config)# management web		Enable Web management by the http method.
Switch(config)# management web timeout [1-1440]	[1-1440]	To disconnect the Managed Switch when web management is inactive for a certain period of time. The allowable value is from 1 to 1440 (minutes).
No command		
Switch(config)# no management console		Disable Console management.
Switch(config)# no management console timeout		Reset console timeout back to the default (300 seconds).
Switch(config)# no management ssh		Disable SSH management.
Switch(config)# no management telnet		Disable Telnet management.
Switch(config)# no management telnet port		Reset Telnet port back to the default. The default port number is 23.
Switch(config)# no management web		Disable Web management.
Switch(config)# no management web timeout		Reset web timeout value back to the default (20 minutes).
Show command		
Switch(config)# show management		Show the current management configuration of the Managed Switch.
Examples of Management command		
Switch(config)# management console timeout 300		The console management will timeout (logout automatically) when it is inactive for 300 seconds.
Switch(config)# management telnet		Enable Telnet management.
Switch(config)# management telnet port 23		Set Telnet port to port 23.

2.5.13 Mirror Command

Mirror command	Parameter	Description
Switch(config)# mirror mode [by-port]	[by-port]	Enable mirror mode by-port
Switch(config)# mirror source [port_list]	[port_list]	Specify the source port(s) to be mirrored
Switch(config)# mirror destination [port]	[port]	Specify the destination port for mirroring
No command		
Switch(config)# no mirror mode		Disable mirror mode
Show command		
Switch(config)# show mirror		Show port mirror information
Mirror command example		
Switch(config)# mirror mode by-port Switch(config)# mirror source 1-3 Switch(config)# mirror destination 4		Enable mirror mode and set port 4 as mirror destination and port 1-3 as source port.

2.5.14 NTP Command

Set up required configurations for Network Time Protocol.

Command	Parameter	Description
Switch(config)# ntp		Enable the Managed Industrial Gigabit 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 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 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 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.

2.5.15 QoS Command

1. Set up QoS

QoS command	Parameter	Description
Switch(config)# qos [802.1p | dscp]	[802.1p | dscp]	Specify QoS mode.
Switch(config)# qos dscp-map [0-63] [0-7]	[0-63]	Specify a DSCP bit value.
	[0-7]	Specify a queue value.
Switch(config)# qos management-priority [0-7]	[0-7]	Specify management default 802.1p bit.
Switch(config)# qos queuing-mode [weight]	[weight]	Specify QoS queuing mode as weight mode.

Switch(config)# qos queue-weighted [1:2:4:8:16:32:64:128]	[1:2:4:8:16:32:64:128]	Specify the queue weighted.
Switch(config)# qos remarking dscp		Globally enable DSCP remarking.
Switch(config)# qos remarking dscp-map [1-8]	[1-8]	Specify the DSCP and priority mapping ID.
Switch (config-dscp-map-ID)# new-dscp [0-63]	[0-63]	Specify the new DSCP bit value for the selected priority mapping ID.
Switch (config-dscp-map-ID)# rx-dscp [0-63]	[0-63]	Specify the received DSCP bit value for the selected priority mapping ID.
Switch(config)# qos remarking 802.1p		Globally enable 802.1p remarking.
Switch(config)# qos remarking 802.1p-map [1-8]	[1-8]	Specify the 802.1p and priority mapping ID.
Switch (config-802.1p-map-ID)# priority [0-7]	[0-7]	Specify the new 802.1p bit value for the selected priority mapping ID.
Switch(config)# qos 802.1p-map [0-7] [0-7]	[0-7]	Specify an 802.1p bit value.
	[0-7]	Specify a queue value.
No command		
Switch(config)# no qos		Disable QoS function.
Switch(config)# no qos dscp-map [0-63]	[0-63]	Reset the specified DSCP bit value back to the default queue value (Q(0)).
Switch(config)# no qos management-priority		Reset management 802.1p bit back to the default (0).
Switch(config)# no qos queuing-mode		Specify QoS queuing mode as strict mode.
Switch(config)# no qos queue-weighted		Reset the queue weighted value back to the default.
Switch(config)# no qos remarking dscp		Globally disable DSCP remarking.
Switch(config)# no qos remarking dscp-map [1-8]	[1-8]	Reset the DSCP remaking for the specified priority mapping ID back to the default.
Switch (config-dscp-map-ID)# no new-dscp		Reset the new DSCP bit value for the selected priority mapping ID back to the default.
Switch (config-dscp-map-ID)# no rx-dscp		Reset the received DSCP bit value for the selected priority mapping ID back to the default.
Switch(config)# no qos remarking 802.1p		Globally disable 802.1p remarking.
Switch(config)# no qos remarking 802.1p-map [1-8]	[1-8]	Reset the 802.1p remaking for the specified priority mapping ID back to the default.

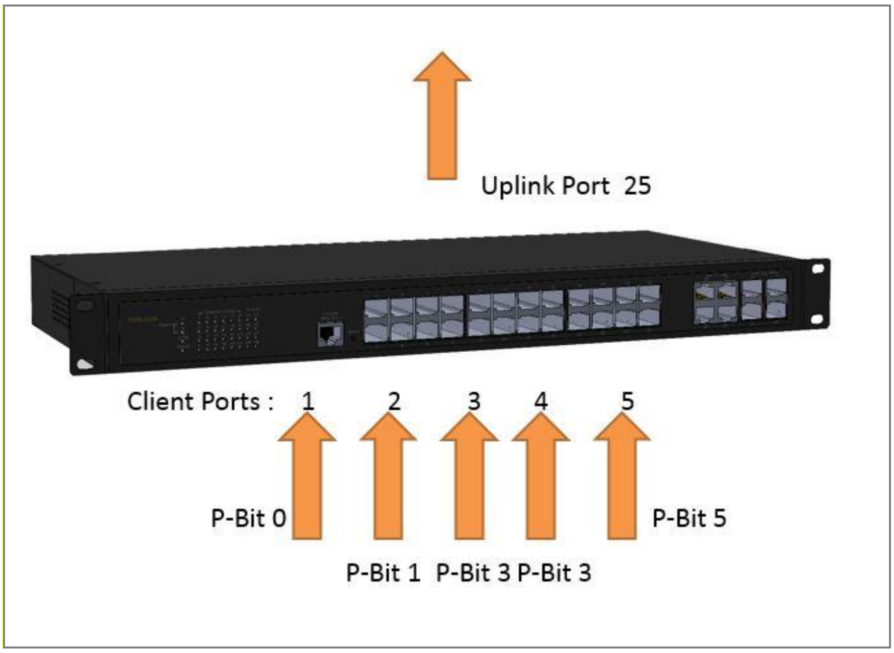
Switch (config-802.1p-map-ID)# no priority		Reset the new 802.1p bit value for the selected priority mapping ID back to the default.
Switch(config)# no qos 802.1p-map [0-7]	[0-7]	Reset the specified 802.1p bit value back to the default queue value (Q(0)).
Show command		
Switch(config)# show qos		Show QoS configuration.
Switch(config)# show qos interface		Show QoS interface overall information.
Switch(config)# show qos interface [port-list]	[port-list]	Show the selected QoS interface information.
Switch(config)# show qos remarking		Show QoS remarking information.
Switch (config-dscp-map-ID)# show		Show the DSCP mapping configuration for the selected priority mapping ID.
Switch (config-802.1p-map-ID)# show		Show the 802.1p mapping configuration for the selected priority mapping ID.

2. Use “interface” command to configure a group of ports’ QoS settings.

QoS & 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)# qos rate-limit ingress [0,500-1000000]	[0,500-1000000] kbps	Specify the ingress rate limit value. 0:Disable
Switch(config-if-PORT-PORT)# qos rate-limit egress [0,500-1000000]	[0,500-1000000] kbps	Specify the egress rate limit value. 0:Disable
Switch(config-if-PORT-PORT)# qos user-priority [0-7]	[0-7]	Specify the default priority bit (P-bit) to the selected interfaces.
No command		
Switch(config-if-PORT-PORT)# no qos rate-limit ingress		Disable QoS ingress rate limit setting.
Switch(config-if-PORT-PORT)# no qos rate-limit egress		Disable QoS egress rate limit setting.
Switch(config-if-PORT-PORT)# no qos user-priority		Reset the user priority value setting back to the default.

For QoS configuration via CLI, we take a 28-port Managed Switch for example to let the users have a clear understanding of these QoS commands.

Under this network environment, the Managed Switch will be configured as Table 1. Port 1-5 are client ports and Port 25 is the uplink port of the device. Client ports will receive the data traffic with different VLAN P-bit value. Port 3, Port 4 and Port 5 are also limited to specified bandwidth in the different rate limit in ingress and egress.



QoS Mode: 802.1p; Egress Mode: Weight; Port 25: Uplink Port. Queue-Weighted: 1(Q0):2(Q1):3(Q2):4(Q3):5(Q4):6(Q5):7(Q6):8(Q7)					
802.1p Priority Map	**P-Bit**	**Queue Mapping**	**Ingress Rate**	**Egress Rate**	**Remark**
Port 1	0	Q0	Default	Default	The rest of P-Bits are default value.
Port 2	1	Q1	Default	Default	
Port 3	3	Q2	10000	10000	
Port 4	3	Q2	10000	10000	
Port 5	5	Q3	1G	1G	

Table 1

Below is the complete CLI commands applied to a Managed Switch.

Command		**Purpose**
STEP1	**configure** **Example:** Switch# config	**Enter the global configuration mode.**

	Switch(config)#	
STEP2	qos 802.1p **Example:** Switch(config)# qos 802.1p OK !	**In this example, it configures the QoS Mode to 802.1p.**
STEP3	qos queuing-mode weight **Example:** Switch(config)# qos queuing-mode weight **OK !**	**In this example, it configures Configure Egress Mode as "Weight".**
STEP4	qos queue-weighted *weighted* **Example:** Switch(config)# qos queue-weighted 1:2:3:4:5:6:7:8 OK !	**In this example, it configures the Queue Weighted to : 1(Q0):2(Q1):3(Q2):4(Q3): 5(Q4):6(Q5):7(Q6):8(Q7).**
STEP5	qos 802.1p-map *802.1p_list queue_value* **Example:** Switch(config)# qos 802.1p-map 0 0 Switch(config)# qos 802.1p-map 1 1 Switch(config)# qos 802.1p-map 3 2 Switch(config)# qos 802.1p-map 5 3	**In this example, it configures the P-Bit 0 with Queue Mapping to Q0, the P-Bits 1 with Queue Mapping to Q1, the P-Bits 3 with Queue Mapping to Q2, and the P-Bit 5 with Queue Mapping to Q3.**
STEP6	interface *port_list* **Example:** Switch(config)# interface 1 Switch(config-if-1)#	**Specify the Port 1 that you would like to configure P-Bit.**
STEP7	qos user-priority *P-Bit* **Example:** Switch(config-if-1)# qos user-priority 0	**In this example, it configures P-Bit value as 0 for Port 1.**
STEP8	exit **Example:** Switch(config-if-1)# exit Switch(config)#	**Return to the global configuration mode.**
STEP9	interface *port_list* **Example:** Switch(config)# interface 2 Switch(config-if-2)#	**Specify the Port 2 that you would like to configure P-Bit.**
STEP10	qos user-priority *P-Bit* **Example:** Switch(config-if-2)# qos user-priority 1	**In this example, it configures P-Bit value as 1 for Port 2.**

STEP11	exit **Example:** Switch(config-if-2)# exit Switch(config)#	**Return to the global configuration mode.**
STEP12	interface *port_list* **Example:** Switch(config)# interface 3, 4 Switch(config-if-3,4)#	**Specify the Port 3 and Port 4 that you would like to configure QoS Rate limit.**
STEP13	qos rate-limit ingress *limit_rate(kbps)* **Example:** Switch(config-if-3,4)# qos rate-limit ingress 10000 OK !	**In this example, it configures Port 3 and Port 4 with 10M Ingress Rate.**
STEP14	qos rate-limit egress *limit_rate(kbps)* **Example:** Switch(config-if-3,4)# qos rate-limit egress 10000 OK !	**In this example, it configures Port 3 and Port 4 with 10M Egress Rate.**
STEP15	qos user-priority *P-Bit* **Example:** Switch(config-if-3,4)# qos user-priority 3	**In this example, it configures P-Bit value as 3 for Port 3 and Port 4.**
STEP16	exit **Example:** Switch(config-if-3,4)# exit Switch(config)#	**Return to the global configuration mode.**
STEP17	interface *port_list* **Example:** Switch(config)# interface 5 Switch (config-if-5)#	**Specify the Port 5 that you would like to configure QoS Rate limit.**
STEP18	qos rate-limit ingress *limit_rate(kbps)* **Example:** Switch(config-if-5)# qos rate-limit ingress 1000000 OK !	**In this example, it configures Port 5 with 1G Ingress Rate.**
STEP19	qos rate-limit egress *limit_rate(kbps)* **Example:** Switch(config-if-5)# qos rate-limit egress 1000000 OK !	**In this example, it configures Port 5 with 1G Engress Rate.**

STEP20	qos user-priority *P-Bit* **Example:** Switch(config-if-5)# qos user-priority 5	**In this example, it configures P-Bit value as 5 for Port 5.**
STEP21	exit **Example:** Switch(config-if-5)# exit Switch(config)#	**Return to the global configuration mode.**
STEP22	exit **Example:** Switch(config)# exit Switch#	**Return to the Privileged mode.**
STEP23	write **Example:** Switch# write Save Config Succeeded!	**Save the running configuration into the startup configuration.**

After completing the QoS settings for your Managed switches, you can issue the commands listed below for checking your configuration

Example 1,

Switch(config)# show qos

```
==========================================================================
QoS Information
==========================================================================
QoS Mode    : 802.1p
Egress Mode : weight
Weight          : 1:2:3:4:5:6:7:8

Press Ctrl-C to exit or any key to continue!

Tag  Priority
-----  --------
  0      Q0
  1      Q1
  2      Q0
  3      Q2
  4      Q0
  5      Q3
  6      Q0
  7      Q0

Press Ctrl-C to exit or any key to continue!


DSCP  Priority   DSCP  Priority   DSCP  Priority   DSCP  Priority
--------  ----------  ---------  ---------   --------- ---------   ---------  --------
      0      Q0          1      Q0          2       Q0        3         Q0
      4      Q0          5      Q0          6       Q0        7         Q0
      8      Q0          9      Q0        10       Q0       11         Q0
    12      Q0        13      Q0        14       Q0       15         Q0
    16      Q0        17      Q0        18       Q0       19         Q0
    20      Q0        21      Q0        22       Q0       23         Q0
    24      Q0        25      Q0        26       Q0       27         Q0
    28      Q0        29      Q0        30       Q0       31         Q0

Press Ctrl-C to exit or any key to continue!

   32      Q0          33      Q0         34       Q0        35         Q0
   36      Q0          37      Q0         38       Q0        39         Q0
   40      Q0          41      Q0         42       Q0        43         Q0
   44      Q0          45      Q0         46       Q0        47         Q0
   48      Q0          49      Q0         50       Q0        51         Q0
   52      Q0          53      Q0         54       Q0        55         Q0
   56      Q0          57      Q0         58       Q0        59         Q0
   60      Q0          61      Q0         62       Q0        63         Q0
```

Example 2,

Switch(config)# show vlan interface

```
==========================================================================
IEEE 802.1q Tag VLAN Interface :
==========================================================================
Dot1q-Tunnel EtherType : : 0x9100
Port   Access-vlan   User Priority  Port VLAN Mode    Trunk-vlan
------ ------------- ------------- ------------------ -----------
   1             1              0     access             1
   2             1              1     access             1
   3             1              3     access             1
   4             1              3     access             1
   5             1              5     access             1
   6             1              0     access             1
   7             1              0     access             1
   8             1              0     access             1
   9             1              0     access             1
  10             1              0     access             1

Press Ctrl-C to exit or any key to continue!

  11            1               0     access             1
  12            1               0     access             1
  13            1               0     access             1
  14            1               0     access             1
  15          . 1               0     access             1
  16            1               0     access             1
  17            1               0     access             1
  18            1               0     access             1
  19            1               0     access             1
  20            1               0     access             1

Press Ctrl-C to exit or any key to continue!

21              1               0     access             1
22              1               0     access             1
23              1               0     access             1
24              1               0     access             1
25              1               0     access             1
26              1               0     access             1
27              1               0     access             1
28              1               0     access             1

Switch(config)#
```

Example 3,

Switch(config)# show qos interface

```
========================================================================
QoS port Information :
========================================================================
Port                     : 1
Ingress Rate Limiter : disable
Egress Rate Limiter  : disable

Press Ctrl-C to exit or any key to continue!

Port                     : 2
Ingress Rate Limiter : disable
Egress Rate Limiter  : disable

Press Ctrl-C to exit or any key to continue!

Port                      : 3
Ingress Rate Limiter :   10 Mbps
Egress Rate Limiter  :   10 Mbps

Press Ctrl-C to exit or any key to continue!

Port                      : 4
Ingress Rate Limiter :   10 Mbps
Egress Rate Limiter  :   10 Mbps

Press Ctrl-C to exit or any key to continue!

Port                      : 5
Ingress Rate Limiter : 1000 Mbps
Egress Rate Limiter  : 1000 Mbps

Press Ctrl-C to exit or any key to continue!

Port                     : 6
Ingress Rate         er : disable
Egress Rate   :   :  r  : disable
              :   :
Press Ctrl-C  :   :   or any key to continue!


Port                      : 28
Ingress Rate Limiter : disable
Egress Rate Limiter  : disable

Switch(config)#
```

2.5.16 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 | auto-backup | cold-start | fast-redundancy | port-link | power-failure | warm-start]	[all | auth-fail | auto-backup | cold-start | fast-redundancy | port-link | power-failure | 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. **auto-backup:** A trap will be sent when the auto backup succeeds or fails. **cold-start:** A trap will be sent when the device boots up. **fast-redundancy:** A trap will be sent when any specified redundancy port in fast redundancy is link up/link down. **port-link:** A trap will be sent when the link is up or down. **power-failure:** A trap will be sent when the power 1/2 failure occurs or when either one is back on. **warm-start:** A trap will be sent when the device restarts.
No command		
Switch(config)# no snmp-server trap-type [all | auth-fail | auto-backup | cold-start | fast-redundancy | port-link | power-failure | warm-start]	[all | auth-fail | auto-backup | cold-start | fast-redundancy | port-link | power-failure | warm-start]	Specify a trap type that will not be sent when a certain situation occurs.
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.

2.5.17 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 Protocol function on aggregated ports.
Switch(config)# spanning-tree aggregated-port cost [0-200000000]	[0-200000000]	Specify aggregated ports' path cost. The default value is "1".
Switch(config)# spanning-tree aggregated-port priority [0-15]	[0-15]	Specify aggregated ports' priority. The default setting is "8". **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. The default value is "4" 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. The default value is "1" second.
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. The default value is "6" seconds.
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. The default value is "8". **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-		Reset aggregated ports' cost to the

tree aggregated-port cost		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.
Switch(config)# no spanning-tree priority		Reset the priority value on a per switch basis back to the default.
Switch(config)# no spanning-tree version		Reset the RSTP version back to the 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 [0-200000000]	[0-200000000]	Specify cost value on the selected interfaces. The default setting is "0".
Switch(config-if-PORT-PORT)# spanning-tree priority [0-15]	[0-15]	Specify priority value on the selected interfaces. **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-if-PORT-PORT)# spanning-tree edge		Set the selected interfaces to edge ports.

Switch(config-if-PORT-PORT)# spanning-tree 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). **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.
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.

2.5.18 Switch Command

Switch command	Description
Switch(config)# switch statistics polling	Enable the Switch to refresh the counter information and current state in a fixed interval.
No command	
Switch(config)# no switch statistics polling	Disable the Switch to refresh the counter information and current state in a fixed interval.

2.5.19 Switch-info Command

To set up the Managed Industrial 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 Switch.
Switch(config)# switch-info system-location [system_location]	[system_location]	Enter a brief description of the Managed Industrial 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 Switch. Use a descriptive name to identify the Managed Industrial 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 Switch. By default, the hostname prompt shows the model name of this Managed Industrial 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”.

2.5.20 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.

2.5.21 Security Command

When a device on the network is malfunctioning or application programs are not well designed or properly configured, broadcast storms may occur, network performance may be degraded or, in the worst situation, a complete halt may happen. The Managed Switch allows users to set a threshold rate for broadcast traffic on a per switch basis so as to protect network from broadcast storms. Any broadcast packets exceeding the specified value will then be dropped.

Enable or disable broadcast storm control.

Security command	Parameter	Description
Switch(config)# security storm-protection		Globally enable the storm control function.
Switch(config)# security storm-protection rates [64-1000000]	[64-1000000] kbps	To set up the maximum packet rate of each port. The allowable value is between 64 and 1000000 kbps.
No command		
Switch(config)# no security storm-protection		Globally disable the storm control function.
Switch(config)# no security storm-protection rates		Reset the maximum packet rate of each port back to the default. (256 kbps)
Show command		
Switch(config)# show security storm-protection		Show the current storm control configuration.

2.5.22 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.

2.5.23 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.

2.5.24 VLAN Command

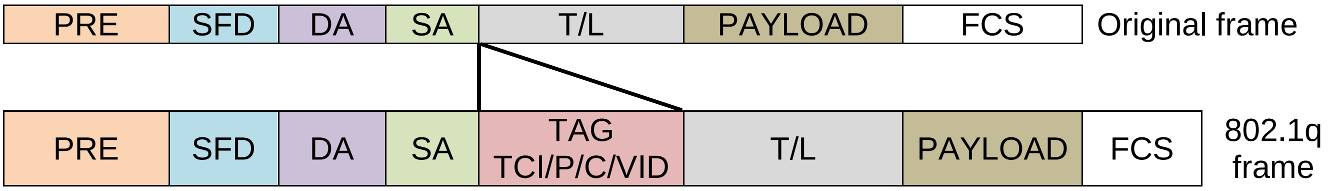
A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast 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	[1-4094]	Specify the selected ports' Trunk-

dot1q-vlan trunk-vlan [1-4094]		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.

2.5.25 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. Set up LACP configuration

Command	Parameter	Description
Switch(config-if-PORT-PORT)# channel-group lacp		Enable LACP on the selected interfaces.
Switch(config-if-PORT-PORT)# channel-group lacp key [0-255]	[0-255]	Specify a key to the selected interfaces.
Switch(config-if-PORT-PORT)# channel-group lacp type [active]	[active]	Specify the selected interfaces to active LACP role.
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-	[port_list]	Show or verify the selected interfaces’

group lacp status [port_list]		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.

5. **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).

6. **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.

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

Dot1x & Interface command	Parameter	Description
Switch(config-if-PORT-PORT)# dot1x mab		Enable MAC authentication bypass.
Switch(config-if-PORT-PORT)# dot1x max-req [1-10]	[1-10]	Configure EAP-request/identity retry times from switch to client before restarting the authentication process.
Switch(config-if-PORT-PORT)# dot1x port-control [auto | unauthorized]	[auto | unauthorized]	Specify the 802.1X/MAB port type "auto", "authorized" or "unauthorized" to the selected ports. **"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, both 802.1X-aware and 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-if-PORT-PORT)# dot1x radius-assigned vlan		Enable radius-assigned vlan of the specified port.
Switch(config-if-PORT-PORT)# dot1x reauthenticate		Re-authenticate the selected interfaces right now.
Switch(config-if-PORT-PORT)# dot1x reauthentication		Enable the selected ports’ auto reauthentication function.
Switch(config-if-PORT-PORT)# dot1x timeout eap-timeout [1-255]	[1-255]	Specify EAP authentication timeout 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.
Switch(config-if-PORT-PORT)# dot1x timeout reauth-period [1-65535]	[1-65535]	Specify a period of reauthentication time that a client authenticates with the authentication server. The allowable value is between 1 and 65535 seconds.
No command		
Switch(config-if-PORT-PORT)# no dot1x mab		Disable MAC authentication bypass.
Switch(config-if-PORT-PORT)# no dot1x max-req		Reset EAP-request/identity retry times back to the default. (2 times)
Switch(config-if-PORT-PORT)# no dot1x port-control		Reset the selected interfaces’ 802.1X/MAB port type back to the default (authorized state).
Switch(config-if-PORT-PORT)# no dot1x radius-assigned vlan		Disable radius-assigned vlan of the specified port(s).
Switch(config-if-PORT-PORT)# no dot1x reauthentication		Disable the selected ports’ auto reauthentication function.
Switch(config-if-PORT-PORT)# no dot1x timeout eap-timeout		Reset EAP authentication timeout value back to the default. (30 seconds).
Switch(config-if-PORT-PORT)# no dot1x timeout reauth-period		Reset EAP reauthentication period back to the default. (3600 seconds).
Examples of Dot1x & interface command		
Switch(config-if-1-3)# dot1x port-control auto		Set up the selected ports to “auto”

	state.
Switch(config-if-1-3)# dot1x reauthenticate	Re-authenticate the selected interfaces immediately.

8. To set up LLDP:

Command	Parameter	Description
Switch(config-if-PORT-PORT)# lldp		Enable LLDP function.
No command		
Switch(config-if-PORT-PORT)# no lldp		Disable LLDP function.

9. To set up loop detection:

Command	Parameter	Description
Switch(config-if-PORT-PORT)# loop-detection		Enable loop detection on port(s).
No command		
Switch(config-if-PORT-PORT)# no loop-detection		Disable loop detection on port(s).

10. To configure QoS

Command	Parameter	Description
Switch(config-if-PORT-PORT)# qos rate-limit ingress [0,500-1000000]	[0,500-1000000] kbps	Specify the ingress rate limit value. 0:Disable
Switch(config-if-PORT-PORT)# qos rate-limit egress [0,500-1000000]	[0,500-1000000] kbps	Specify the egress rate limit value. 0:Disable
Switch(config-if-PORT-PORT)# qos user-priority [0-7]	[0-7]	Specify the default priority bit (P-bit) to the selected interfaces.
No command		
Switch(config-if-PORT-PORT)# no qos rate-limit ingress		Disable QoS ingress rate limit setting.
Switch(config-if-PORT-PORT)# no qos rate-limit egress		Disable QoS egress rate limit setting.
Switch(config-if-PORT-PORT)# no qos user-priority		Reset the user priority value setting back to the default.

11. To shutdown the selected interface:

Command	Parameter	Description
Switch(config-if-PORT-PORT)#		Administratively disable the selected

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

12. 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.

13. 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-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.

14. To set RSTP configuration

Command	Parameter	Description
Switch(config-if-PORT-PORT)# spanning-tree		Enable spanning-tree protocol.
Switch(config-if-PORT-PORT)# spanning-tree cost [0-200000000]	[0-200000000]	Specify ports' path cost. The default value is "0".
Switch(config-if-PORT-PORT)# spanning-tree priority [0-15]	[0-15]	Specify bridge 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-if-PORT-PORT)# spanning-tree edge		Enable ports to shift to forwarding state when the link is up.
Switch(config-if-PORT-PORT)# spanning-tree 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). **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.
No command		
Switch(config-if-PORT-PORT)# no spanning-tree		Disable spanning-tree
Switch(config-if-PORT-PORT)# no spanning-tree cost		Clear the cost of ports specified.
Switch(config-if-PORT-PORT)# no spanning-tree priority		Cancel the priority specified.
Switch(config-if-PORT-PORT)# no spanning-tree edge		Disable ports to shift to forwarding state when the link is up.
Switch(config-if-PORT-PORT)# no spanning-tree p2p		Disable the type of ports specified.

15. 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 [1-4094]	[xx:xx:xx:xx:xx:xx:]	Specify a static MAC address
	[1-4094]	Specify VLAN ID
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:xx:]	Delete static MAC address entry
	[1-4094]	

2.5.26 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.

2.5.27 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.

2.5.28 show log command

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

2.5.29 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 Switch by the factory.
Switch(config)# show running-config	Display the configurations currently used in the Managed Industrial 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.

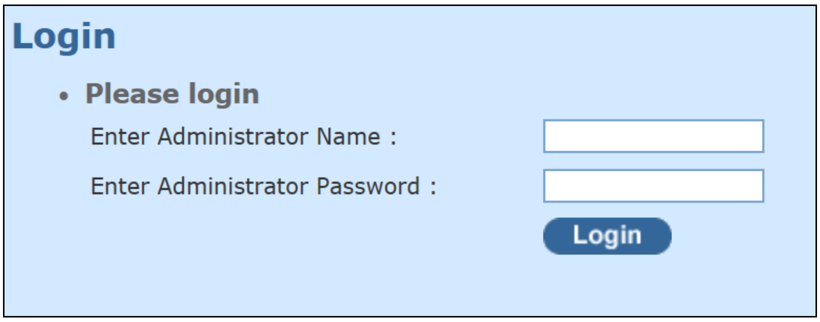
3. WEB MANAGEMENT

The Managed Industrial Switch can be managed via a Web browser. The default IP of the Managed Industrial 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 Switch through a Web browser:

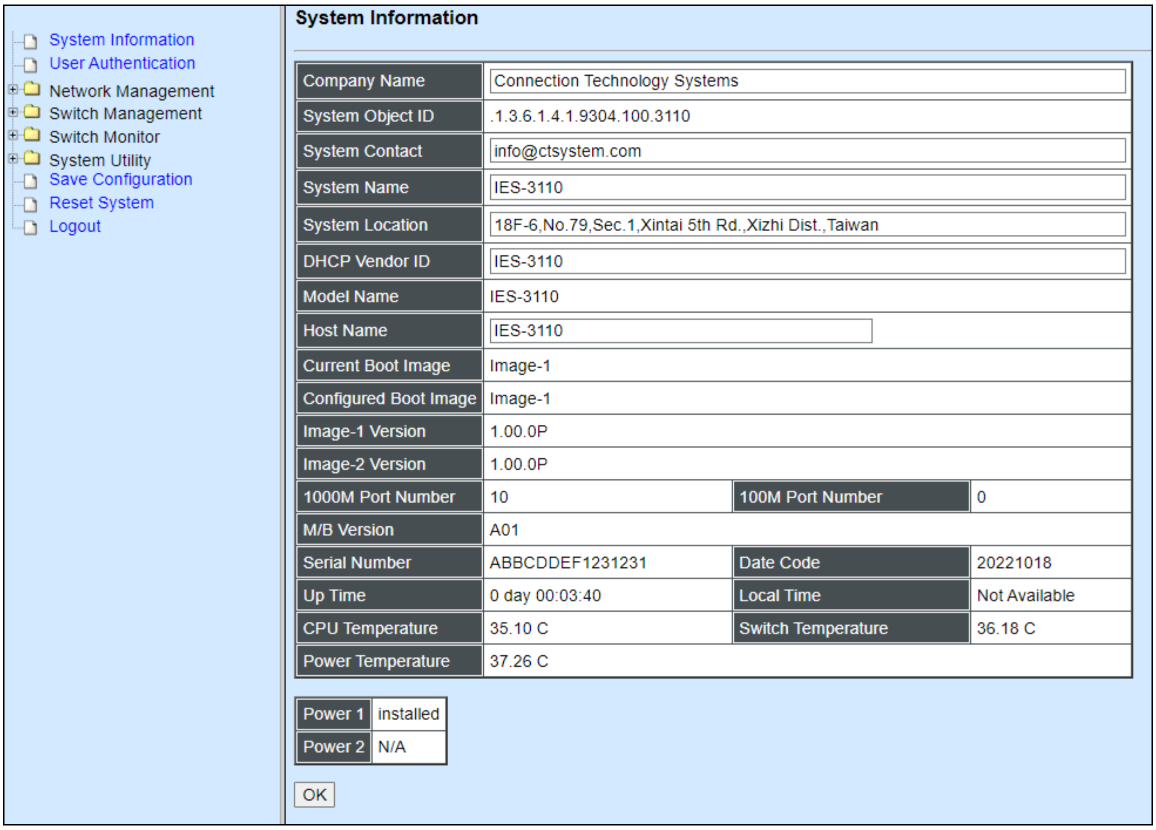
1. Use the RS-232 RJ-45 console port or one of the 10/100/1000Base-T RJ-45 ports (as the temporary RJ-45 Management console port) to login the Managed Industrial Switch and set up the assigned IP parameters including the following:
   - IP address
   - Subnet Mask
   - Default Gateway IP address, if required
2. Run a Web browser and specify the Managed Industrial Switch's IP address to reach it. (The Managed Industrial Switch can be reached at **"http://192.168.0.1"** before any change.)
3. Login to the Managed Industrial 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	.1.3.6.1.4.1.9304.100.3110
System Contact	info@ctsystem.com
System Name	IES-3110
System Location	18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan
DHCP Vendor ID	IES-3110
Model Name	IES-3110
Host Name	IES-3110
Current Boot Image	Image-1
Configured Boot Image	Image-1
Image-1 Version	1.00.0P
Image-2 Version	1.00.0P
1000M Port Number	10	100M Port Number	0
M/B Version	A01
Serial Number	ABBCDDEF1231231	Date Code	20221018
Up Time	0 day 00:03:40	Local Time	Not Available
CPU Temperature	35.10 C	Switch Temperature	36.18 C
Power Temperature	37.26 C

Power 1	installed
Power 2	N/A

1. **System Information:** Name the Managed Industrial 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 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.

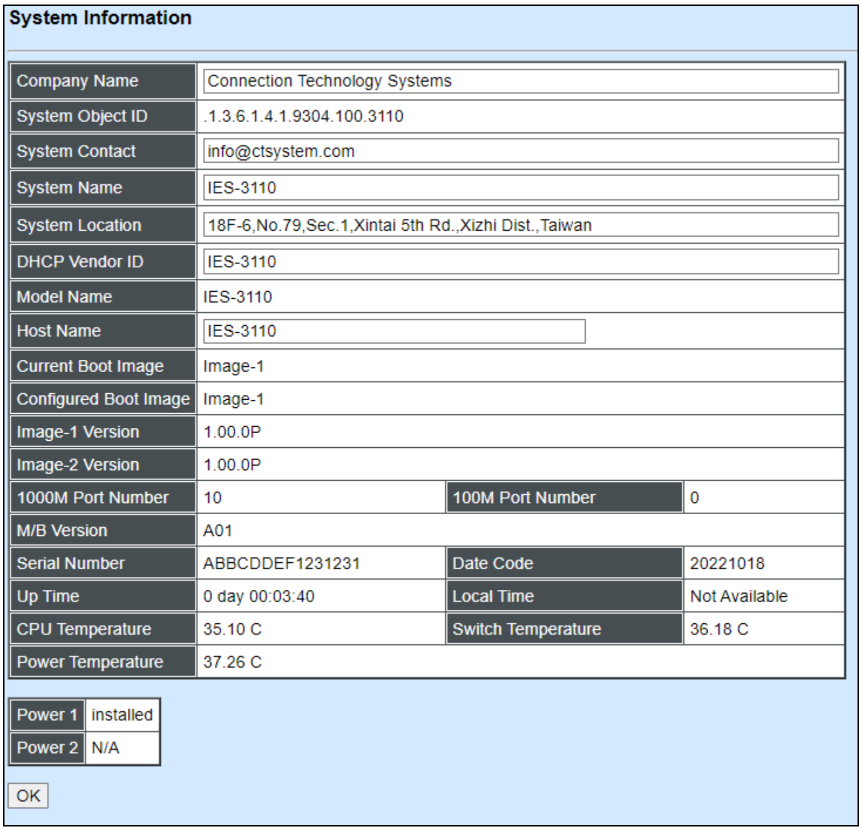
7. **Save Configuration:** Save all changes to the system.

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

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

3.1 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	.1.3.6.1.4.1.9304.100.3110		
System Contact	info@ctsystem.com		
System Name	IES-3110		
System Location	18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan		
DHCP Vendor ID	IES-3110		
Model Name	IES-3110		
Host Name	IES-3110		
Current Boot Image	Image-1		
Configured Boot Image	Image-1		
Image-1 Version	1.00.0P		
Image-2 Version	1.00.0P		
1000M Port Number	10	100M Port Number	0
M/B Version	A01		
Serial Number	ABBCDDEF1231231	Date Code	20221018
Up Time	0 day 00:03:40	Local Time	Not Available
CPU Temperature	35.10 C	Switch Temperature	36.18 C
Power Temperature	37.26 C		

Power 1	installed
Power 2	N/A

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

System Name: Enter a unique name up to 55 alphanumeric characters for this Managed Industrial Switch. Use a descriptive name to identify the Managed Industrial 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 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 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

Switch Temperature: View-only field that shows the current temperature of the switch

Power Temperature: View-only field that shows the current temperature of the power in use

Power 1: View-only field that shows the status of Power 1

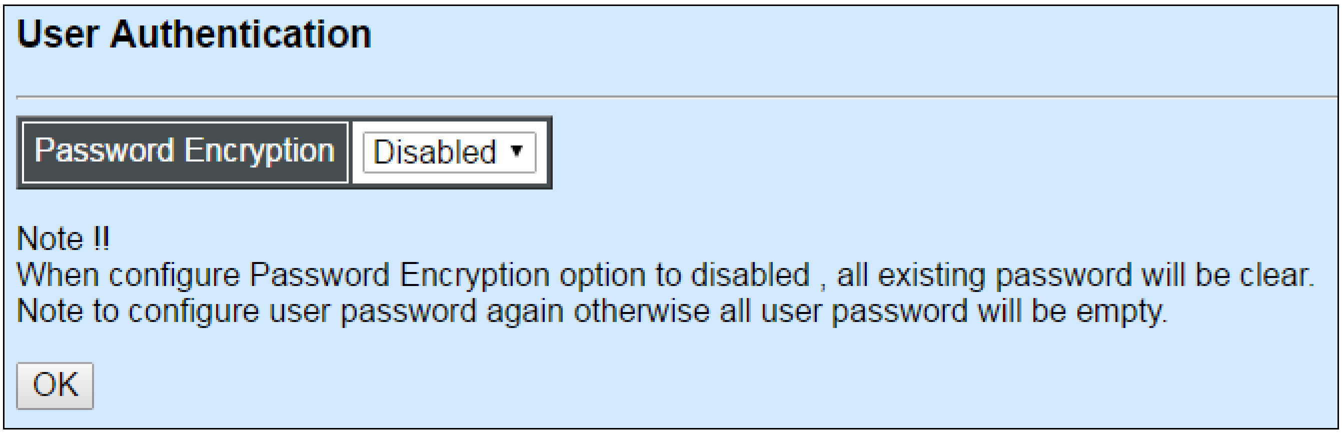
Power 2: View-only field that shows the status of Power 2

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

3.2 User Authentication

To prevent any un-authorized access, only registered users are allowed to access the Managed Industrial Switch. Users who want to access the Managed Industrial 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.

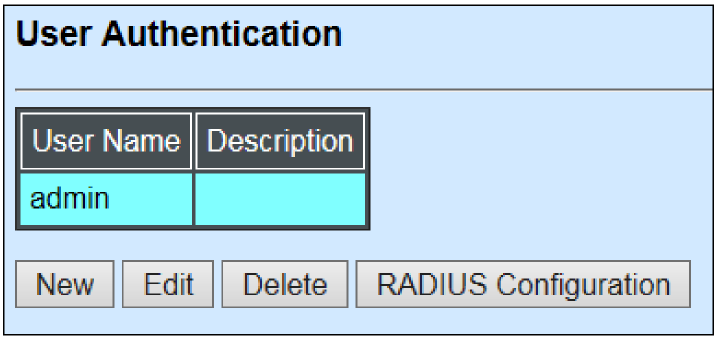


User Authentication

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.



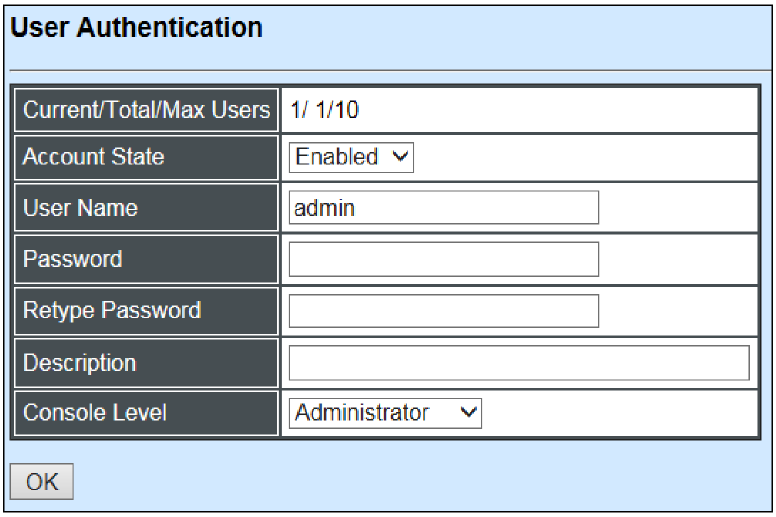
User Authentication

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	1/ 1/10
Account State	Enabled
User Name	admin
Password	
Retype Password	
Description	
Console Level	Administrator

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.

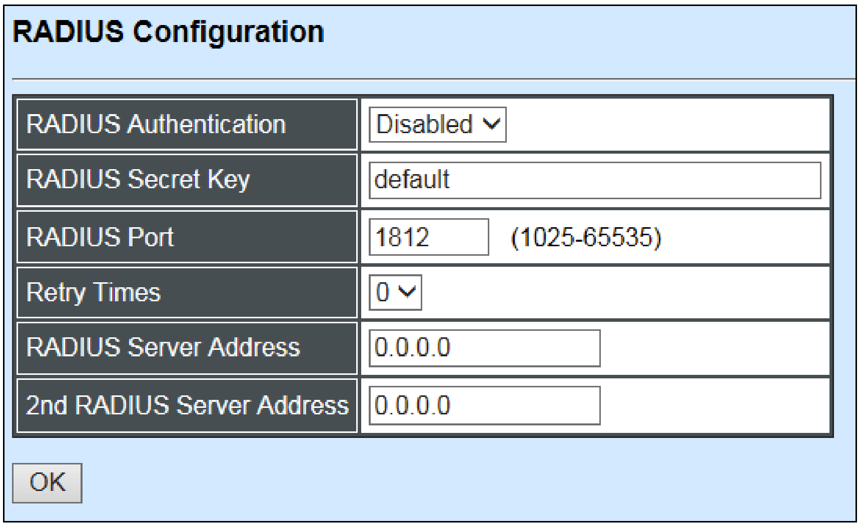
Read Only: Read only access right.

NOTE: *If you forget the login password, the only way to gain access to the Web Management is to set the Managed Industrial 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 Switch.). When the Managed Industrial 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.*

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”.

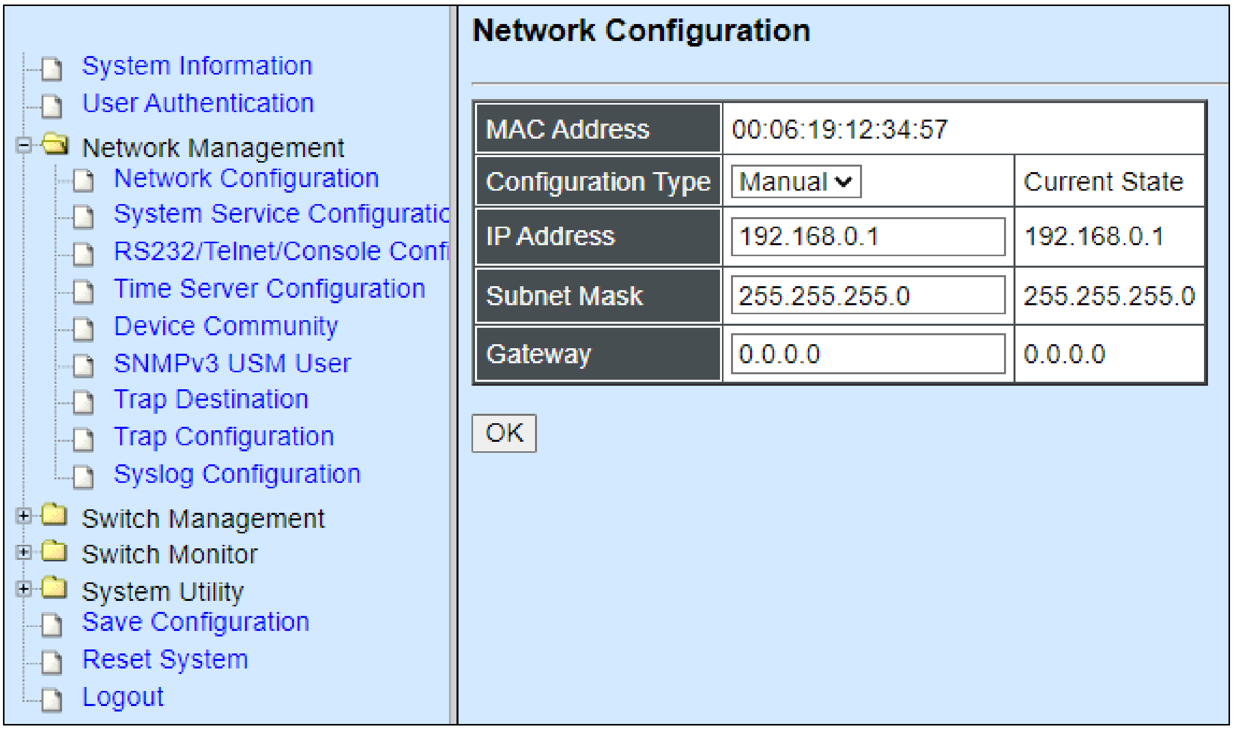
Retry Time: Times of trying to reconnect if the RADIUS server is not reachable. The default value is “0”.

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

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

3.3 Network Management

In order to enable network management of the Managed Industrial 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	00:06:19:12:34:57	
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 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. **Device Community:** View the registered SNMP community name list. Add a new community name or remove an existing community name.

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

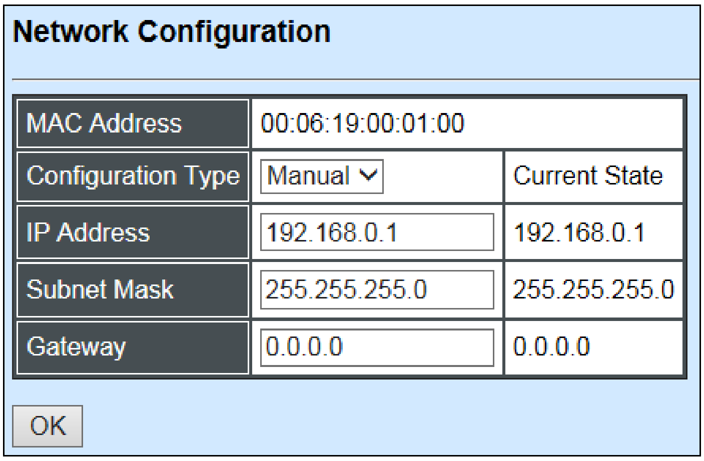
7. **Trap Destination:** View the registered SNMP trap destination list. Add a new trap destination or remove an existing trap destination.

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

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

3.3.1 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 Switch. You cannot change the Managed Industrial 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 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 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 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.)

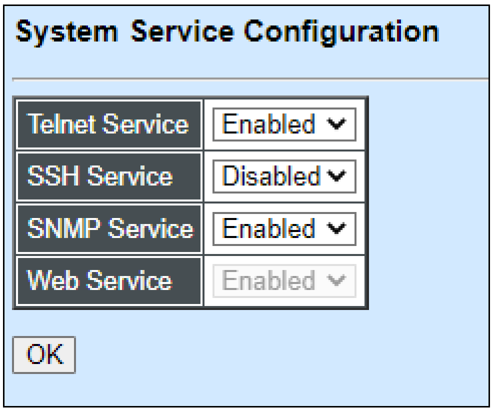
Subnet Mask: Specify the subnet mask. The default subnet mask values for the three Internet address classes are as follows:

- 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 Switch. This address is required when the Managed Industrial 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 Switch are on the same network.

3.3.2 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 **Telnet** or **SSH** for the system service type.

SSH Service: To enable or disable the SSH Management service.

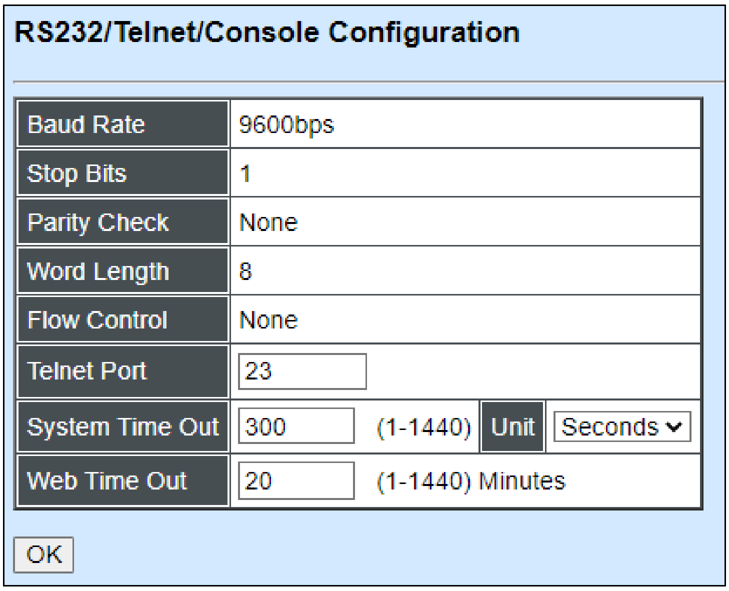
SNMP Service: Select Disabled or Enabled for the system service type.

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

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

3.3.3 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) Minutes

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*.

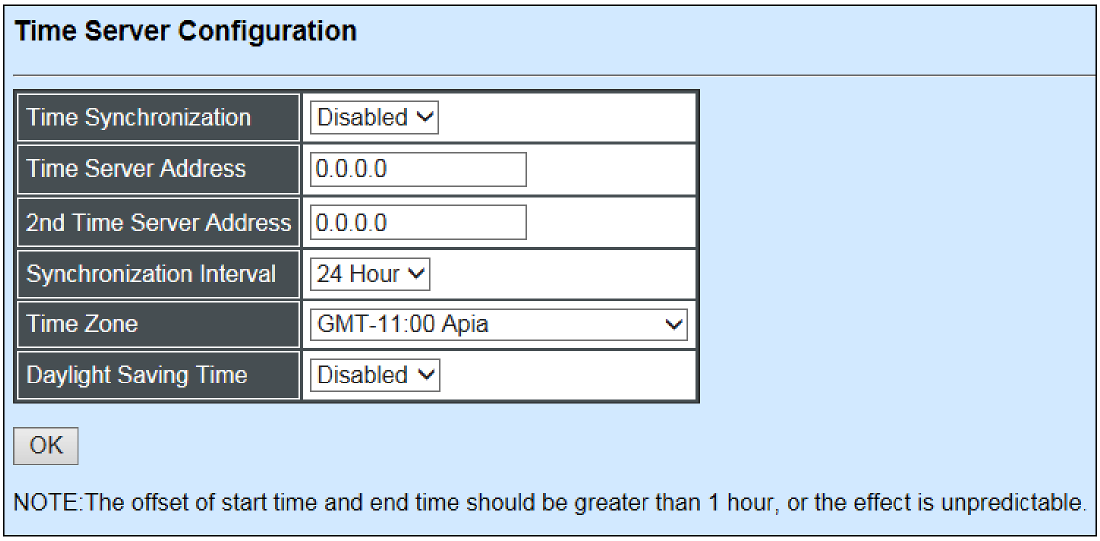
System Time Out: Specify the desired time that the Managed Industrial Switch will wait before disconnecting an inactive console/telnet. The default value is *300* seconds.

Web Time Out: Specify the desired time that the Managed Switch will wait before disconnecting an inactive web session. Valid range: 1-1440 minutes. The default value is *20* minutes.

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

3.3.4 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 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.

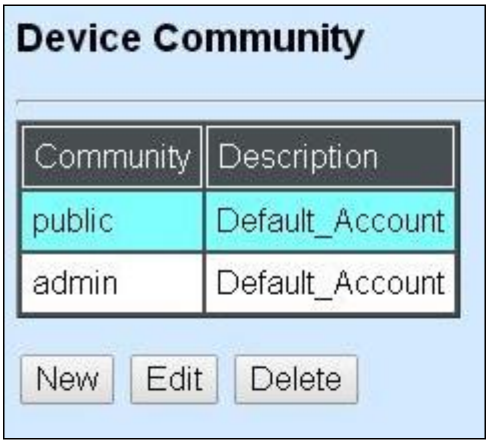
Daylight Saving Time Recurring Start — Click the pull-down menu to select the start date of daylight saving time using calendar algorithm.

Daylight Saving Time Recurring Start — Click the pull-down menu to select the start date of daylight saving time using calendar algorithm.

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

3.3.5 Device Community

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



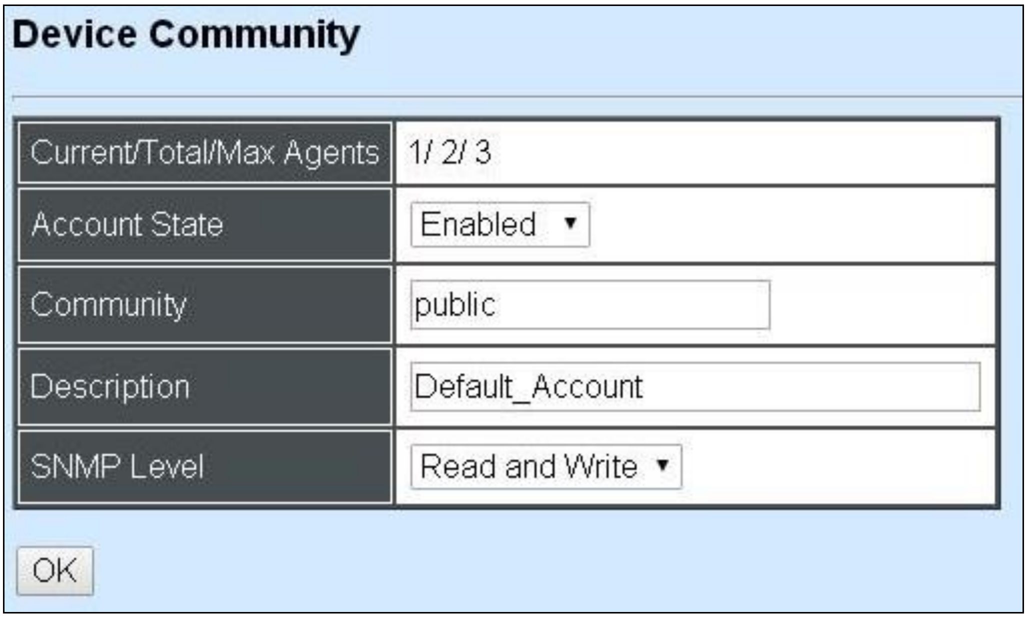
Device Community

Community	Description
public	Default_Account
admin	Default_Account

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

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

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



Device Community

Current/Total/Max Agents	1/ 2/ 3
Account State	Enabled
Community	public
Description	Default_Account
SNMP Level	Read and Write

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.

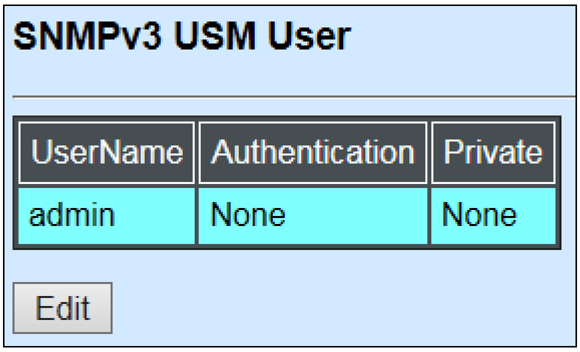
Read & Write: Partial access right.

Read Only: Read only access right.

3.3.6 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.

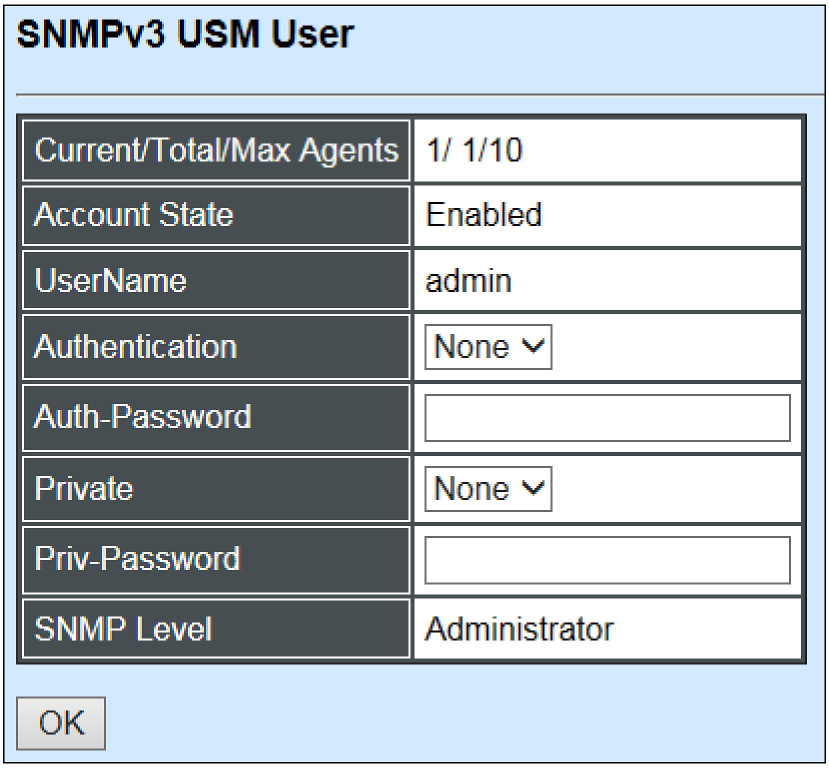
Note: *The SNMPv3 user account is generated from "User Authentication" (Section 3.1)*



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.

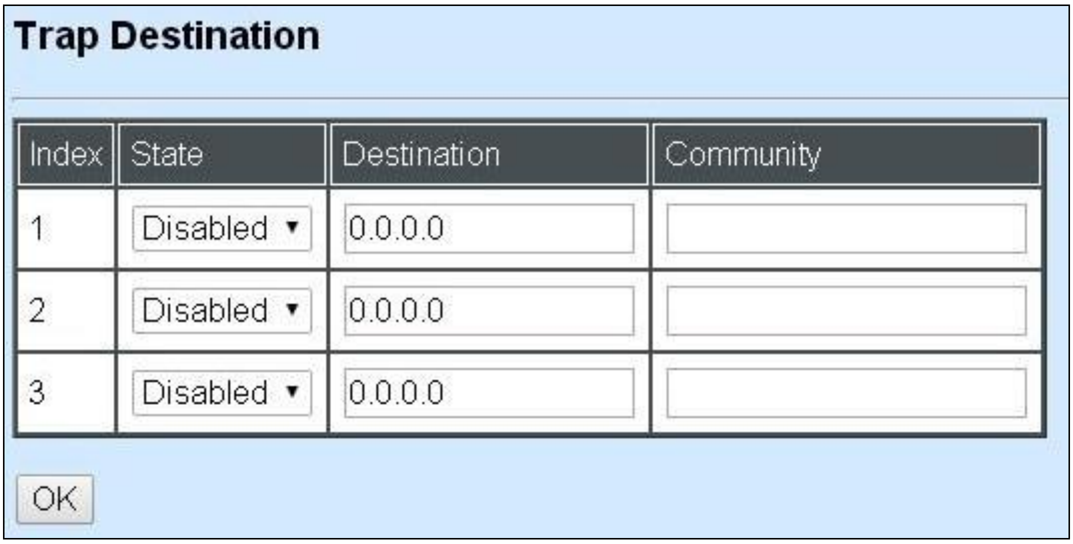
Read Only: Allow to view only.

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.

3.3.7 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.

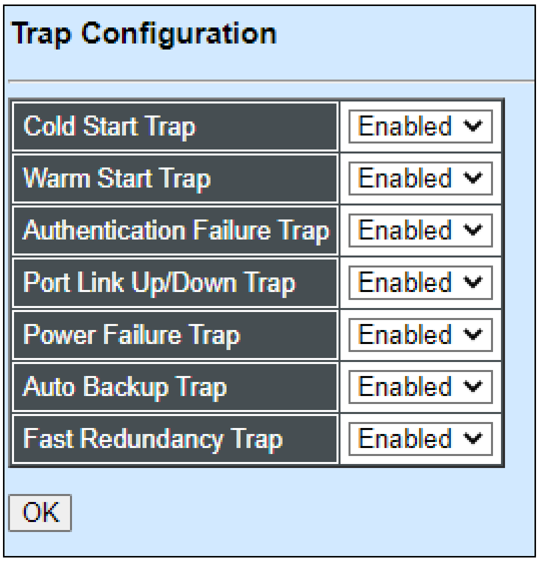
Destination: Set up IP address for the trap destination.

Community: Set up community for the specific trap destination.

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

3.3.8 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 ▾
Power Failure Trap	Enabled ▾
Auto Backup Trap	Enabled ▾
Fast Redundancy Trap	Enabled ▾

Cold Start Trap: Enable or disable the Managed Switch to send a trap when the Managed Switch is turned on.

Warm Start Trap: Enable or disable the Managed Switch to send a trap when the Managed Switch restarts.

Authentication Failure Trap: Enable or disable the Managed Switch to send authentication failure trap after any unauthorized users attempt to login.

Port Link Up/Down Trap: Enable or disable the Managed Switch to send port link up/link down trap.

Power Failure Trap: Enable or disable the Managed Switch to send a trap when the power 1/2 failure occurs or power it/them on again.

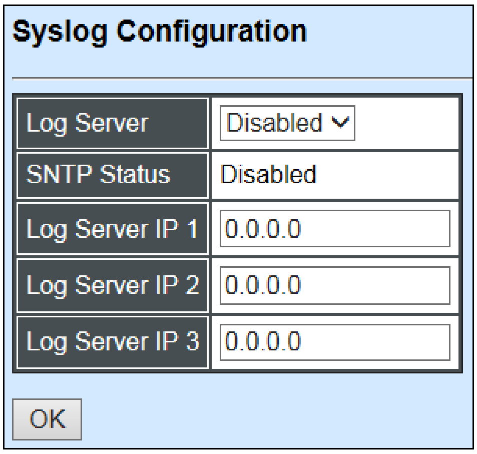
Auto Backup Trap: Enable or disable the Managed Switch to send a trap when the auto backup succeeds or fails.

Fast Redundancy Trap: Enable or disable the Managed Switch to send a trap when any specified redundancy port in fast redundancy links up or links down.

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

3.3.9 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.

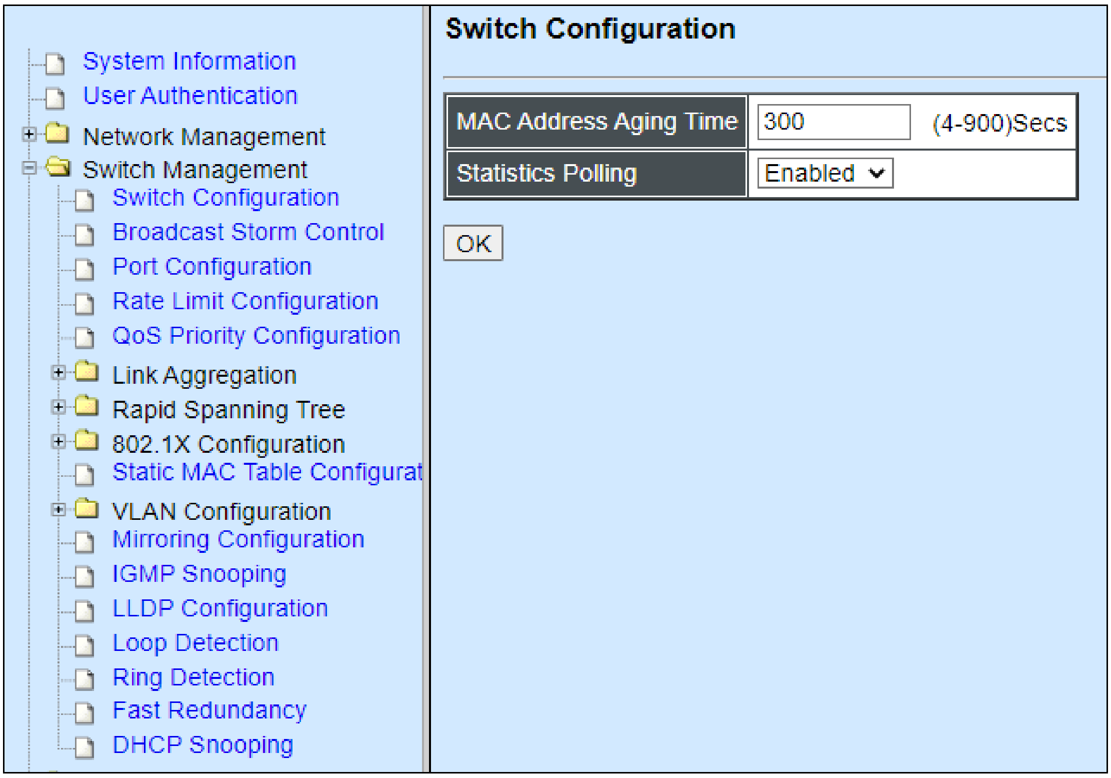
Log server IP 2: Set up the second Log server's IP address if needed

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

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

3.4 Switch Management

To manage the Managed Industrial 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

MAC Address Aging Time	300	(4-900)Secs
Statistics Polling	Enabled	

1. **Switch Configuration:** Set up MAC address aging time, and enable/disable statistics polling.

2. **Broadcast Storm Control:** Prevent the Managed Industrial Switch from broadcast storms.

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

4. **Rate Limit Configuration:** To configure each port's Ingress and Egress Rate.

5. **QoS Priority Configuration:** Set up the priority mode, priority queuing, priority remarking, and so on.

6. **Link Aggregation:** Set up port trunk and LACP port configuration.

7. **Rapid Spanning Tree:** Set up RSTP switch settings, aggregated port settings, physical port settings, etc.

8. **802.1X Configuration:** Set up the 802.1X system, port admin state, port reauthenticate.

9. **Static MAC Table Configuration:** Create or delete static MAC address entries.

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

11. **Mirroring Configuration:** Set up the source port(s) to mirror to the destination port for traffic monitoring.

12. **IGMP Snooping:** Set up IGMP Snooping function.

13. **LLDP Configuration:** Enable or disable LLDP on ports and set up LLDP-related attributes.

14. **Loop Detection:** Enable or disable Loop Detection function.

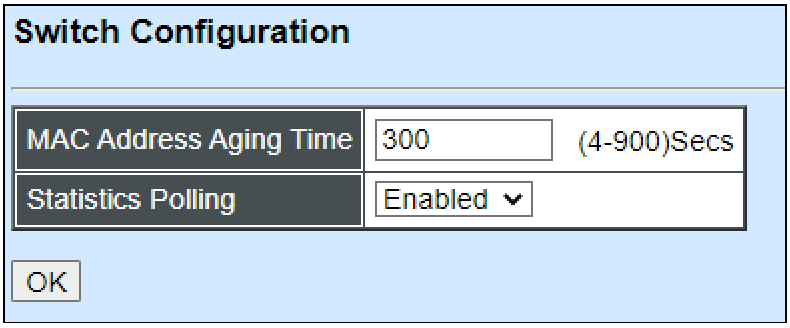
15. **Ring Detection:** Set up Ring Detection.

16. **Fast Redundancy:** Configure Fast Ring v2 or Chain protocol and investigate a comprehensive table displaying the up-to-date Fast Redundancy status for the monitoring and analysis of the configured network redundancy.

17. **DHCP Snooping:** Set up DHCP Snooping & Trust Port configuration.

3.4.1 Switch Configuration

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



Switch Configuration

MAC Address Aging Time	300 (4-900)Secs
Statistics Polling	Enabled

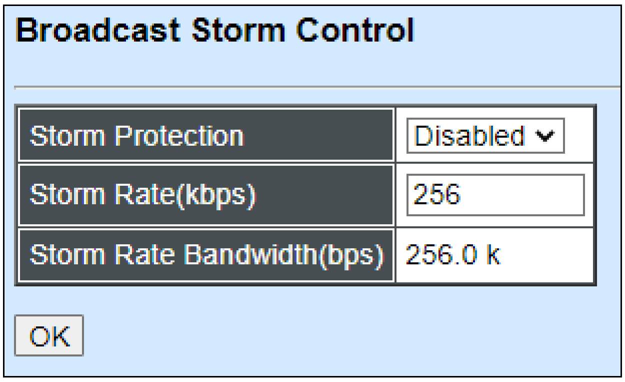
MAC Address Aging Time: Set up MAC Address Aging Time manually. Entries in the MAC address table containing source MAC addresses and their associated ports will be deleted if they are not accessed within the aging time. The default setting is “300” seconds.

Statistics Polling: Enable or disable Statistics Polling.

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

3.4.2 Broadcast Storm Control

Click the option **Broadcast Storm Control** from the **Switch Management** menu and then the following screen page appears.



Broadcast Storm Control

Storm Protection	Disabled
Storm Rate(kbps)	256
Storm Rate Bandwidth(bps)	256.0 k

Storm Protection: Enable or disable Storm Protection function.

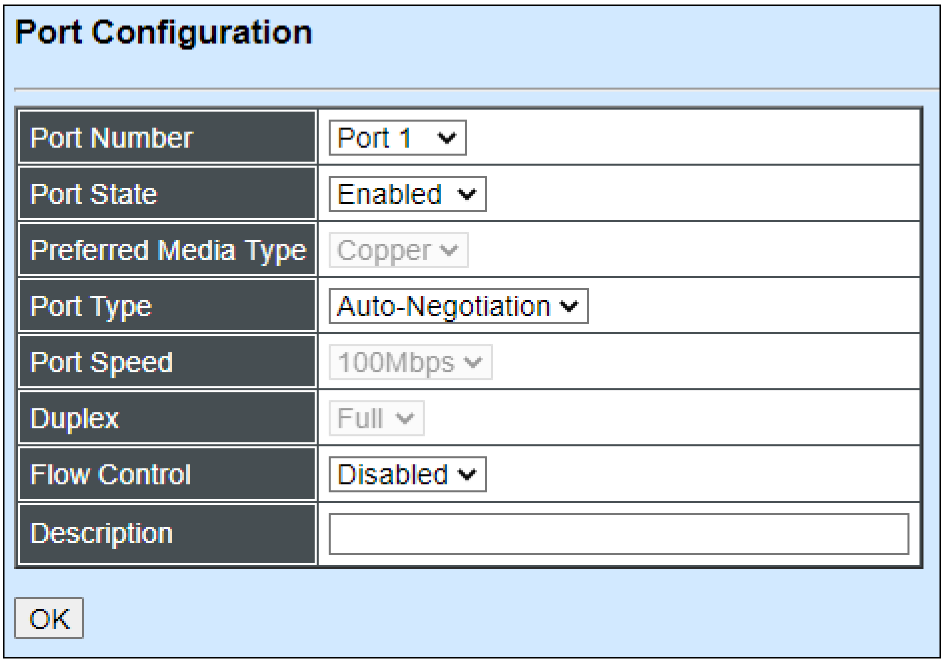
Storm Rate (kbps): Set up storm rate value. Packets exceeding the value will be dropped. (The Storm Rate range can be configured within 32~1000000kbps), the default value is 256.

Storm Rate Bandwidth (bps): Display the current configured storm rate bandwidth.

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

3.4.3 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	100Mbps
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).

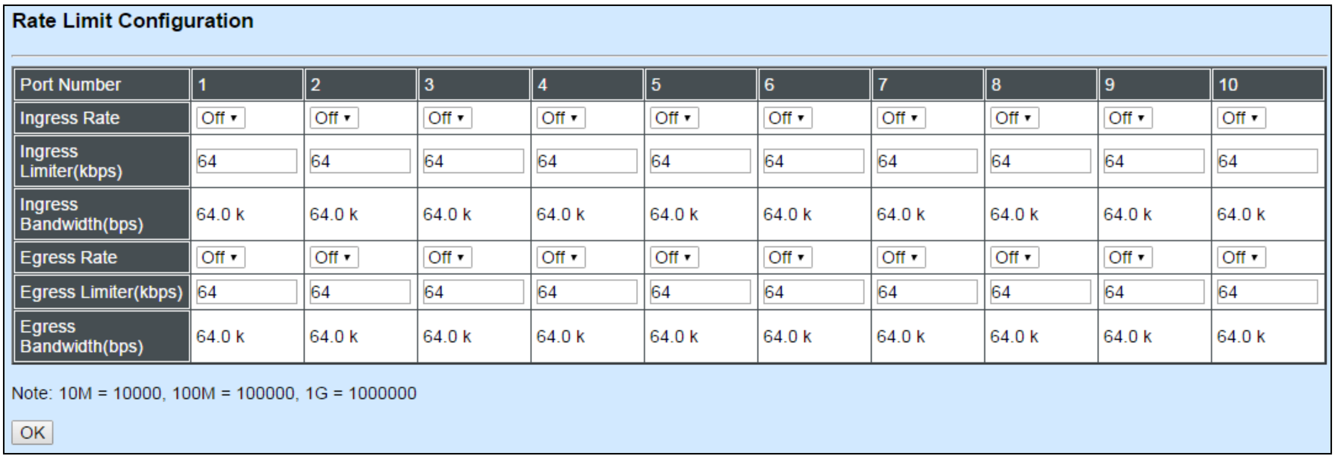
Flow Control: Enable or disable Flow Control function.

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

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

3.4.4 Rate Limit Configuration

Click the folder **Rate Limit Configuration** from the left column and then the following screen page appears.



Rate Limit Configuration

Port Number	1	2	3	4	5	6	7	8	9	10
Ingress Rate	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾
Ingress Limiter(kbps)	64	64	64	64	64	64	64	64	64	64
Ingress Bandwidth(bps)	64.0 k	64.0 k	64.0 k	64.0 k	64.0 k	64.0 k	64.0 k	64.0 k	64.0 k	64.0 k
Egress Rate	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾
Egress Limiter(kbps)	64	64	64	64	64	64	64	64	64	64
Egress Bandwidth(bps)	64.0 k	64.0 k	64.0 k	64.0 k	64.0 k	64.0 k	64.0 k	64.0 k	64.0 k	64.0 k

Note: 10M = 10000, 100M = 100000, 1G = 1000000

Ingress Rate: Click the pull-down menu to set up Port Ingress Rate, on or off.

Ingress Limiter: Enter ingress bandwidth for each port (the allowable bandwidth is between 32 and 1000000).

Ingress Bandwidth (Kbps): Display current configured ingress bandwidth.

Egress Rate: Click the pull-down menu to set up Port Egress Rate, on or off.

Egress Limiter (Kbps): Enter egress bandwidth for each port (the allowable bandwidth is between 32 and 1000000).

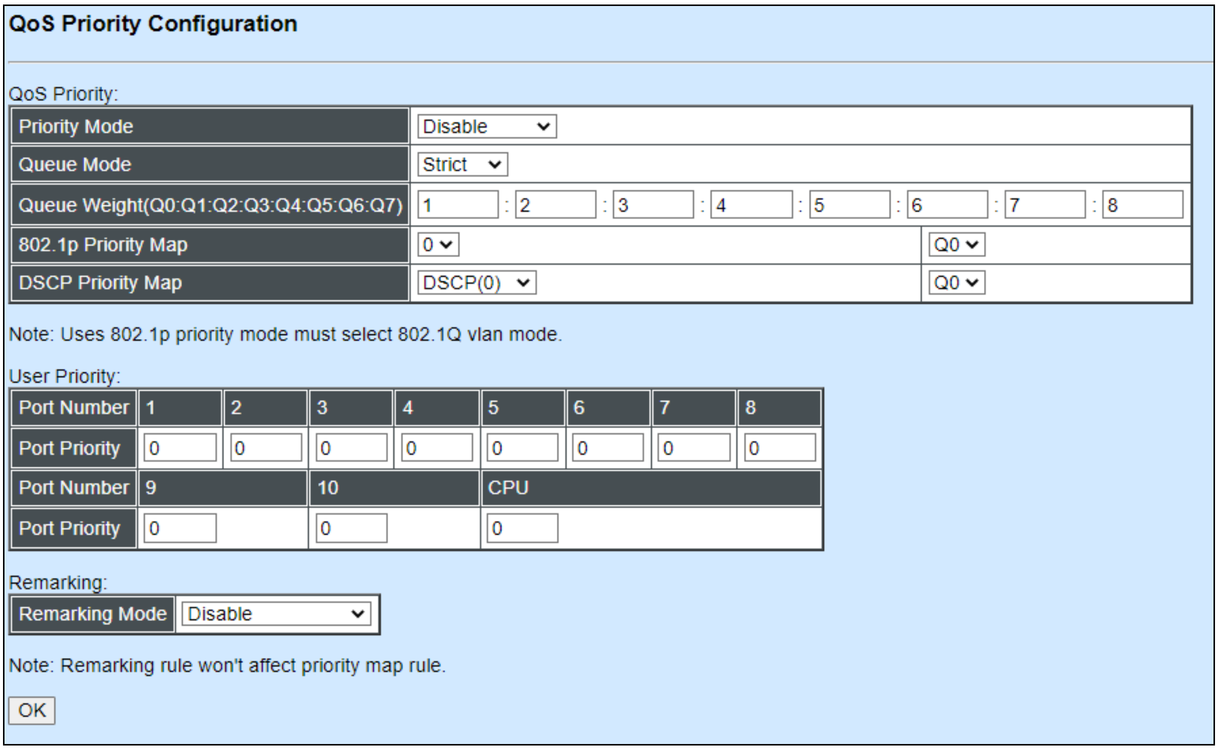
Egress Bandwidth (Kbps): Display current configured egress bandwidth.

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

3.4.5 QoS Priority 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 : 3 : 4 : 5 : 6 : 7 : 8	
802.1p Priority Map	0	Q0
DSCP Priority Map	DSCP(0)	Q0

Note: Uses 802.1p priority mode must select 802.1Q vlan mode.

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		CPU			
Port Priority	0		0		0			

Remarking:

Remarking Mode	Disable

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

OK

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

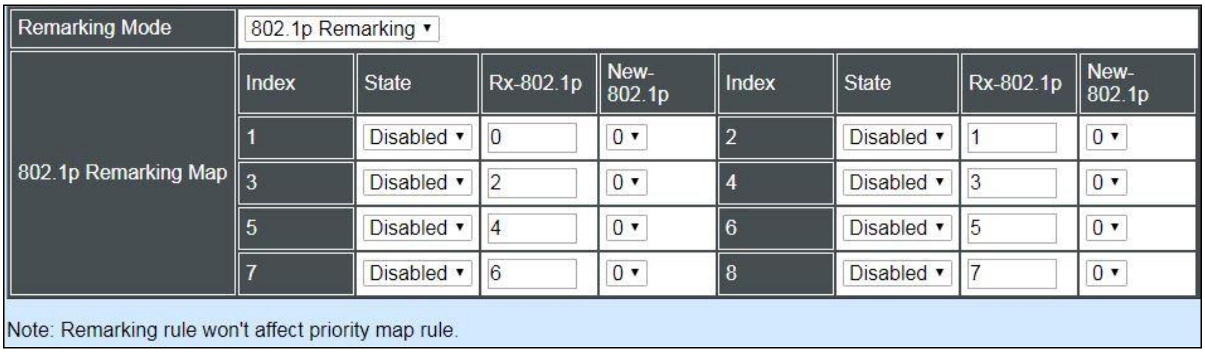
Note: *802.1p priority mode can only be applied under 802.1q VLAN mode.*

Remarking

Remarking Mode: Select **802.1p Remarking** or **DSCP Remarking** as the remarking mode. Select **Disable** to disable priority value remarking.

Configure 802.1p Remarking:

From the **Remarking Mode** pull-down menu**,** select **802.1p Remarking** to enable 802.1p remarking for the Managed Switch.



Remarking Mode	802.1p Remarking ▾							
802.1p Remarking Map	Index	State	Rx-802.1p	New-802.1p	Index	State	Rx-802.1p	New-802.1p
	1	Disabled ▾	0	0 ▾	2	Disabled ▾	1	0 ▾
	3	Disabled ▾	2	0 ▾	4	Disabled ▾	3	0 ▾
	5	Disabled ▾	4	0 ▾	6	Disabled ▾	5	0 ▾
	7	Disabled ▾	6	0 ▾	8	Disabled ▾	7	0 ▾

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

Index: The port on the Managed Switch

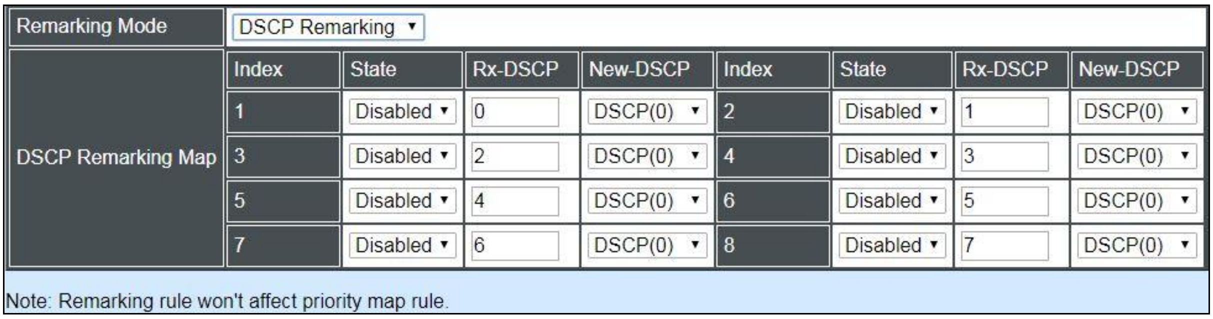
State: Enable or disable 802.1p Remarking on the selected interface.

Rx-802.1p: The 802.1p priority value carried by the incoming traffic.

New-802.1p: The new 802.1p priority value with which the Managed Switch will replace the older one that comes with the data packet originally.

Configure DSCP Remarking:

From the **Remarking Mode** pull-down menu**,** select **DSCP Remarking** to enable DSCP remarking for the Managed Switch.



Remarking Mode	DSCP Remarking ▾							
DSCP Remarking Map	Index	State	Rx-DSCP	New-DSCP	Index	State	Rx-DSCP	New-DSCP
	1	Disabled ▾	0	DSCP(0) ▾	2	Disabled ▾	1	DSCP(0) ▾
	3	Disabled ▾	2	DSCP(0) ▾	4	Disabled ▾	3	DSCP(0) ▾
	5	Disabled ▾	4	DSCP(0) ▾	6	Disabled ▾	5	DSCP(0) ▾
	7	Disabled ▾	6	DSCP(0) ▾	8	Disabled ▾	7	DSCP(0) ▾

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

Index: The port on the Managed Switch

State: Enable or disable DSCP Remarking on the selected interface.

Rx-DSCP: The DSCP priority value carried by the incoming traffic.

New-DSCP: The new DSCP priority value with which the Managed Switch will replace the older one that comes with the data packet originally.

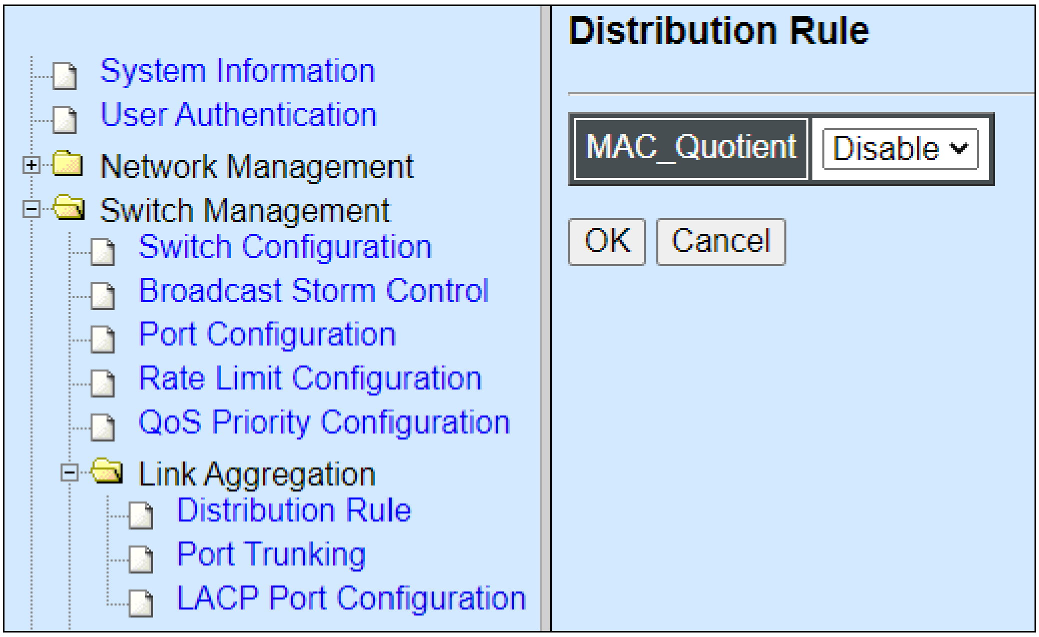
3.4.6 Link Aggregation

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

MAC_Quotient: Disable

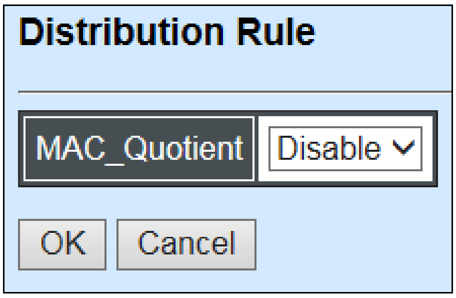
1. Distribution Rule: Configure the distribution rule of Port Trunking group(s).

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

3. LACP Port Configuration: Set up the configuration of LACP on all or some ports.

3.4.6.1 Distribution Rule

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



Distribution Rule

MAC_Quotient: Disable

MAC_Quotient: Enable or disable distributing packets according to the MAC address.

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

1. Identifying MAC

It checks the last three bits of Source MAC and Dst. MAC and XOR algorithm distributes them.

XOR Algorithm:

0 & 0 = 0

0 & 1 = 1

1 & 0 = 1

1 & 1 = 0

Three bits results in eight combinations (0~7), it is used to determine which packet should be sent to.

Example:

Source MAC 11:22:33:44:55:66

⇧ The last digit 6 occupies 4 bits (Use the last three bits ⇨ 0100)

Dst. MAC   33:44:55:66:77:88

⇧ The last digit 8 occupies 4 bits (Use the last three bits ⇨ 1000)

XOR Algorithm:

Src. MAC – 1 1 0

Dst. MAC – 0 0 0

Result   – 1 1 0 = 6

2. MAC Quotient Distribution

Example 1:

Assume that 2 ports are aggregated

8(bit)/2(port) = 4 (Integer) ⇨ each port is evenly distributed 4 types of bit

8(bit)/2(port) = 0 (Remainder) ⇨ The first ports will be distributed extra bits, if any

If enabled:

Port 1 will get 4 bits ⇨ 0, 1, 2, 3

Port 2 will get 4 bits ⇨ 4, 5, 6, 7

Example 2:

Assume that 3 ports are aggregated

8(bit)/2(port) = 2 (Integer) ⇨ each port is distributed 2 types of bit at least

8(bit)/2(port) = 2 (Remainder) ⇨ The first two ports will be additionally gotten 1 bit respectively

If enabled:

Port 1 will get 3 bits ⇨ 0, 1, 2

Port 2 will get 3 bits ⇨ 3, 4, 5

Port 3 will get 2 bits ⇨ 6, 7

Example 3:

Assume that 6 ports are aggregated

8(bit)/6(port) = 1 (Integer) ⇨ each port is distributed 1 type of bit at least

8(bit)/6(port) = 2 (Remainder) ⇨ The first two ports will be additionally gotten 1 bit respectively

If enabled:

Port 1 will get 2 bits ⇨ 0, 1

Port 2 will get 2 bits ⇨ 2, 3

Port 3 will get 1 bit ⇨ 4

Port 4 will get 1 bit ⇨ 5

Port 5 will get 1 bit ⇨ 6

Port 6 will get 1 bit ⇨ 7

3. Disabling MAC Quotient

If MAC Quotient is disabled, 8 types of bit are distributed in another way.

Example 1

Assume that 2 ports are aggregated

Port 1 will get 4 bits ⇨ 0, 2, 4, 6

Port 2 will get 4 bits ⇨ 1, 3, 5, 7

Example 2

Assume that 3 ports are aggregated

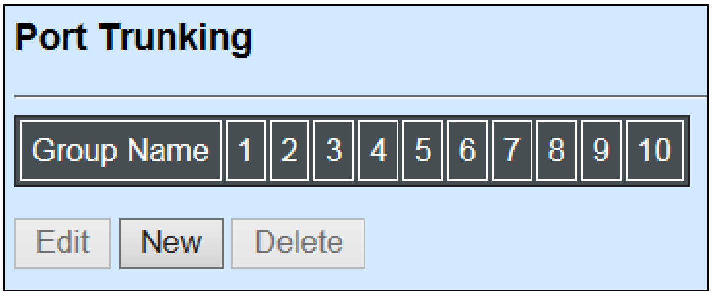
Port 1 will get 3 bits ⇨ 0, 3, 6

Port 2 will get 3 bits ⇨ 1, 4, 7

Port 3 will get 2 bits ⇨ 2, 5

3.4.6.2 Port Trunking

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



Port Trunking

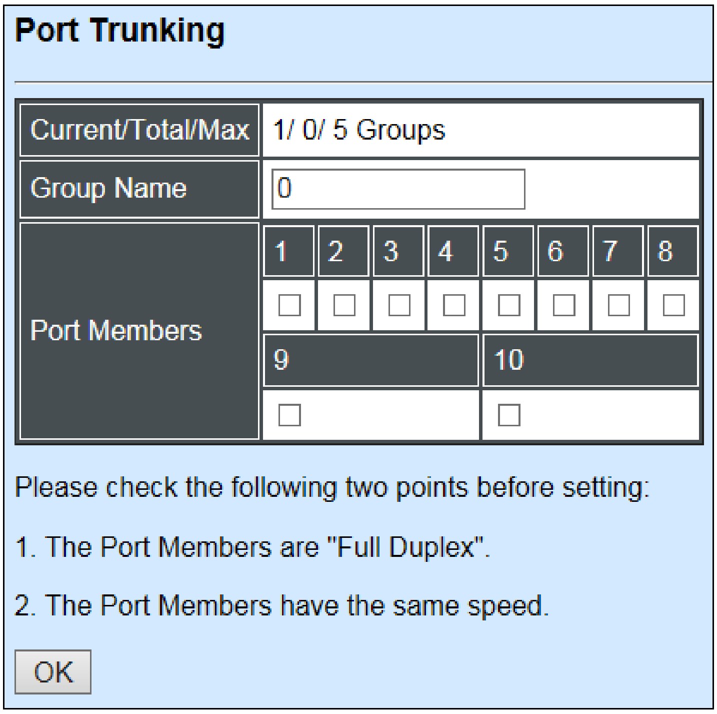
Group Name	1	2	3	4	5	6	7	8	9	10

The Managed Industrial 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/ 5 Groups							
Group Name	0							
Port Members	1	2	3	4	5	6	7	8
	□	□	□	□	□	□	□	□
	9				10			
	□				□			

Please check the following two points before setting:

1. The Port Members are "Full Duplex".

2. The Port Members have the same speed.

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.

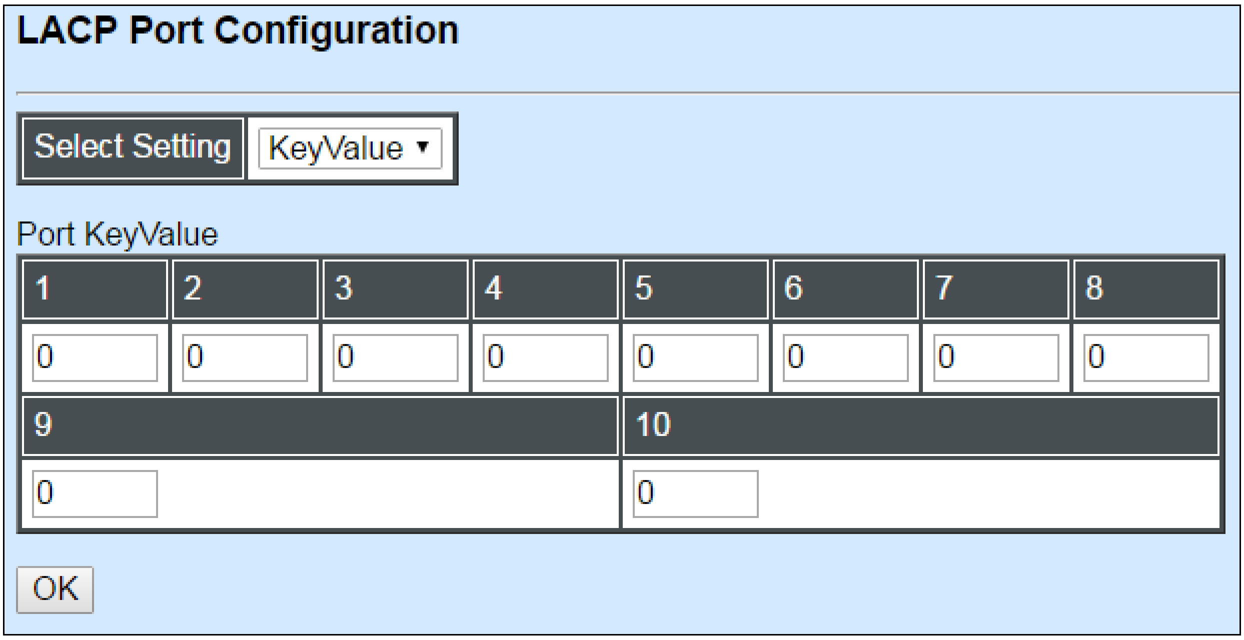
NOTE: *All trunking ports in the group must be members of the same VLAN, and QoS default priority configurations must be identical. Furthermore, all of the LACP aggregated links must be in the same speed and should be configured as full duplex.*

3.4.6.3 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

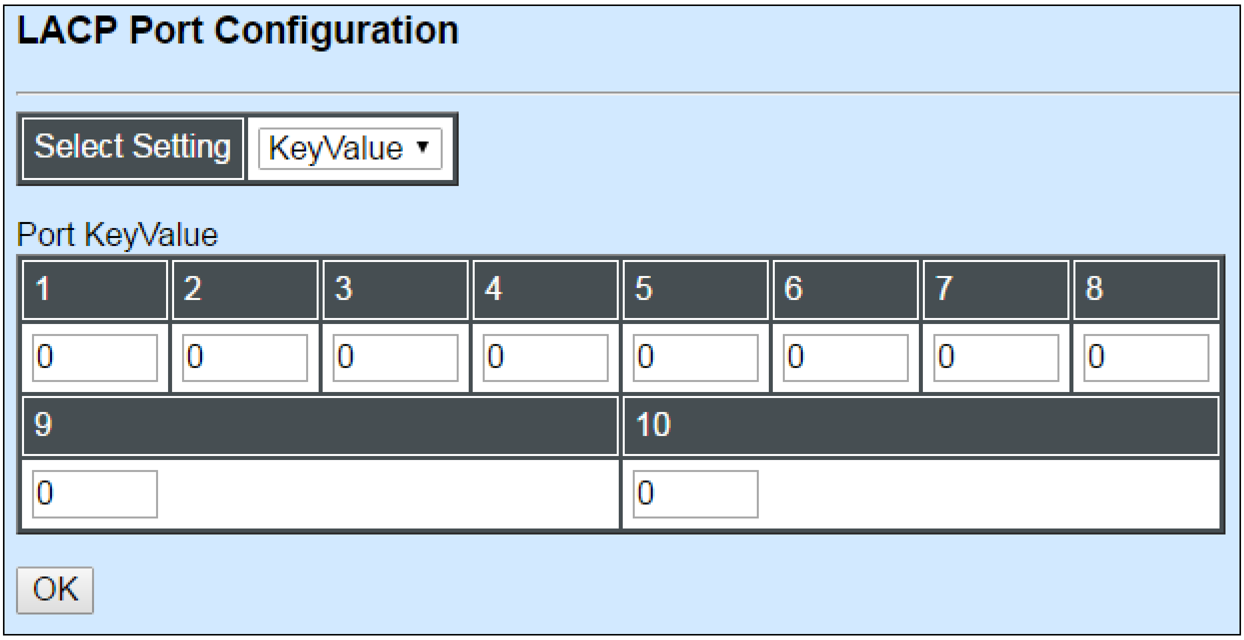
1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0

9	10
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

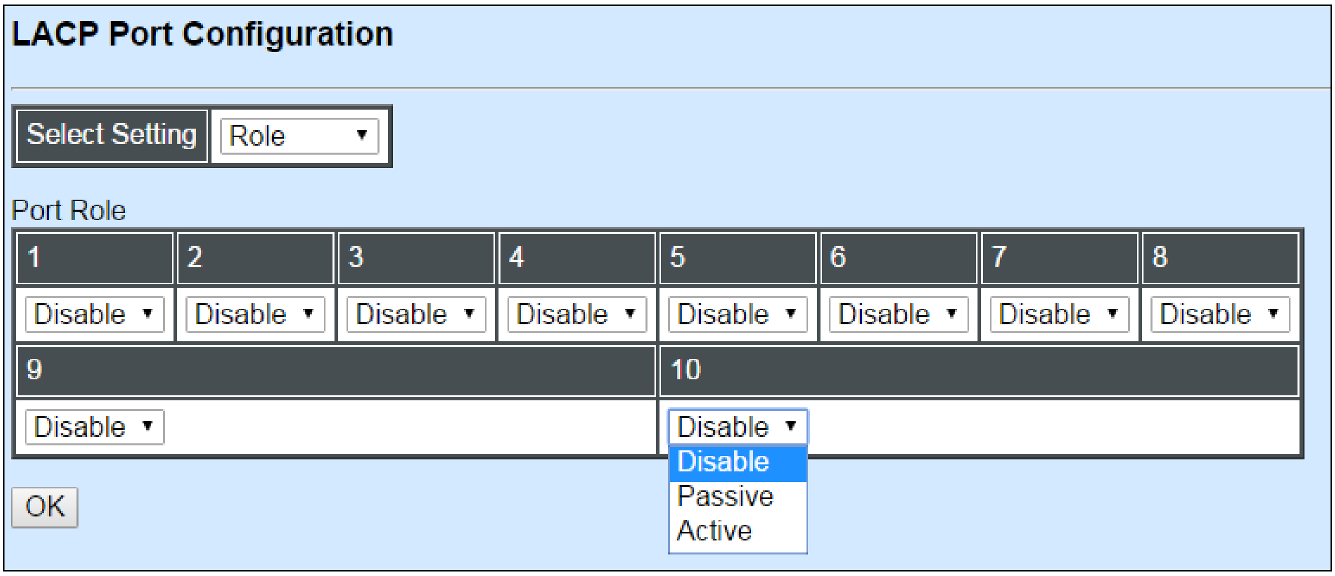
1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0

9	10
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 ▾

9	10
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.

3.4.7 Rapid Spanning Tree

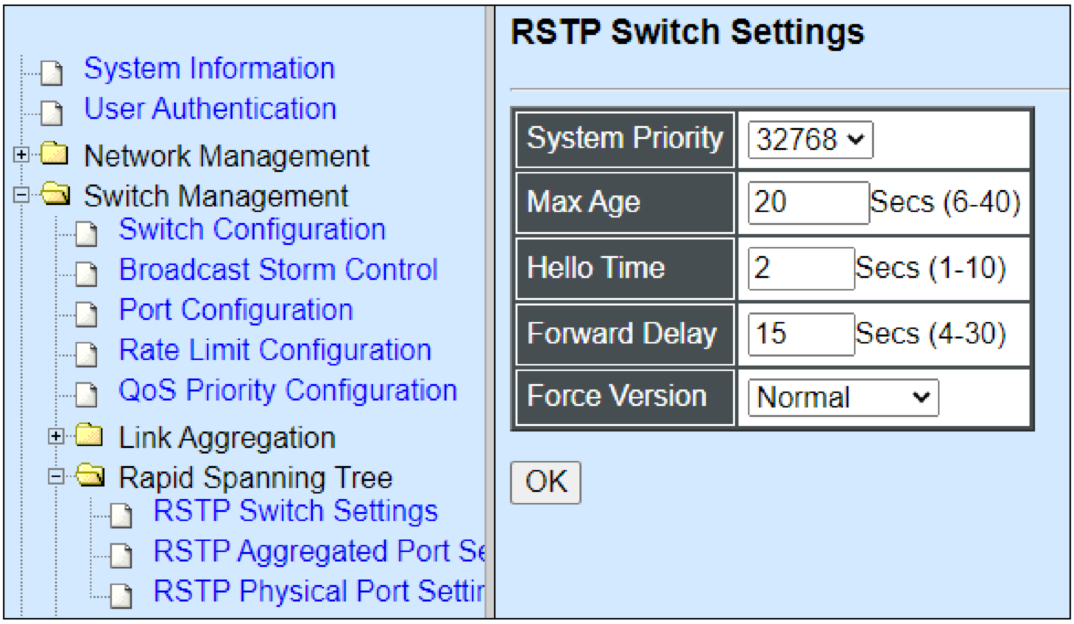
The Spanning Tree Protocol (STP), defined in the IEEE Standard 802.1D, creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches) and disables the links which are not part of that tree, leaving a single active path between any two network nodes.

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	20 Secs (6-40)
Hello Time	2 Secs (1-10)
Forward Delay	15 Secs (4-30)
Force Version	Normal

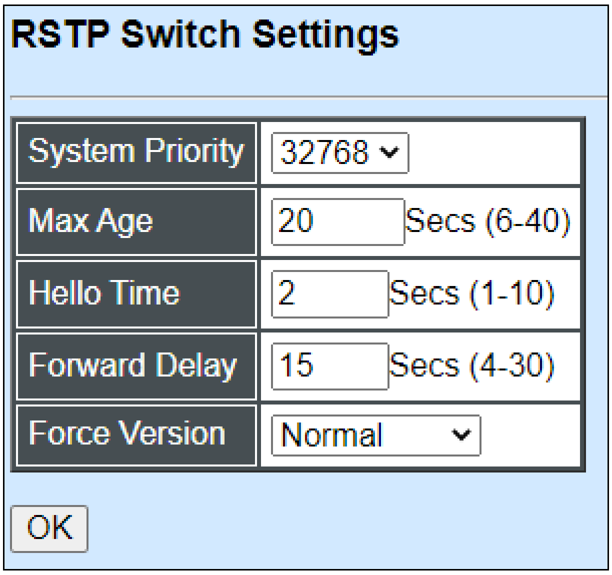
1. **RSTP Switch Settings:** Set up system priority, max Age, hello time, etc.

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.

3.4.7.1 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	20 Secs (6-40)
Hello Time	2 Secs (1-10)
Forward Delay	15 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 default setting is “32768”.

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 default value is set “20” seconds.

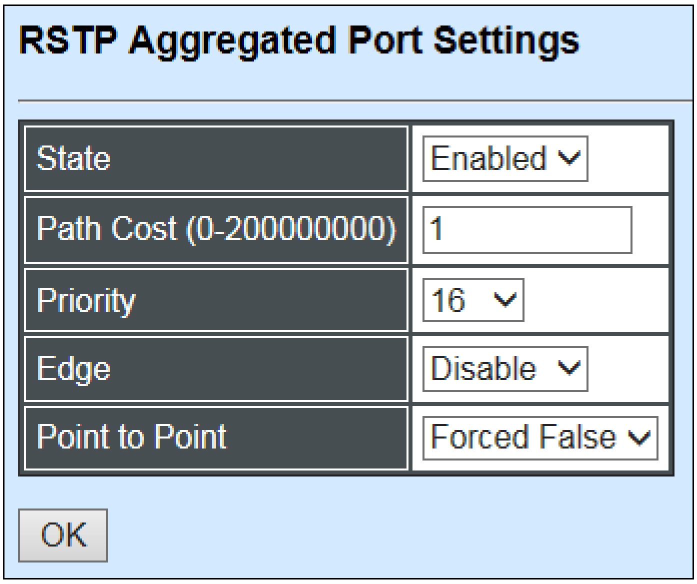
Hello Time: Periodically, a hello packet is sent out by the Root Bridge and the Designated Bridges that are used to communicate information about the topology throughout the entire Bridged Local Area Network. The default setting is set “2” second.

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. The default setting is “15” seconds.

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

3.4.7.2 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. The default setting is “1”.

Priority: You can choose Port Priority available value: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 and 240. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority. The default value is 16.

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:

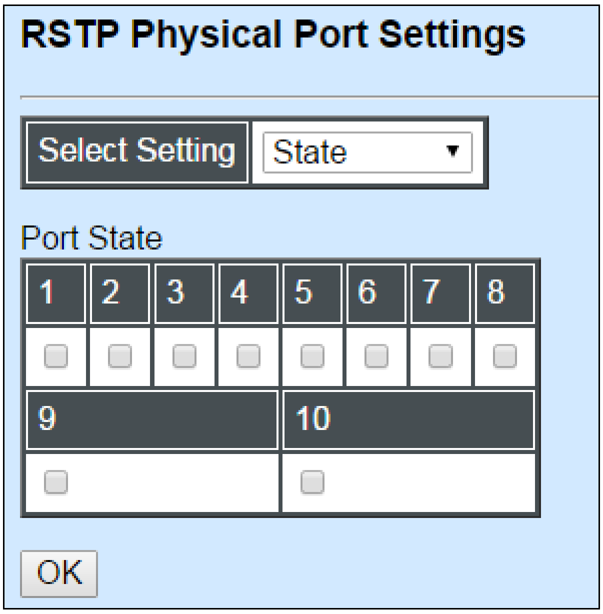
> **Forced True:** indicates a point-to-point (P2P) shared link.P2P ports are similar to edge ports; however, they are restricted in that a P2P port must operate in full duplex. Similar to edge ports, P2P ports transit to a forwarding state rapidly thus benefiting from RSTP.
>
> **Forced False:** the 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.

3.4.7.3 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 drop-down box of Select Setting.



RSTP Physical Port Settings

Select Setting: State ▾

Port State

1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□

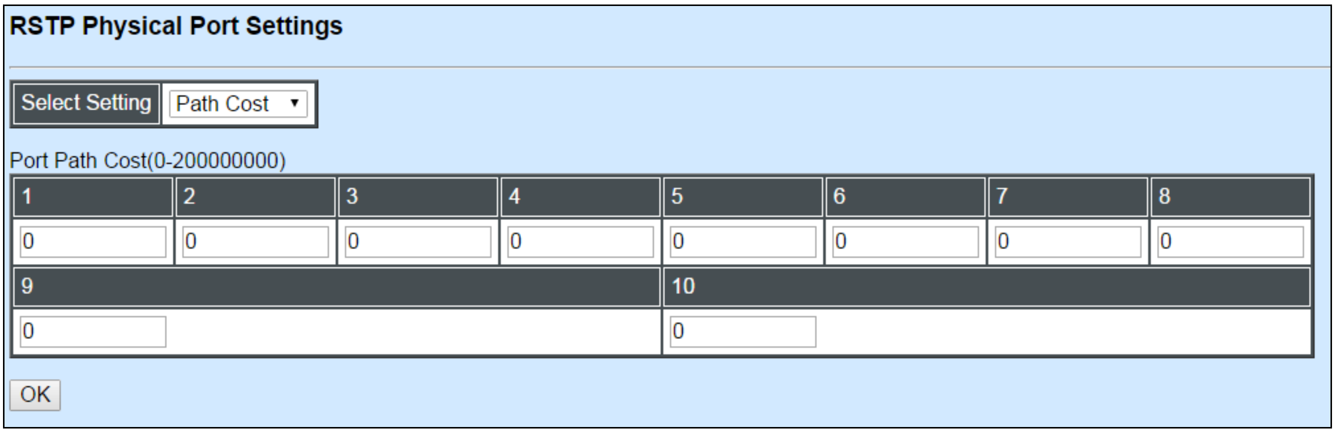
9	10
□	□

OK

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)

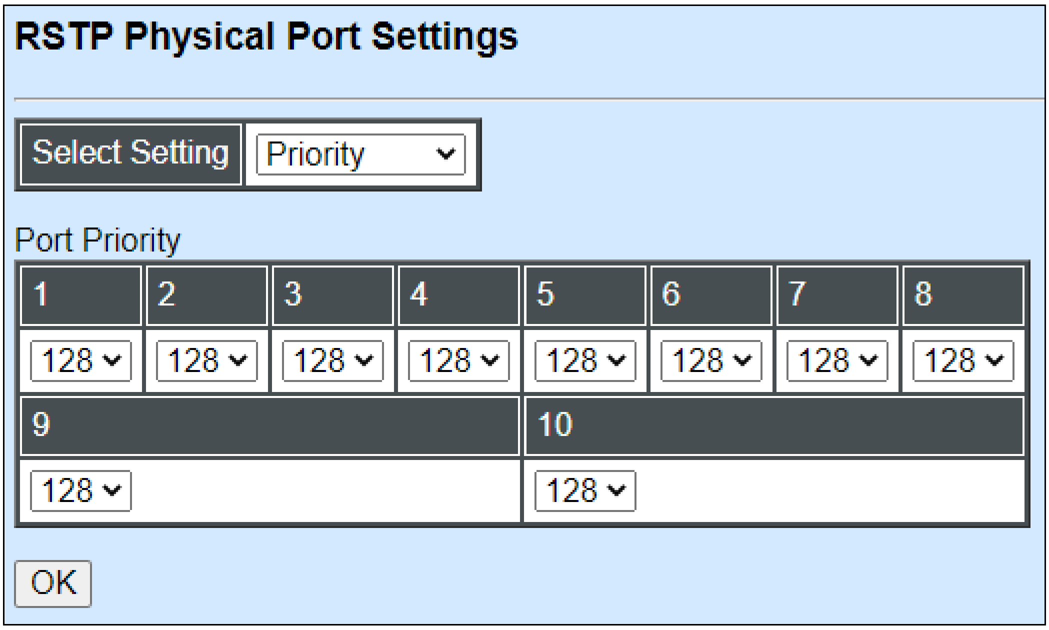
1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0

9	10
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

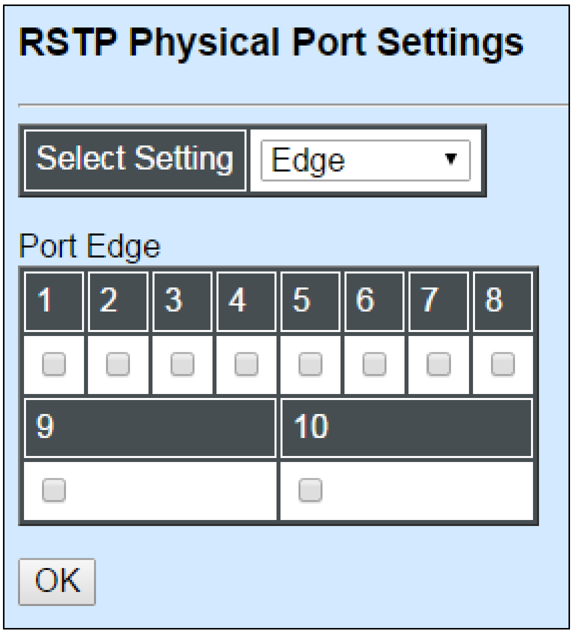
1	2	3	4	5	6	7	8
128	128	128	128	128	128	128	128

9	10
128	128

You can choose Port Priority available value: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 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

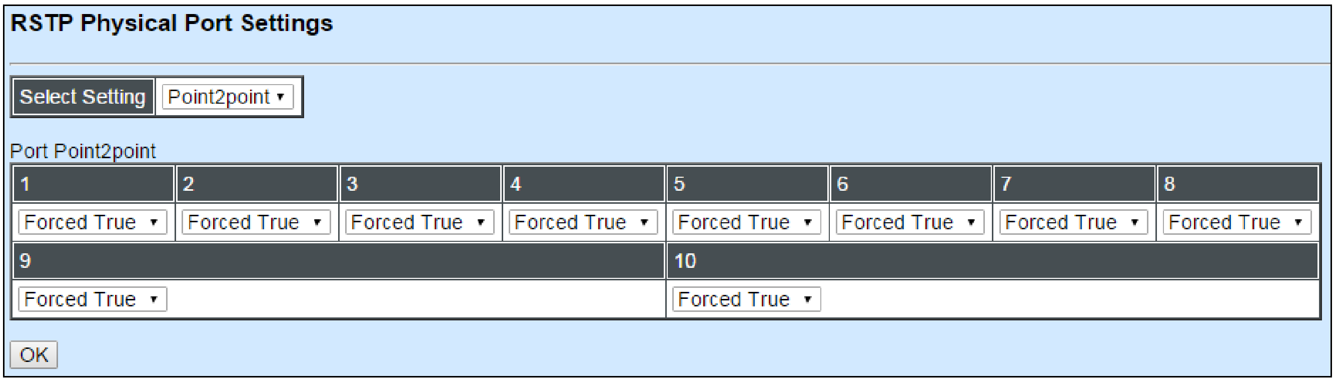
1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□

9	10
□	□

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
Forced True	Forced True

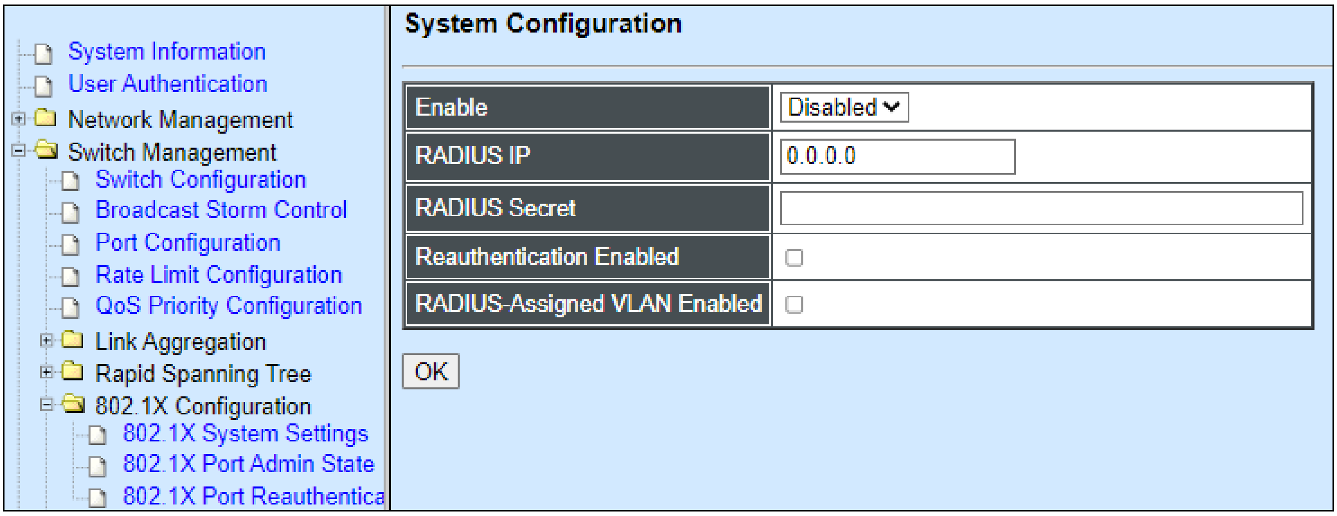
Set up the Point to Point setting. The default setting is “Forced True”.

3.4.8 802.1X 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 Configuration** from the **Switch Management** menu and then three options will be displayed as follows.



System Configuration

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

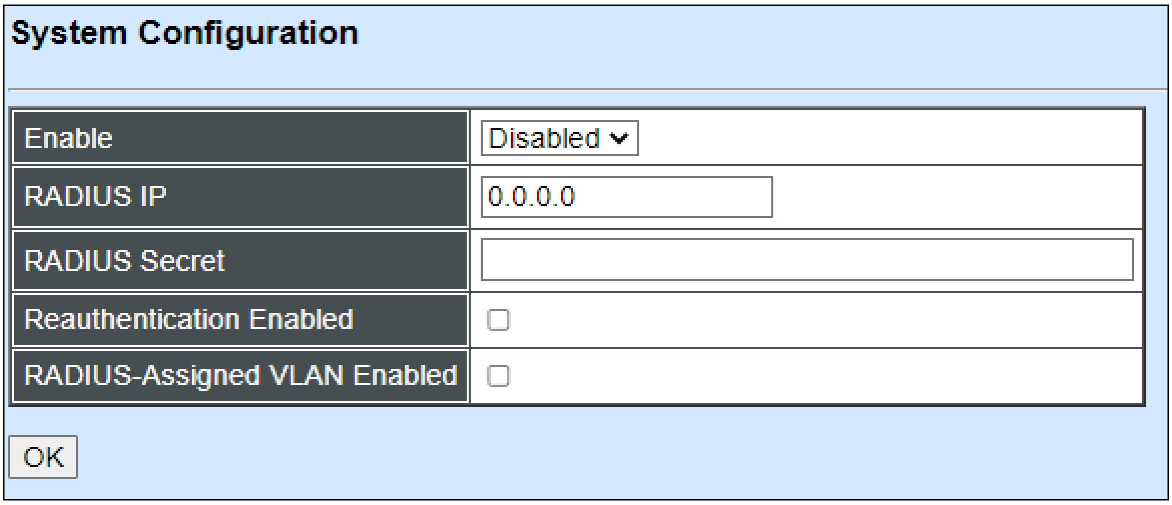
1. **802.1X System Settings:** Set up system 802.1X RADIUS IP, RADIUS Secret, Reauthentication, EAP Timeout, and so on.

2. **802.1X Port Admin State:** Set up the port authorization state.

3. **802.1X Port Reauthenticate:** Set up the port reatentication.

3.4.8.1 802.1X System Settings

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



System Configuration

Enable	Disabled
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.

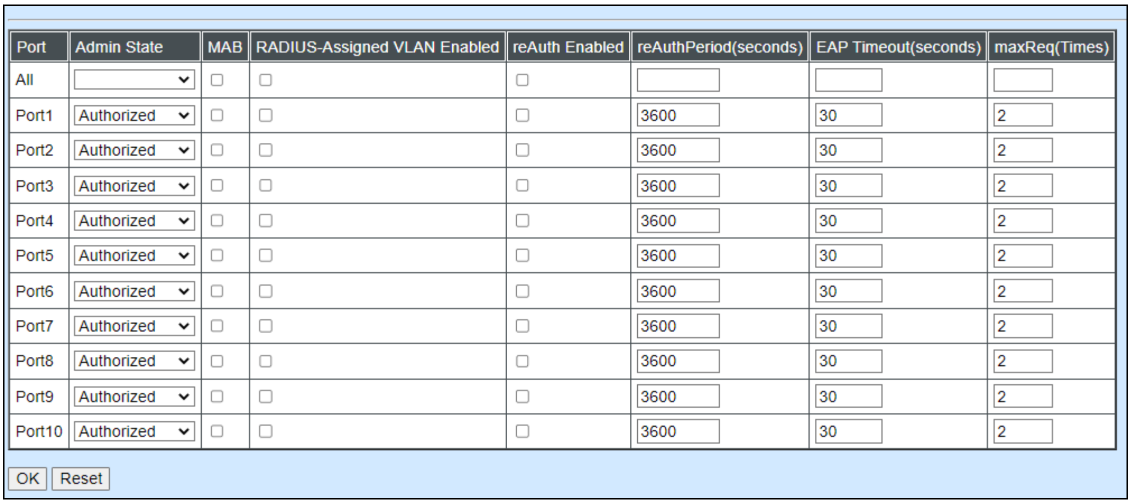
RADIUS Secret: The identification number assigned to each RADIUS authentication server with which the client shares a secret.

Reauthentication Enabled: Enable or disable Reauthentication.

RADIUS-Assigned VLAN Enabled: Globally allow the RADIUS server to send a VLAN assignment to the device.

3.4.8.2 802.1X Port Admin State

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



Port	Admin State	MAB	RADIUS-Assigned VLAN Enabled	reAuth Enabled	reAuthPeriod(seconds)	EAP Timeout(seconds)	maxReq(Times)
All		□	□	□			
Port1	Authorized	□	□	□	3600	30	2
Port2	Authorized	□	□	□	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
Port10	Authorized	□	□	□	3600	30	2

Port: The number of each port.

Admin State: Include Authorized, Unauthorized and Auto 3 options for the user to set up the port authorization state for each port. Each state is described 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), which uses the connecting device's MAC address to grant or deny network access.297

RADIUS-Assigned VLAN Enabled: Allow the RADIUS server to send a VLAN assignment to the device port.

Re-Authentication Enabled: Enable or disable the auto re-authentication function for each port.

Re-Authentication Period (Secs 1-65535): Specify a period of authentication time that a client authenticates with the authentication server. Valid range: 1-65535 seconds. Default: 3600 seconds.

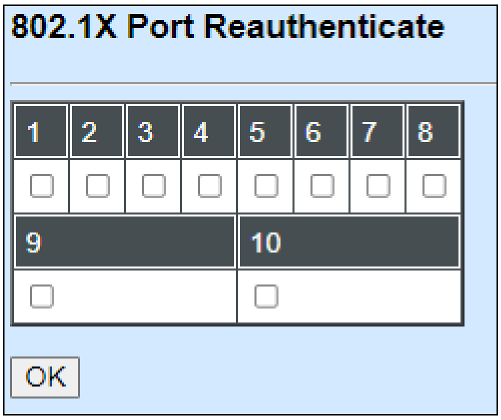
Re-Authenticate: By clicking on the **Re-Auth** button of the corresponding port number, the authentication message will be sent immediately to re-authenticate the specified port right now.

EAP Timeout (Secs 1-255): Specify the time value in seconds that the Managed Switch will wait for a response from the authentication server to an authentication request. Valid range: 1-255 seconds. Default: 30seconds.

Max Request (1-10 Times): Configure EAP-request/identity retry times from the switch to client before restarting the authentication process. In case MAB is enabled, MAB will be applied when exceeding this retry times.

3.4.8.3 802.1X Port Reauthenticate

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



802.1X Port Reauthenticate

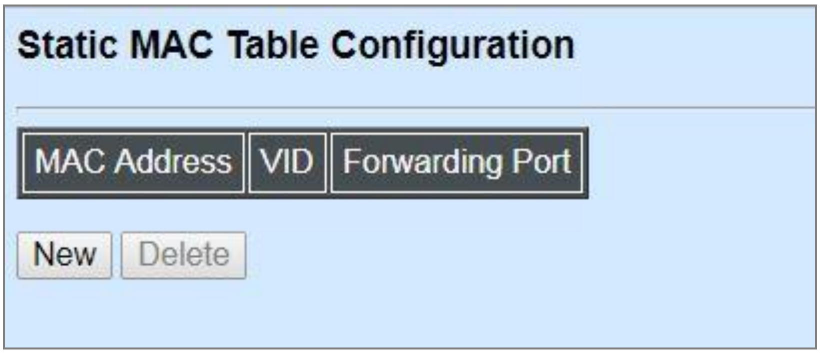
1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□

9	10
□	□

By clicking on the checkbox of the corresponding port number, it will allow to re-authenticate the selected ports right now. When enabled, the authentication message will be sent immediately after you click the **OK** button.

3.4.9 Static MAC Table Configuration

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



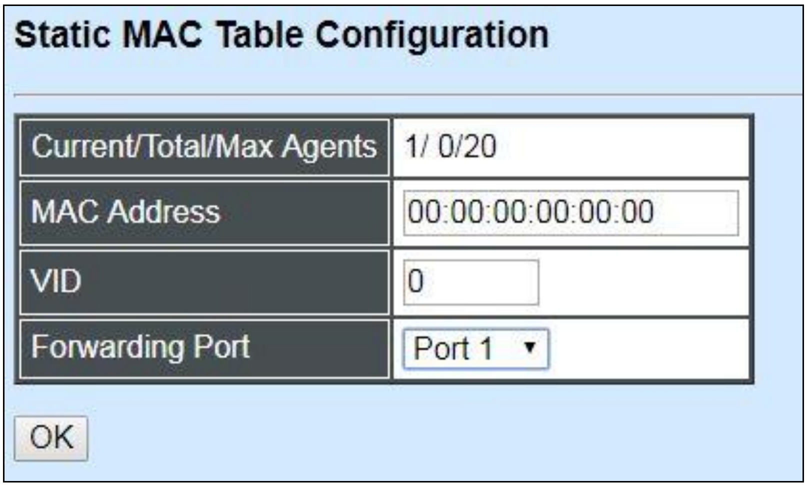
Static MAC Table Configuration

MAC Address	VID	Forwarding Port

NOTE: *The Managed Switch only supports switch-based MAC security and does not support port-based MAC security. The Managed Switch can support up to 20 entries of MAC security list.*

Click **Delete** to remove a MAC address entry.

Click **New** to add a new MAC address entity and then the following screen page appears.



Static MAC Table Configuration

Current/Total/Max Agents	1/ 0/20
MAC Address	00:00:00:00:00:00
VID	0
Forwarding Port	Port 1 ▼

Current/Total/Max Agents: The number of current, total and maximum MAC address entry or entries.

MAC Address: Specify a destination MAC address in the packet with the 00:00:00:00:00:00 format.

VID: Specify the VLAN where the packets with the Destination MAC address can be forwarded.

Forwarding Port: If the incoming packet has the same destination MAC address as the one specified in VID, it will be forwarded to the selected port directly.

3.4.10 VLAN Configuration

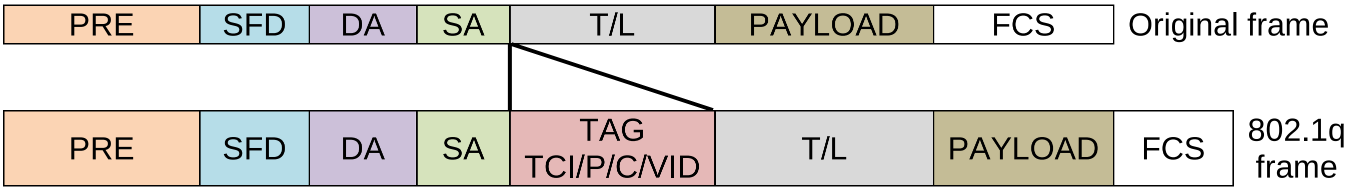
A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast 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 Switch supports two types of VLAN: **Port Based VLAN** and **IEEE 802.1q Tag VLAN.**

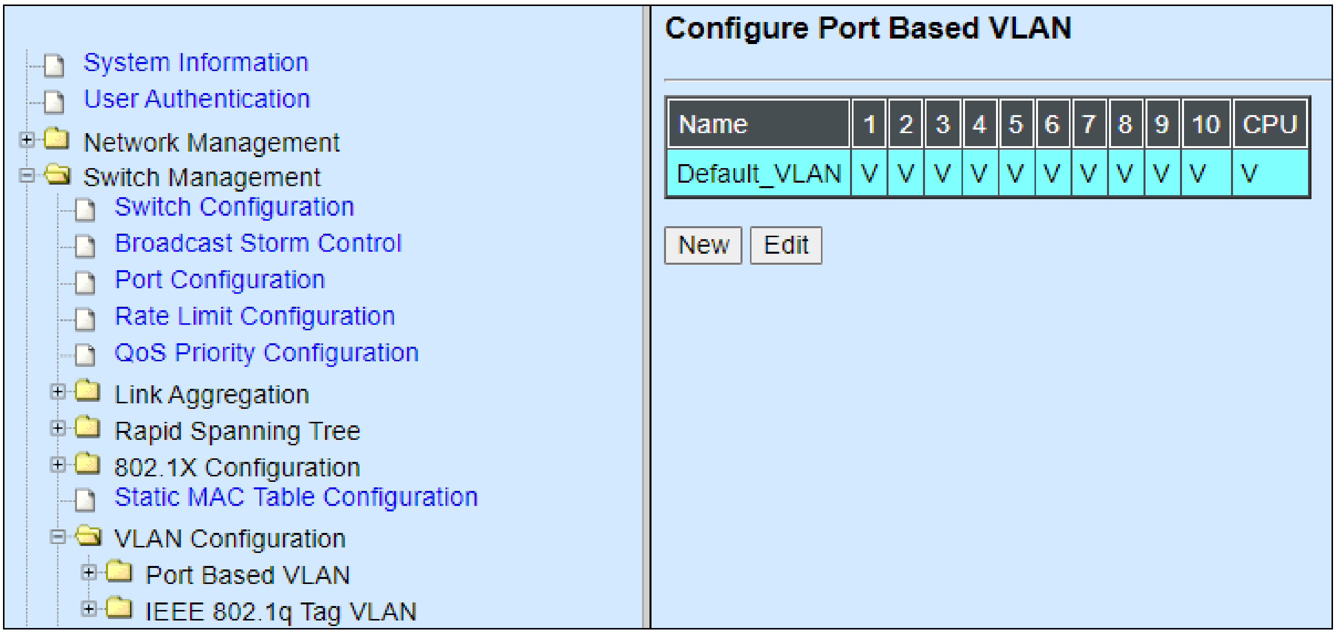
IEEE 802.1Q VLAN Concepts

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	CPU
Default_VLAN	V	V	V	V	V	V	V	V	V	V	V

1. Port Based VLAN: Configure Port-Based VLAN settings.

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

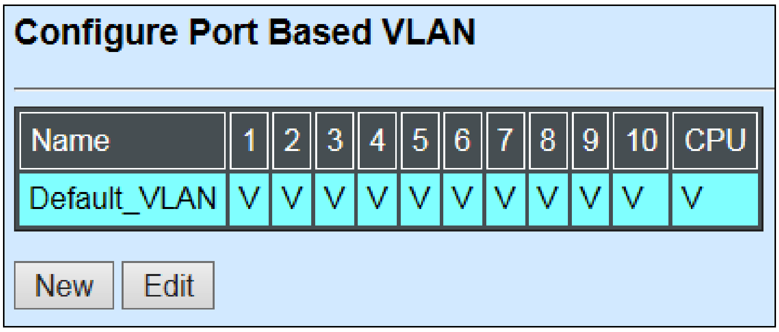
3.4.10.1 Port Based VLAN

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.

3.4.10.1.1 Configure Port Based VLAN

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



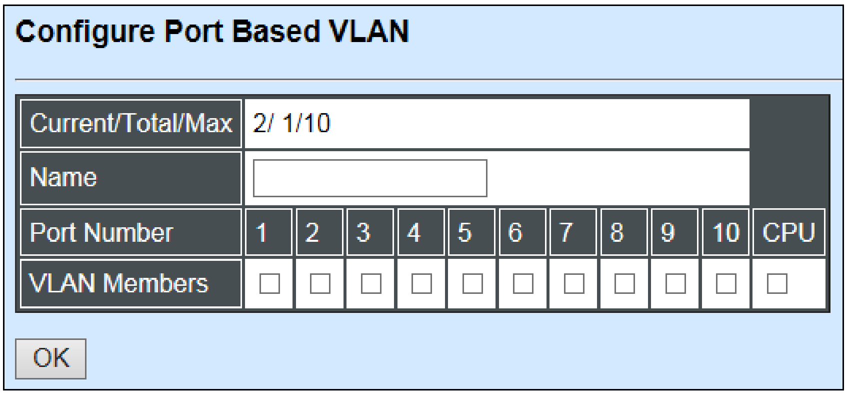
Configure Port Based VLAN

Name	1	2	3	4	5	6	7	8	9	10	CPU
Default_VLAN	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/ 1/10										
Name											
Port Number	1	2	3	4	5	6	7	8	9	10	CPU
VLAN Members	□	□	□	□	□	□	□	□	□	□	□

Current/Total/Max: View-only field.

Current: It shows the number of currently configured VLAN.

Total: It shows the total number of the VLANs.

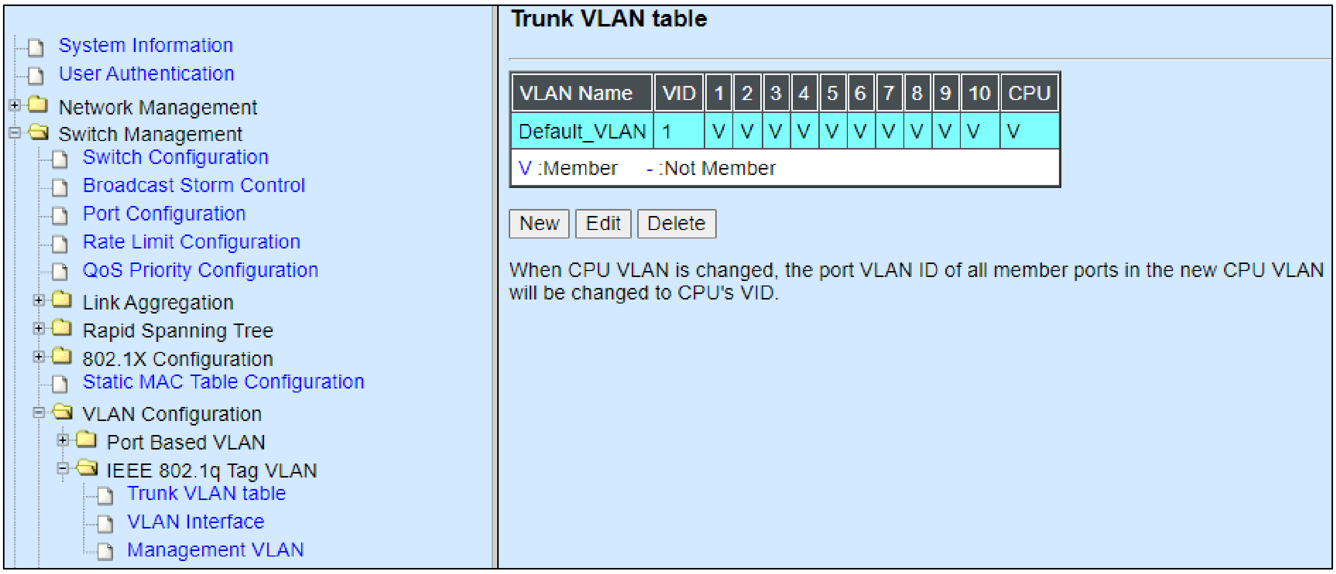
Max: It shows the maximum number available for configuration. The maximum is 10.

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

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

3.4.10.2 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	CPU
Default_VLAN	1	V	V	V	V	V	V	V	V	V	V	V

V :Member - :Not Member

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.

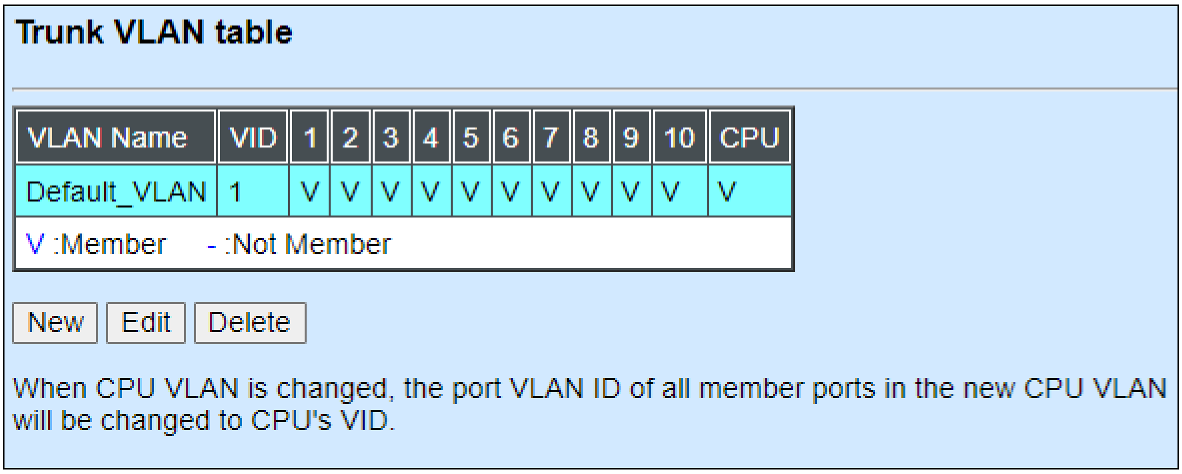
1. Trunk VLAN table: Edit or apply 802.1Q Tag VLAN settings.

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

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

3.4.10.2.1 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	CPU
Default_VLAN	1	V	V	V	V	V	V	V	V	V	V	V

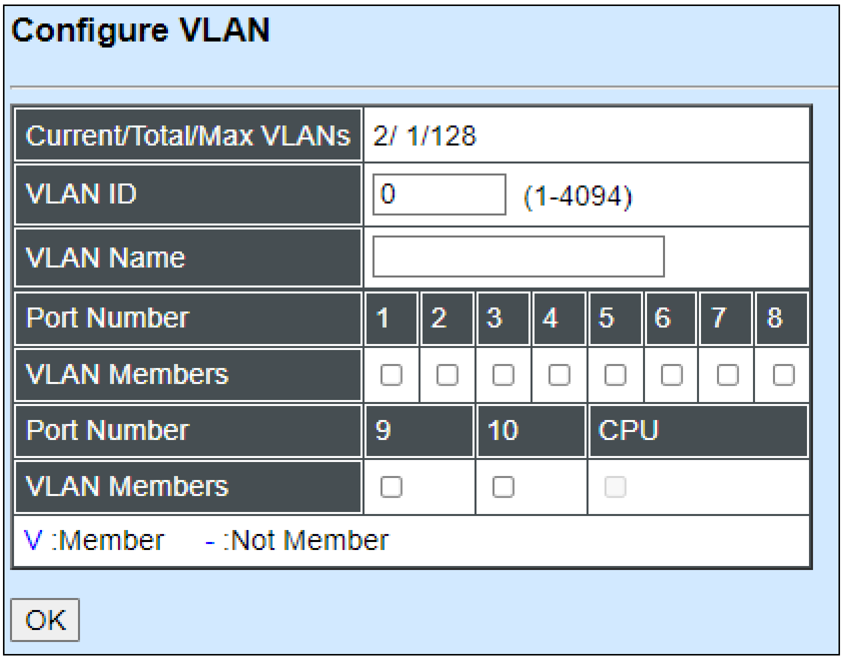
V :Member - :Not Member

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 modify the selected IEEE 802.1Q Tag VLAN setting.

Click **Delete** to remove an existing VLAN you select.

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



Configure VLAN

Current/Total/Max VLANs	2/ 1/128							
VLAN ID	0 (1-4094)							
VLAN Name								
Port Number	1	2	3	4	5	6	7	8
VLAN Members	□	□	□	□	□	□	□	□
Port Number	9		10		CPU			
VLAN Members	□		□		□			

V :Member - :Not Member

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.

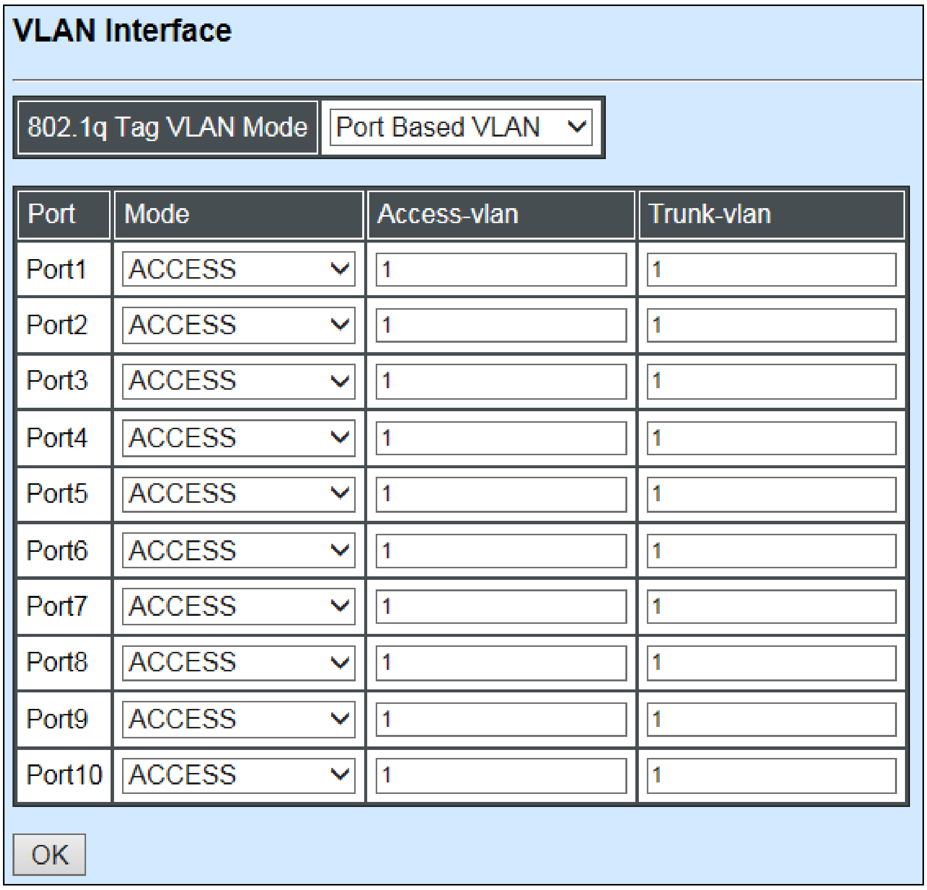
VLAN Name: Specify the name for the currently registered VLAN.

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

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

3.4.10.2.2 VLAN Interface

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



VLAN Interface

802.1q Tag VLAN Mode: Port Based VLAN

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

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.

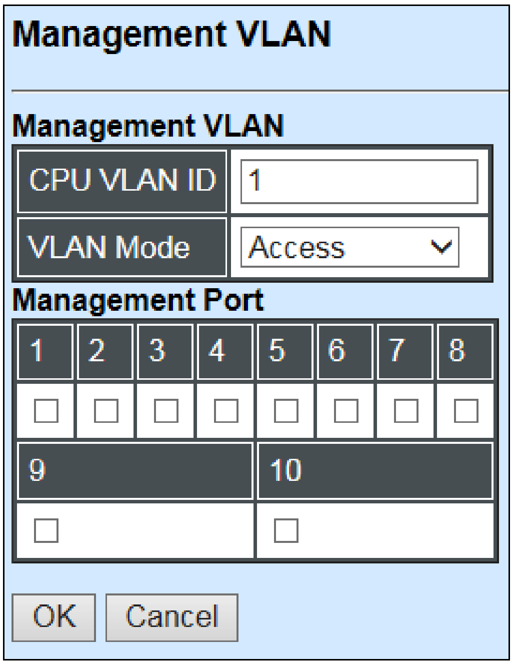
Access-VLAN: Specify the Access-VLAN ID (PVID) for each port. The default VLAN ID is “1”.

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.

3.4.10.2.3 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
□	□

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

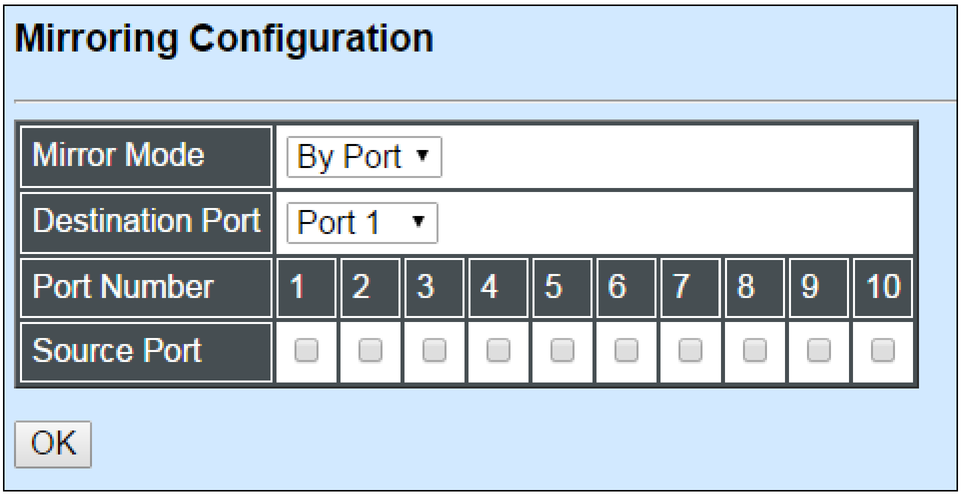
VLAN Mode: Specify the VLAN mode for management VLAN. Three options are available: ACCESS, TRUNK, TRUNK-NATIVE.

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

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

3.4.11 Mirroring Configuration

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



Mirroring Configuration

Mirror Mode	By Port ▾									
Destination Port	Port 1 ▾									
Port Number	1	2	3	4	5	6	7	8	9	10
Source Port	□	□	□	□	□	□	□	□	□	□

Mirror Mode: Either **disabled** or **By Port**.

Destination Port: Specify the port to which the traffic will be mirrored to.

Source Port: Specify the port(s) to which the traffic will be mirrored from as a source.

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

3.4.12 IGMP Snooping

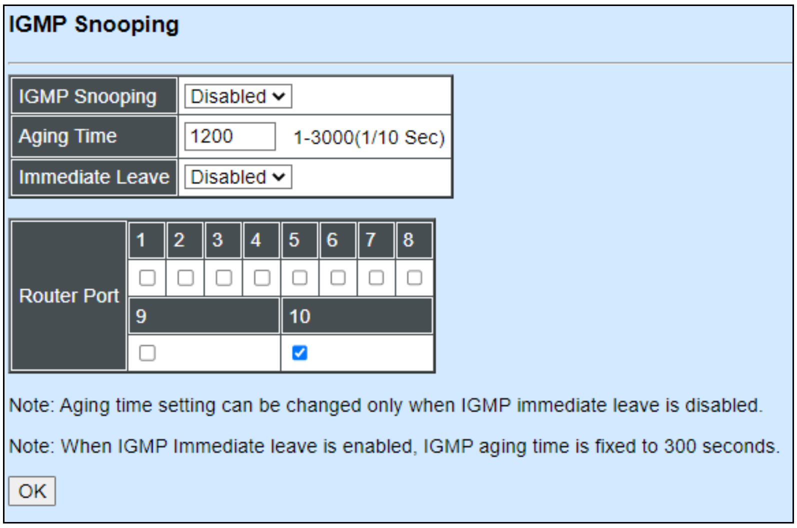
IGMP, Internet Group Management Protocol, is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It can be used for online streaming video and gaming, and allows 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.

Click the option **IGMP Snooping** from the **Management** menu and then the following screen page appears.



IGMP Snooping

IGMP Snooping	Disabled
Aging Time	1200 1-3000(1/10 Sec)
Immediate Leave	Disabled

Router Port	1	2	3	4	5	6	7	8
	□	□	□	□	□	□	□	□
	9				10			
	□				☑			

Note: Aging time setting can be changed only when IGMP immediate leave is disabled.

Note: When IGMP Immediate leave is enabled, IGMP aging time is fixed to 300 seconds.

IGMP Snooping: Enable or disable IGMP Snooping.

Aging Time: Specify the IGMP querier aging time. If the switch does not receive join packets from the end device within the specified time, the entry associated with this end device will be removed from the IGMP table. The default Aging Time is 1200 (1/10 second).

Immediate Leave: Enable or disable Immediate Leave function. This works only when IGMP Snooping is enabled. When Immediate Leave is enabled, the Managed Industrial Switch removes the port immediately when it detects IGMPv1 & IGMPv2 leave message on that port.

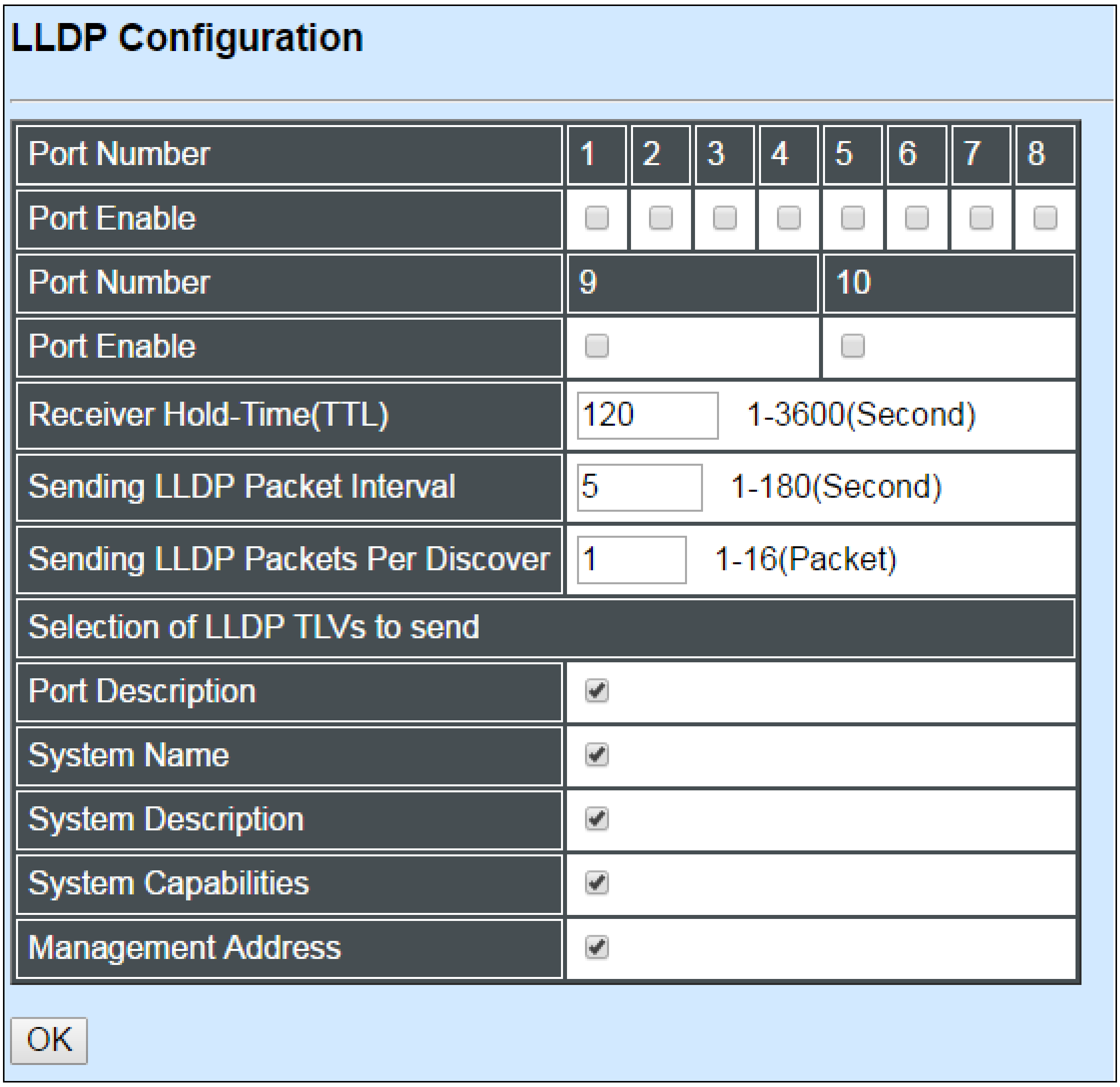
Router Port: When ports are connected to the IGMP administrative routers, they should be checked.

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

3.4.13 LLDP Configuration

LLDP stands for Link Layer Discovery Protocol and runs over data link layer which is used for network devices to send information about themselves to other directly connected devices on the network. By using LLDP, two devices running different network layer protocols can learn information about each other. A set of attributes are used to discover neighbor devices. These attributes contains type, length, and value descriptions and are referred to TLVs. Details such as port description, system name, system description, system capabilities, management address can be sent and received on this Managed Switch. Use Spacebar to select "ON" if you want to receive and send the TLV.

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



LLDP Configuration

Port Number	1	2	3	4	5	6	7	8
Port Enable	□	□	□	□	□	□	□	□
Port Number	9				10			
Port Enable	□				□			
Receiver Hold-Time(TTL)	120 1-3600(Second)							
Sending LLDP Packet Interval	5 1-180(Second)							
Sending LLDP Packets Per Discover	1 1-16(Packet)							
Selection of LLDP TLVs to send								
Port Description	☑							
System Name	☑							
System Description	☑							
System Capabilities	☑							
Management Address	☑							

Port: Check the checkbox to enable LLDP.

Receiver Hold-Time (TTL): Enter the amount of time for receiver hold-time in seconds. The Managed Switch will keep the information sent by the remote device for a period of time you specify here before discarding it.

Sending LLDP Packet Interval: Enter the time interval for updated LLDP packets to be sent.

Sending Packets Per Discover: Enter the amount of packets sent in each discover.

Delay LLDP Initialization: A period of time the Managed Switch will wait before the initial LLDP packet is sent.

Selection of LLDP TLVs to send: LLDP uses a set of attributes to discover neighbor devices. These attributes contains type, length, and value descriptions and are referred to TLVs. Details such as port description, system name, system description, system capabilities, management address can be sent from this Managed Switch.

3.4.14 Loop Detection

In a real network, it is possible the people misconnect the network cable to incur loop condition. In a worst case, the network is out of service thereafter. This section gives a guide to configure the Loop Detection function of the system to prevent the system from loop.

After a proper setting of Loop Detection function, the system detects loop condition by periodically sending loop detection packet. Once the system receives the loop detection packet from itself, it is claimed that it detects loop condition. Then, the system takes the following actions

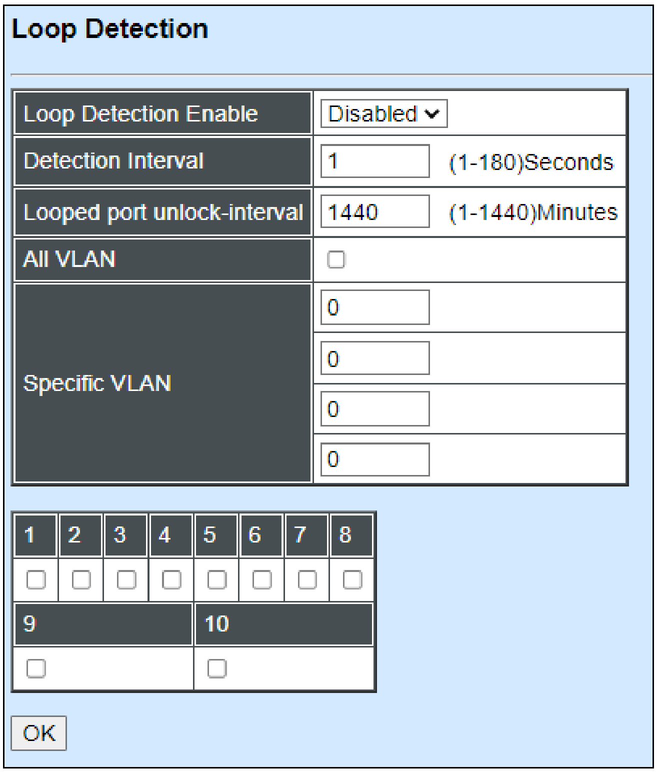
1. It blocks the relevant port to prevent broadcast storms. In other words, the system stops forwarding all the traffic via the looped port. However, the system will process the loop detection packet received on the looped port.
2. It slowly blinks the LED of looped port in orange.
3. It periodically sends loop detection packet to detect the existence of loop condition.

When the system does not receives any loop detection packet from itself for a period of configured **Looped port unlock-interval**. The system claims the loop condition disappears. Then, the system takes the following actions

1. It un-blocks the relevant port. In other words, the system normally forwards all the traffic via the relevant port.
2. It stops slowly blinking the LED of looped port in orange.
3. It periodically sends loop detection packet to detect the existence of loop condition.

***Note:** Under loop condition, the LED of looped port continues to slowly blink orange even the connected network cable is unplugged out of looped port.*

To set up Loop Detection function, select the option **Loop Detection Configuration** from the **Switch Management** menu and then the following screen page appears.



Loop Detection

Loop Detection Enable	Disabled	
Detection Interval	1	(1-180)Seconds
Looped port unlock-interval	1440	(1-1440)Minutes
All VLAN	□	
Specific VLAN	0 0 0 0	

1	2	3	4	5	6	7	8
□	□	□	□	□	□	□	□

9	10
□	□

OK

Loop Detection Enable: Check to enable the Loop Detection function on a system basis. The default setting is disabled.

Detection Interval: This is the time interval (in seconds) that the device will periodically send loop detection packets to detect the presence of looped network. The valid range is from 1 to 180 seconds. The default setting is 1 seconds.

Looped port unlock-interval: This is the time interval for the system to detect the existence of loop condition. System un-blocks the looped port if it does not receive any loop-detection packet during the configured unlock-interval. The unlock-interval can be set from 1 to 1440 minutes. The default setting is 1440 minutes.

Note:
1. Be aware that Looped port unlock-interval converted into seconds should be greater than or equal to Detection Interval seconds multiplied by 10. The ‘10’ is a magic number which is for the system to claims the loop detection disappears when the system does not receive the loop-detection packet from itself at least 10 times. In general, it can be summarized by a formula below:

60* “Looped port unlock-interval” ≧ 10* “Detection Interval“

2. When a port is detected as a looped port, the system keeps the looped port in blocking status until loop situation is gone. In other words, the system stops forwarding all the traffic via the looped port. However, the system will process the loop-detection packet received on the looped port.

All VLAN: Check All VLAN box to enable loop detection on all trunk-VLAN-vid configured in the **VLAN Interface** under **IEEE802.1q Tag VLAN** (Refer to Section 4.4.7.4.1)

***NOTE:** When All VLAN check-box is checked, it invalidates the configured "Specific VLAN".*

Specific VLAN: Set up loop detection on specified VLAN. The maximum number of VLAN ID is up to 4 sets.

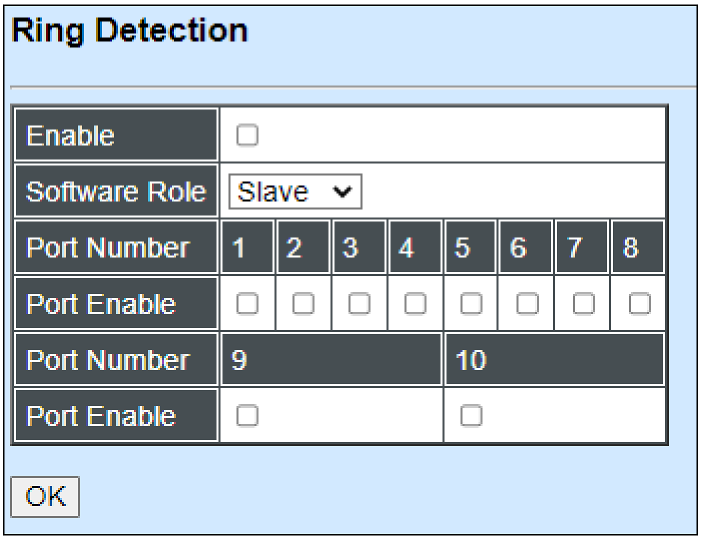
***NOTE:** The configured "Specific VLAN" takes effect when All VLAN check-box is unchecked.*

Port No.: Check to enable the Loop Detection function on the specific port(s).

***NOTE:** Loop Detection and RSTP (Rapid Spanning Tree Protocol) is not allowed to be enabled on the same port at the same time.*

3.4.15 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.



Ring Detection

Enable	□							
Software Role	Slave							
Port Number	1	2	3	4	5	6	7	8
Port Enable	□	□	□	□	□	□	□	□
Port Number	9				10			
Port Enable	□				□			

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

Software 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 possesses the ability of blocking or forwarding packet.

Slave: A role possesses the ability of forwarding packet only.

Port Enable: Set the port to "enabled" or "disabled". When clicking on the checkbox of the corresponding port number, the Ring Detection function will be enabled.

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

3.4.16 Fast Redundancy

Besides RSTP and Ring Detection as we previously mentioned, the employment of fast redundancy on your network will help protect mission-critical links against failures, avoid the occurrence of network loops, and keep network downtime to a minimum to assure the reliability of the network. With these network redundancy, it allows the user to set up redundant loops in a network to provide a backup data transmission route in the event of the disconnection or damage of the cables. By means of this important feature in the network recovery applications, you can be totally free from any loss resulting from the time spent in locating the cable that fails to connect.

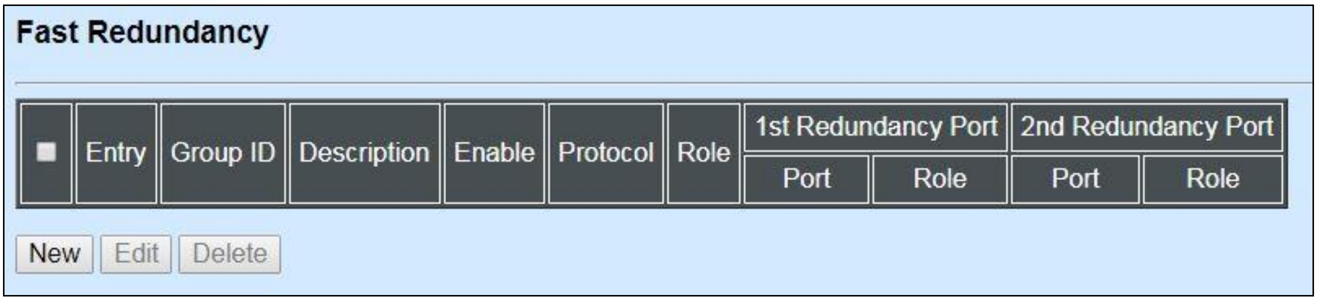
Fast redundancy provides **Fast Ring v2** and **Chain** two redundancy protocols, which allows you to configure 2 rings, 2 chains, or 1 ring & 1 chain at most for a switch.

Please note that all switches on the same ring or chain must be the ones with the same brand and configured using the same redundancy protocol when configuring a redundant ring or chain. You are not allowed to use switches with different brands or mix the Ring Detection, Fast Ring v2 and Chain protocols within the same ring or chain.

In the following table, it lists the difference among forementioned redundancy protocols for your evaluation when employing network redundancy on your network.

	Ring Detection	Fast Ring v2	Chain	RSTP
Topology	Ring	Ring	Ring	Ring
Recovery Time	<30 ms	<50 ms	<1 second (for copper ports) <50 ms (for fiber ports)	Up to 5 seconds

To configure the Fast Ring v2 or Chain fast redundancy, click the option **Fast Redundancy** from the **Switch Management** menu and then the following screen page appears.



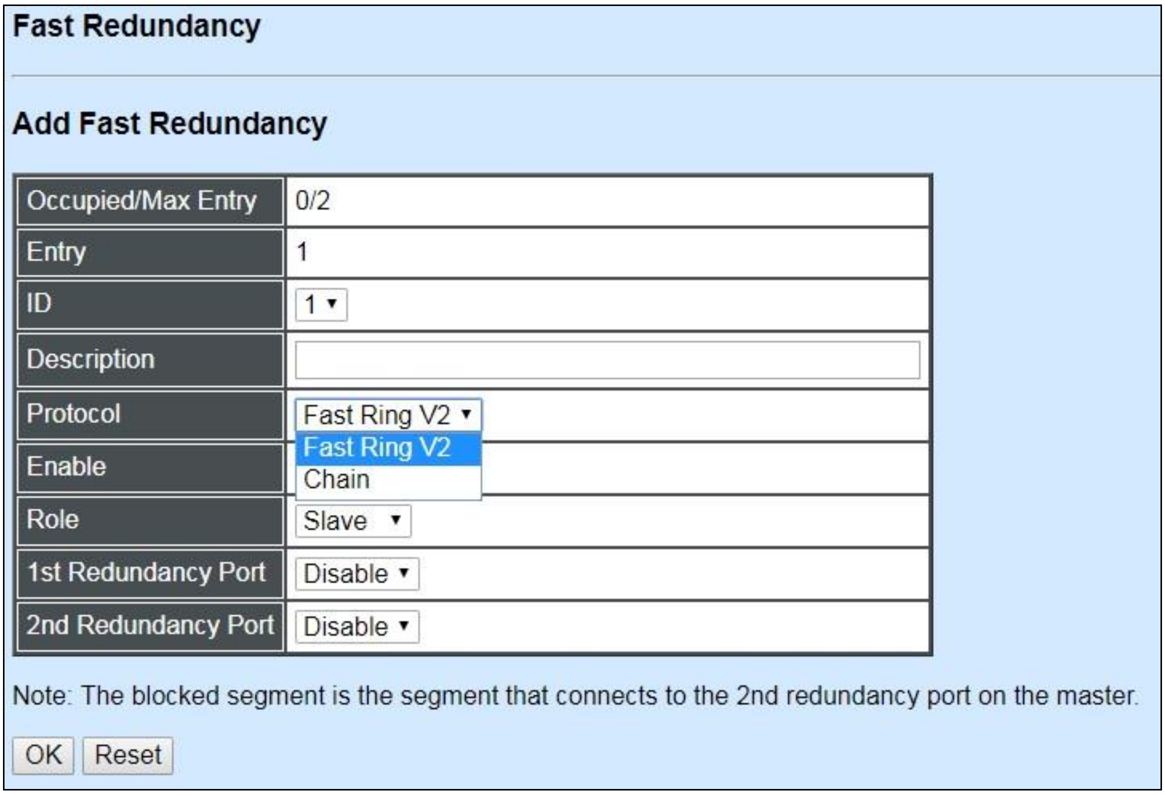
Fast Redundancy

□	Entry	Group ID	Description	Enable	Protocol	Role	1st Redundancy Port		2nd Redundancy Port	
							Port	Role	Port	Role

Click **New** to add a new fast redundancy and then the following screen page appears. Up to 2 sets of fast redundancy can be created.

Click **Edit** to modify the configuration of the selected fast redundancy by clicking on the checkbox of the corresponding entry.

Click **Delete** to remove an existing fast redundancy from the fast redundancy table by clicking on the checkbox of the corresponding entry.



Fast Redundancy

Add Fast Redundancy

Occupied/Max Entry	0/2
Entry	1
ID	1 ▾
Description	
Protocol	Fast Ring V2 ▾ Fast Ring V2 Chain
Enable	
Role	Slave ▾
1st Redundancy Port	Disable ▾
2nd Redundancy Port	Disable ▾

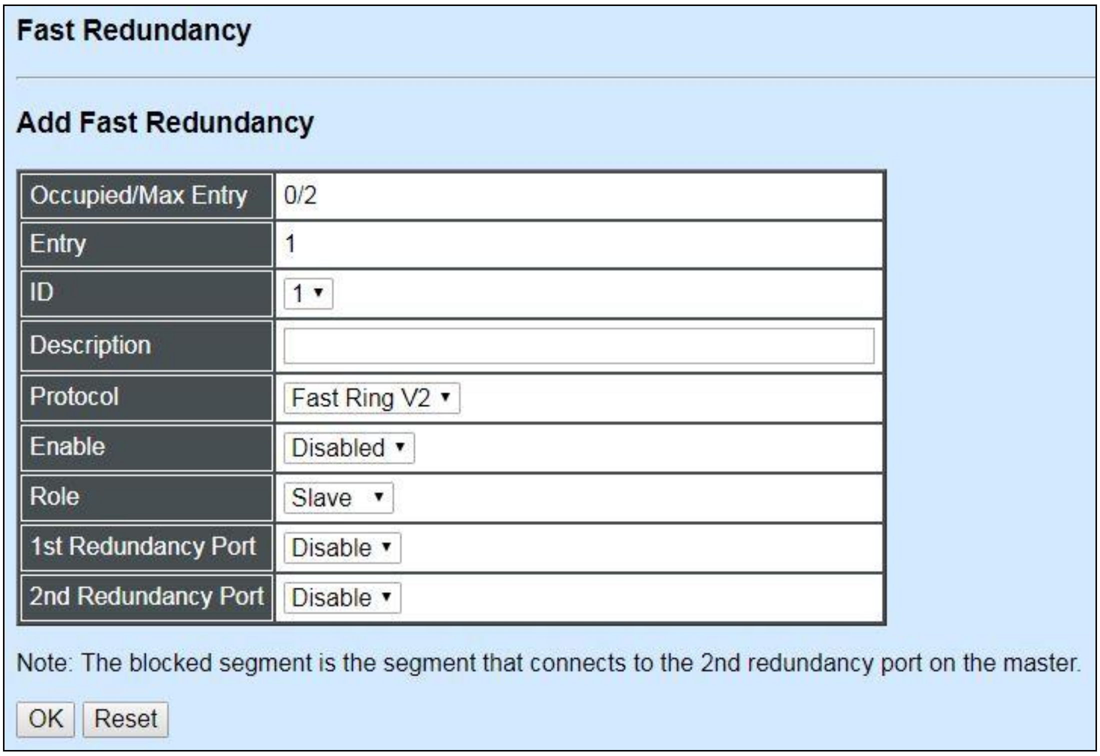
Note: The blocked segment is the segment that connects to the 2nd redundancy port on the master.

3.4.16.1 Fast Ring v2 Protocol

Fast Ring v2 protocol, the newer version of our Ring Detection, is to optimize communication redundancy and achieve a fast recovery time (<50 ms) on the network for up to 200 switches. Like Ring Detection, Fast Ring v2 protocol manually specifies one switch as the master of the network to identify which segment in the redundant ring acts as the backup path, and then automatically block packets from traveling through any of the network's redundant loops.

In the event that one branch of the ring disconnects from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can rebuild the communication with the rest of the network.

In the following subsection, we will explain how the backup path is selected for rings configured by Fast Ring v2 redundancy protocol.



Fast Redundancy

Add Fast Redundancy

Occupied/Max Entry	0/2
Entry	1
ID	1 ▾
Description	
Protocol	Fast Ring V2 ▾
Enable	Disabled ▾
Role	Slave ▾
1st Redundancy Port	Disable ▾
2nd Redundancy Port	Disable ▾

Note: The blocked segment is the segment that connects to the 2nd redundancy port on the master.

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total fast redundancy that have already been created.

Max: This shows the maximum number available for fast redundancy. The maximum number is 2.

Entry: View-only field. This shows the number of fast redundancy that is currently created.

ID: The group ID of the fast redundancy. Up to 2 group IDs can be supported.

Description: The description of the group.

Protocol: Include “Fast Ring v2” and “Chain” two redundancy protocols. To configure a Fast Ring v2 ring redundancy, pull down the menu of **Protocol** and choose **Fast Ring v2** as the protocol for the fast redundancy you configure.

Enable: Enable or disable the ring you configure.

Role: Pull down the menu of **Role** to assign the role of the Managed Switch as either Slave or Master when Fast Ring v2 protocol is chosen.

Master: A role possesses the ability of blocking or forwarding packets. Please note that the blocked segment is the segment that connects to the 2nd redundancy port on the master.

Slave: A role possesses the ability of forwarding packets only.

1st Redundancy Port: Specify which port of the Managed Switch to be acted as the first redundant port. Default value is **Disable**.

2nd Redundancy Port: Specify which port of the Managed Switch to be acted as the secondary redundant port. Default value is **Disable**.

Click **OK**, the new settings will be taken effect immediately. This entry will be listed on the fast redundancy table.

3.4.16.1.1 Configure a Ring Example using the Fast Ring v2 Protocol

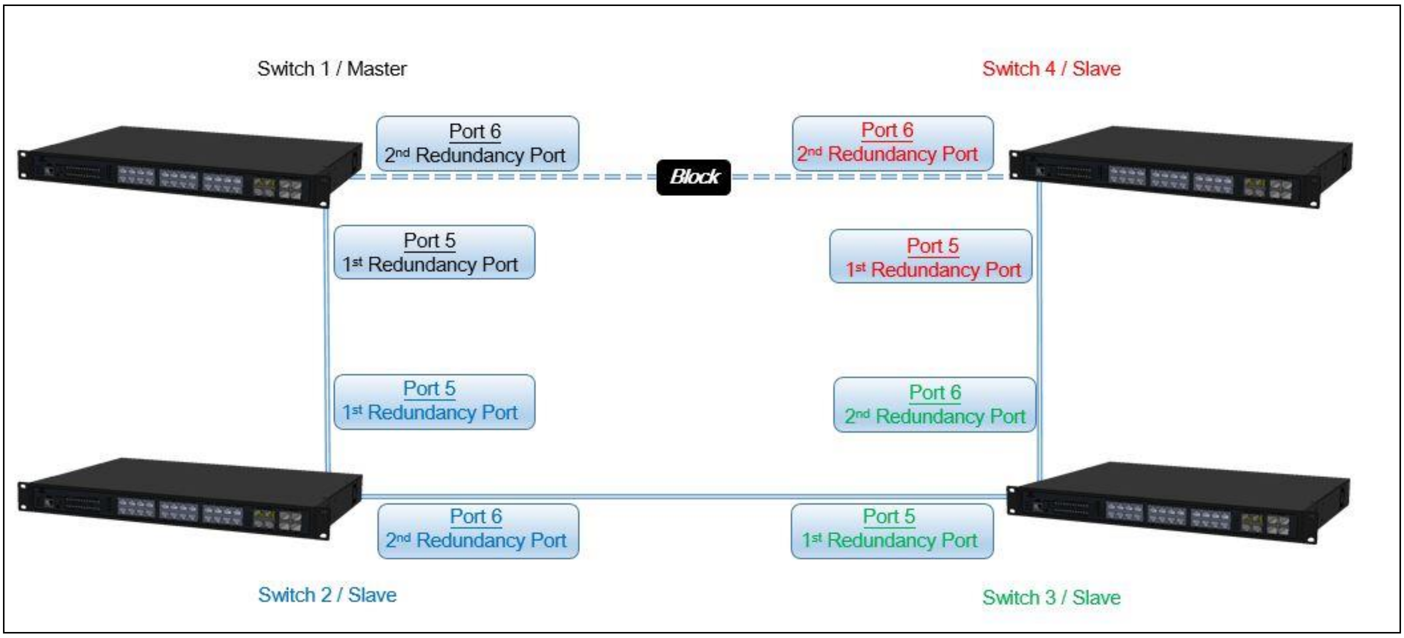


Fig. 1 Fast Ring v2 Example Diagram

The above topology often occurs using the Fast Ring v2 protocol and is configured as the following table.

Switch ID	Role	Redundancy Port	Physical Port
Switch 1	**Master**	1st Redundancy Port	Port 5
		2nd Redundancy Port	Port 6
Switch 2	Slave	1st Redundancy Port	Port 5
		2nd Redundancy Port	Port 6
Switch 3	Slave	1st Redundancy Port	Port 5
		2nd Redundancy Port	Port 6
Switch 4	Slave	1st Redundancy Port	Port 5
		2nd Redundancy Port	Port 6

Fig. 2 Fast Ring v2 Example Diagram

The scenario is described as below:

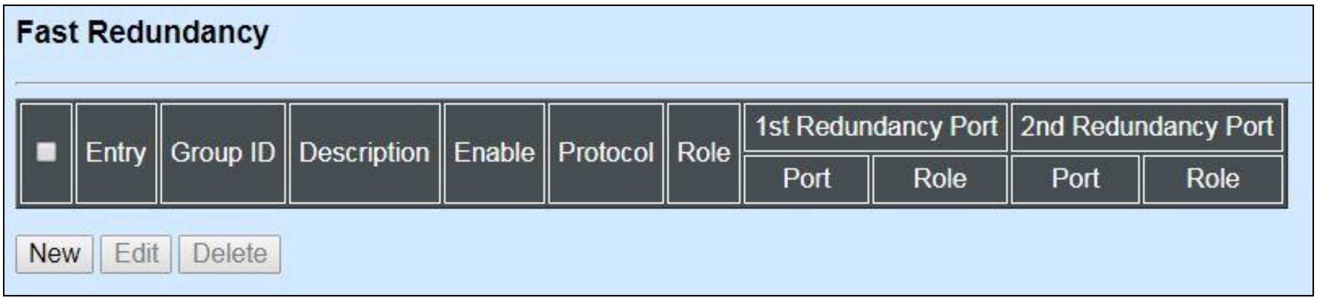
1. Disable DHCP client and set proper static IP address for Switch 1, 2, 3 & 4. In this example, Switch 1 is 192.168.0.101/24; Switch 2 is 192.168.0.102/24; Switch 3 is

192.168.0.103/24 and Switch 4 is 192.168.0.104/24.

2. On Switch 1~4, disable spanning tree protocol to avoid confliction with Fast Ring v2.

Just follow the procedures listed below for step-by-step instructions to configure a ring as Fig. 1 using the Fast Ring v2 protocol.

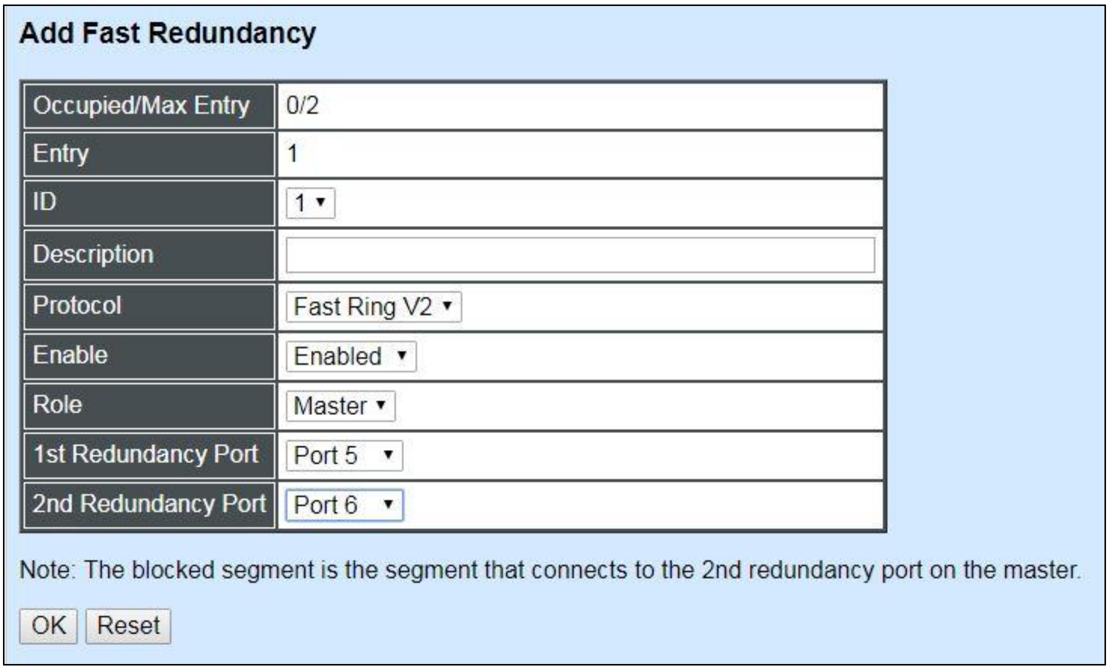
Step 1: Set up the Fast Ring v2 configuration on Switch 1.
1-1. Connect a computer to Switch 1 directly; do not connect to Port 5 & 6.
1-2. Login into the Switch 1 and go to **Switch Management > Fast Redundancy** for the Fast Ring v2 configuration. Click the **New** button to create a Fast Ring v2.



Fast Redundancy

□	Entry	Group ID	Description	Enable	Protocol	Role	1st Redundancy Port		2nd Redundancy Port	
							Port	Role	Port	Role

1-3. Please refer to each column parameter below, set “ID” = 1, “Protocol” = Fast Ring v2, “Enable” = Enabled, “Role” = Master, “1st Redundancy Port” = Port 5 & “2nd Redundancy Port” = Port 6, click **OK** when completing the Fast Ring v2 configuration for Switch 1.



Add Fast Redundancy

Occupied/Max Entry	0/2
Entry	1
ID	1 ▾
Description	
Protocol	Fast Ring V2 ▾
Enable	Enabled ▾
Role	Master ▾
1st Redundancy Port	Port 5 ▾
2nd Redundancy Port	Port 6 ▾

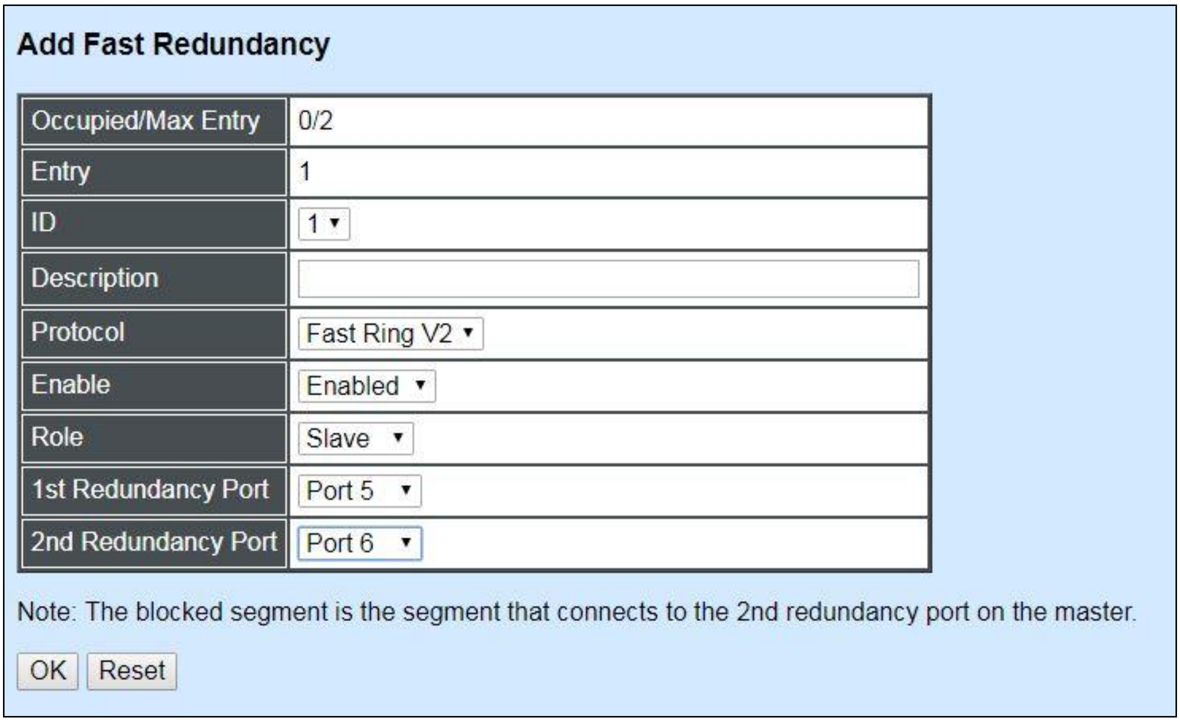
Note: The blocked segment is the segment that connects to the 2nd redundancy port on the master.

Step 2: Set up the Fast Ring v2 configuration on Switch 2, 3 & 4.

2-1. Connect a computer to Switch 2, 3 & 4 directly; do not connect to Port 5 & 6.

2-2. Login into the Switch 2, 3 & 4 and also go to **Switch Management > Fast Redundancy** for the Fast Ring v2 configuration. Click the **New** button to create a Fast Ring v2.

2-3. Please refer to each column parameter below, set "ID" = 1, "Protocol" = Fast Ring v2, "Enable" = Enabled, "Role" = Slave, "1st Redundancy Port" = Port 5 & "2nd Redundancy Port" = Port 6, click **OK** when completing the Fast Ring v2 configuration for Switch 2, 3 & 4.



Add Fast Redundancy

Occupied/Max Entry	0/2
Entry	1
ID	1
Description	
Protocol	Fast Ring V2
Enable	Enabled
Role	Slave
1st Redundancy Port	Port 5
2nd Redundancy Port	Port 6

Note: The blocked segment is the segment that connects to the 2nd redundancy port on the master.

NOTE: *To avoid the occurrence of loop, please do not connect Switch 1, 2, 3 & 4 together in the ring topology before the end of Fast Ring v2 configuration.*

Step 3: Follow the configuration to connect the Switch 1, 2, 3 & 4 together to establish the Fast Ring v2 application.

3.4.16.2 Chain Protocol

Chain protocol is an advanced software technology that gives network administrators the flexibility to build any type of redundant network topology. It also enables the network to recover in less than 50ms for up to 200 switches if at any time a segment of the chain fails.

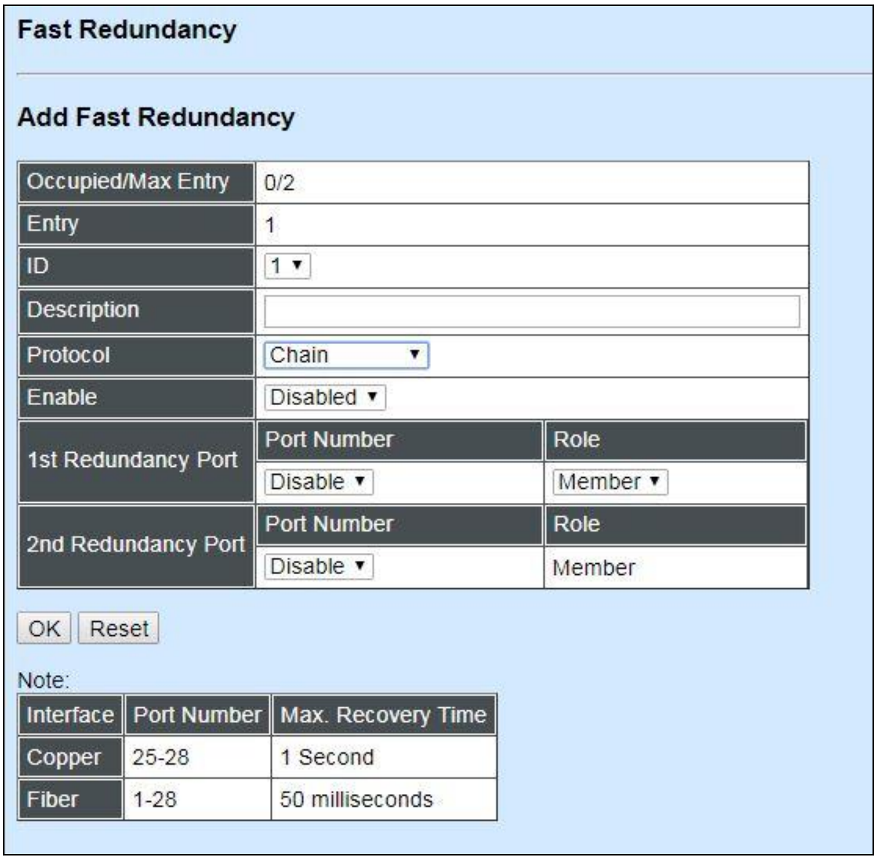
When employing a Chain in your network, you first connect the Managed Switches in a chain, and then simply link the two ends of this chain to an Ethernet network. All switches in the chain can be fallen into three parts:

- A Head switch,
- A Tail switch,
- Member switches.

The Head port of the Head switch usually acts as the external port for the entire chain, the Tail port of the Tail switch acts as the blocked port. When the Head port is disconnected, the Tail port will be immediately activated for the data transferring.

The Chain redundancy protocol can be applied to the networks with a complex topology. If the network uses a multi-ring architecture, Chain protocol can be the best solution to create flexible and scalable topologies with a fast media recovery time.

In the following subsection, we will explain how the backup path is selected for chains configured by the Chain redundancy protocol.



Fast Redundancy

Add Fast Redundancy

Occupied/Max Entry	0/2	
Entry	1	
ID	1 ▾	
Description		
Protocol	Chain ▾	
Enable	Disabled ▾	
1st Redundancy Port	Port Number	Role
	Disable ▾	Member ▾
2nd Redundancy Port	Port Number	Role
	Disable ▾	Member

Note:

Interface	Port Number	Max. Recovery Time
Copper	25-28	1 Second
Fiber	1-28	50 milliseconds

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total fast redundancy that have already been created.

Max: This shows the maximum number available for fast redundancy. The maximum number is 2.

Entry: View-only field. This shows the number of fast redundancy that is currently created.

ID: The group ID of the fast redundancy. Up to 2 group IDs can be supported.

Description: The description of the group.

Protocol: Include “Fast Ring v2” and “Chain” two redundancy protocols. To configure a chain redundancy, pull down the menu of **Protocol** and choose **Chain** as the protocol for the fast redundancy you configure.

Enable: Enable or disable the chain you configure.

Port Number of 1st Redundancy Port: Specify which port of Managed Switch to be acted as the first redundant port. Default value is **Disable**.

Role of 1st Redundancy Port: Include **Head**, **Member** and **Tail** three types of roles.

Port Number of 2nd Redundancy Port: Specify which port of Managed Switch to be acted as the secondary redundant port. Default value is **Disable**.

Role of 2nd Redundancy Port: View-only field. Only **Member** role is allowed.

Click **OK**, the new settings will be taken effect immediately. This entry will be listed on the fast redundancy table.

3.4.16.2.1 Configure a Chain Example using the Chain Protocol

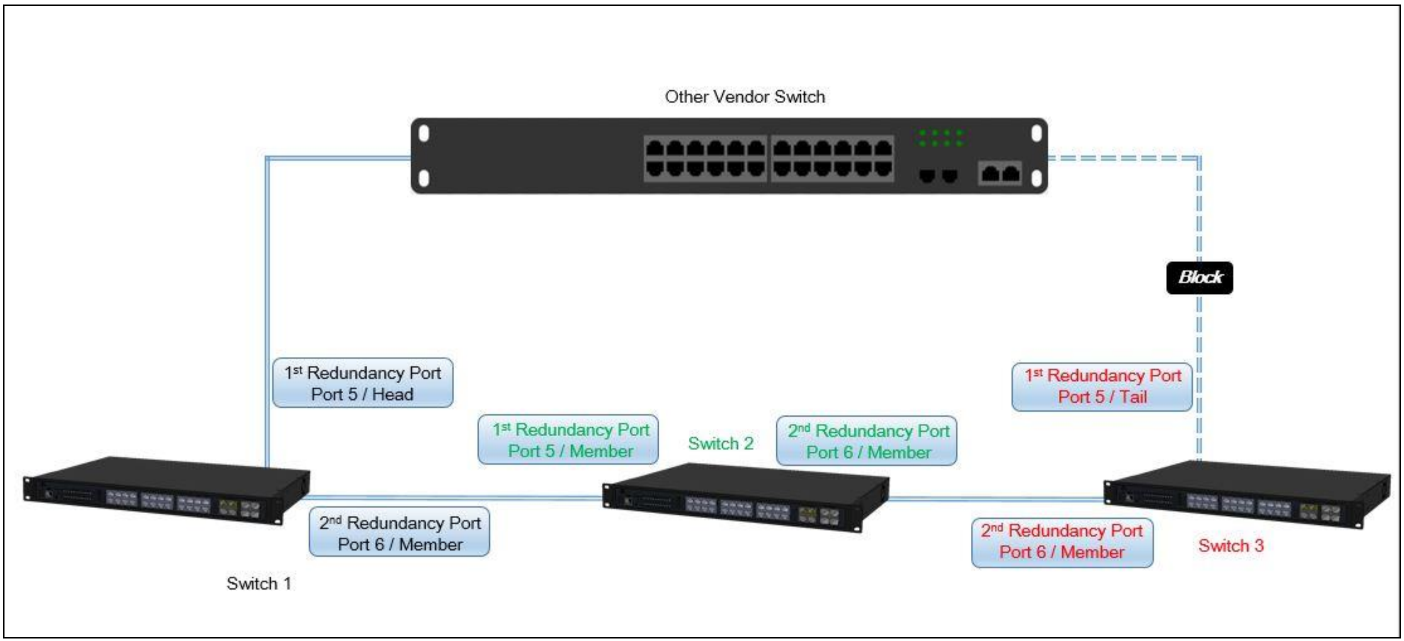


Fig. 3 Chain Example Diagram

The above topology often occurs using the Chain protocol and is configured as the following table.

Switch ID	Redundancy Port	Physical Port	Port Role
Switch 1	1st Redundancy Port	Port 5	**Head**
	2nd Redundancy Port	Port 6	Member
Switch 2	1st Redundancy Port	Port 5	Member
	2nd Redundancy Port	Port 6	Member
Switch 3	1st Redundancy Port	Port 5	**Tail**
	2nd Redundancy Port	Port 6	Member

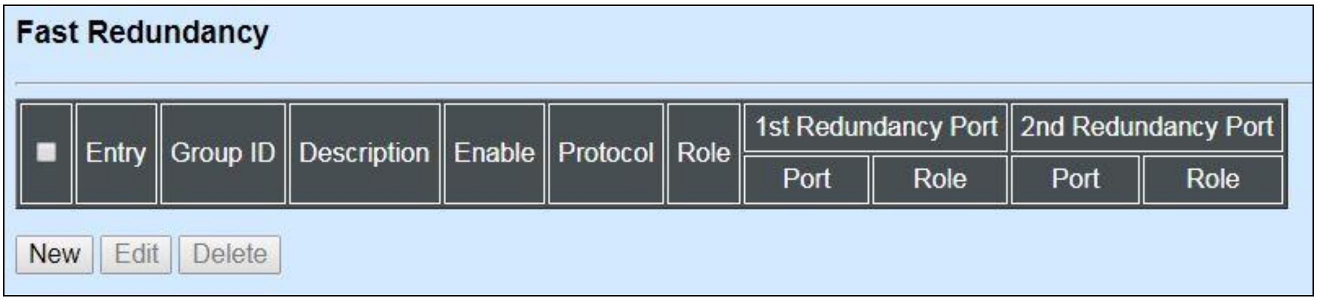
Fig. 4 Chain Configuration

The scenario is described as below:

1. Disable DHCP client and set proper static IP address for Switch 1, 2, & 3. In this example, Switch 1 is 192.168.0.101/24; Switch 2 is 192.168.0.102/24 and Switch 3 is 192.168.0.103/24.
2. On Switch 1~3, disable spanning tree protocol to avoid confliction with Chain.

Just follow the procedures listed below for step-by-step instructions to configure a chain as Fig. 3 using the Chain protocol.

Step 1: Set up the Chain configuration on Switch 1.
1-1. Connect a computer to Switch 1 directly; do not connect to Port 5 & 6.
1-2. Login into the Switch 1 and go to **Switch Management > Fast Redundancy** for the chain configuration. Click the **New** button to create a chain.

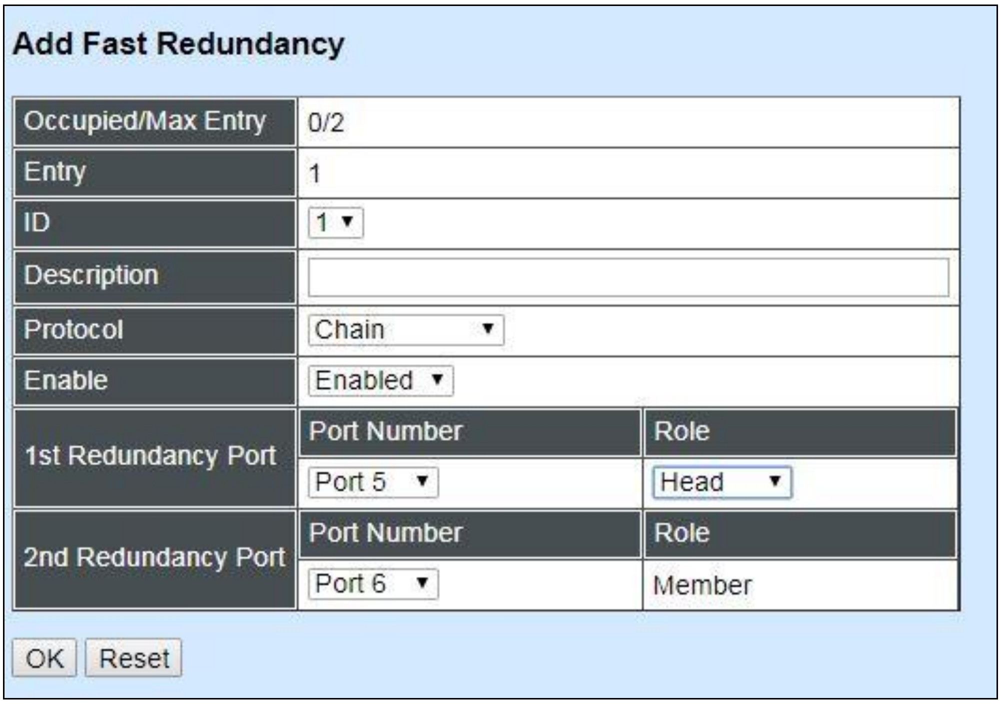


Fast Redundancy

■	Entry	Group ID	Description	Enable	Protocol	Role	1st Redundancy Port		2nd Redundancy Port	
							Port	Role	Port	Role

New Edit Delete

1-3. Please refer to each column parameter below, set “ID” = 1, “Protocol” = Chain, “Enable” = Enabled, “1st Redundancy Port / Port Number” = Port 5, “1st Redundancy Port / Role” = Head, & “2nd Redundancy Port / Port Number” = Port 6, click **OK** when completing the chain configuration for Switch 1.



Add Fast Redundancy

Occupied/Max Entry	0/2	
Entry	1	
ID	1 ▼	
Description		
Protocol	Chain ▼	
Enable	Enabled ▼	
1st Redundancy Port	Port Number	Role
	Port 5 ▼	Head ▼
2nd Redundancy Port	Port Number	Role
	Port 6 ▼	Member

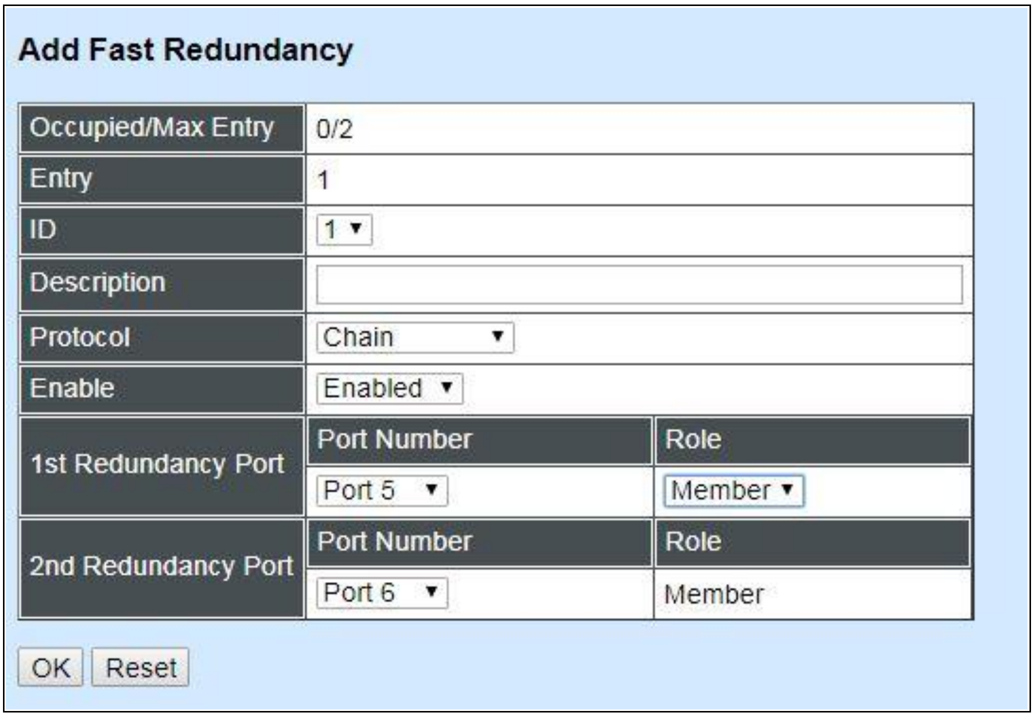
OK Reset

Step 2: Set up the Chain configuration on Switch 2.

2-1. Connect a computer to Switch 2 directly; do not connect to Port 5 & 6.

2-2. Login into the Switch 2 and also go to **Switch Management > Fast Redundancy** for the chain configuration. Click the **New** button to create a chain.

2-3. Please refer to each column parameter below, set “ID” = 1, “Protocol” = Chain, “Enable” = Enabled, “1st Redundancy Port / Port Number” = Port 5, “1st Redundancy Port / Role” = Member, & “2nd Redundancy Port / Port Number” = Port 6, click **OK** when completing the chain configuration for Switch 2.



Add Fast Redundancy

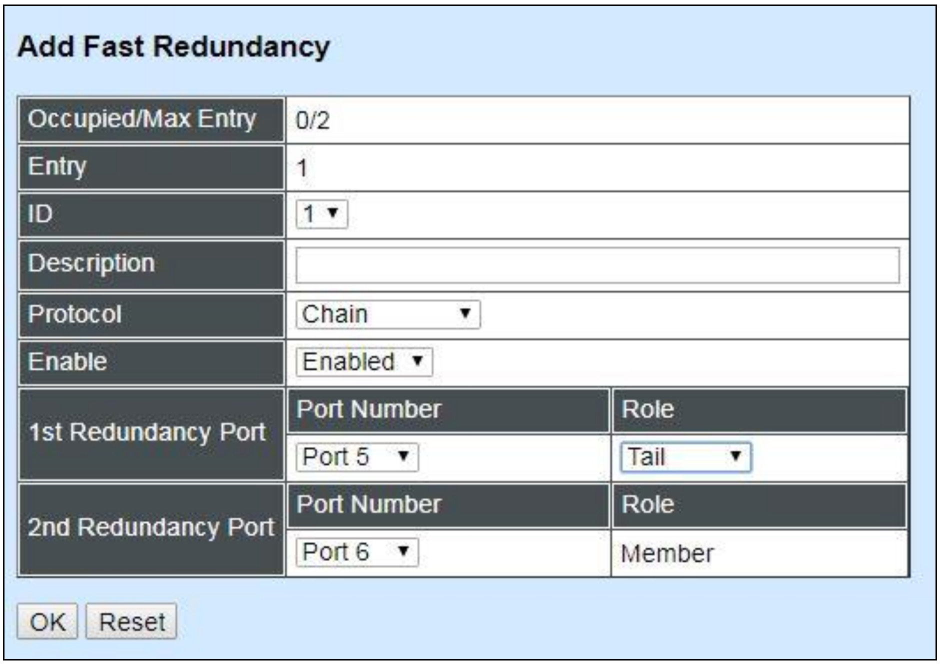
Occupied/Max Entry	0/2	
Entry	1	
ID	1 ▼	
Description		
Protocol	Chain ▼	
Enable	Enabled ▼	
1st Redundancy Port	Port Number	Role
	Port 5 ▼	Member ▼
2nd Redundancy Port	Port Number	Role
	Port 6 ▼	Member

Step 3: Set up the Chain configuration on Switch 3.

3-1. Connect a computer to Switch 3 directly; do not connect to Port 5 & 6.

3-2. Login into the Switch 3 and also go to **Switch Management > Fast Redundancy** for the chain configuration. Click the **New** button to create a chain.

3-3. Please refer to each column parameter below, set “ID” = 1, “Protocol” = Chain, “Enable” = Enabled, “1st Redundancy Port / Port Number” = Port 5, “1st Redundancy Port / Role” = Tail, & “2nd Redundancy Port / Port Number” = Port 6, click **OK** when completing the chain configuration for Switch 3.



Add Fast Redundancy

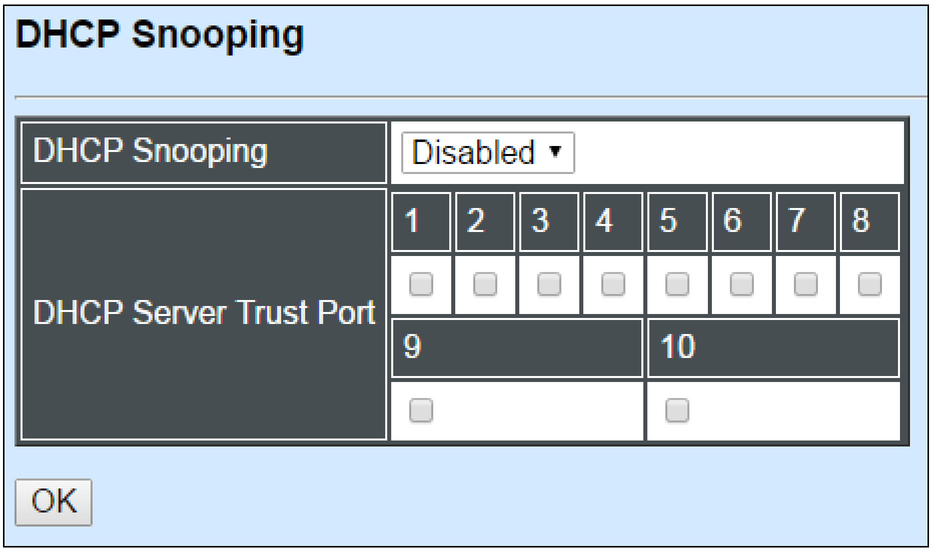
Occupied/Max Entry	0/2	
Entry	1	
ID	1 ▼	
Description		
Protocol	Chain ▼	
Enable	Enabled ▼	
1st Redundancy Port	Port Number	Role
	Port 5 ▼	Tail ▼
2nd Redundancy Port	Port Number	Role
	Port 6 ▼	Member

NOTE: *To avoid the occurrence of loop, please do not connect Switch 1, 2, & 3 together in the chain topology before the end of Chain configuration.*

Step 4: Follow the configuration to connect the Switch 1, 2, & 3 together to establish Chain application.

3.4.17 DHCP Snooping

Select the option **DHCP Snooping** from the **Switch Management** menu and then the following screen page appears.



DHCP Snooping

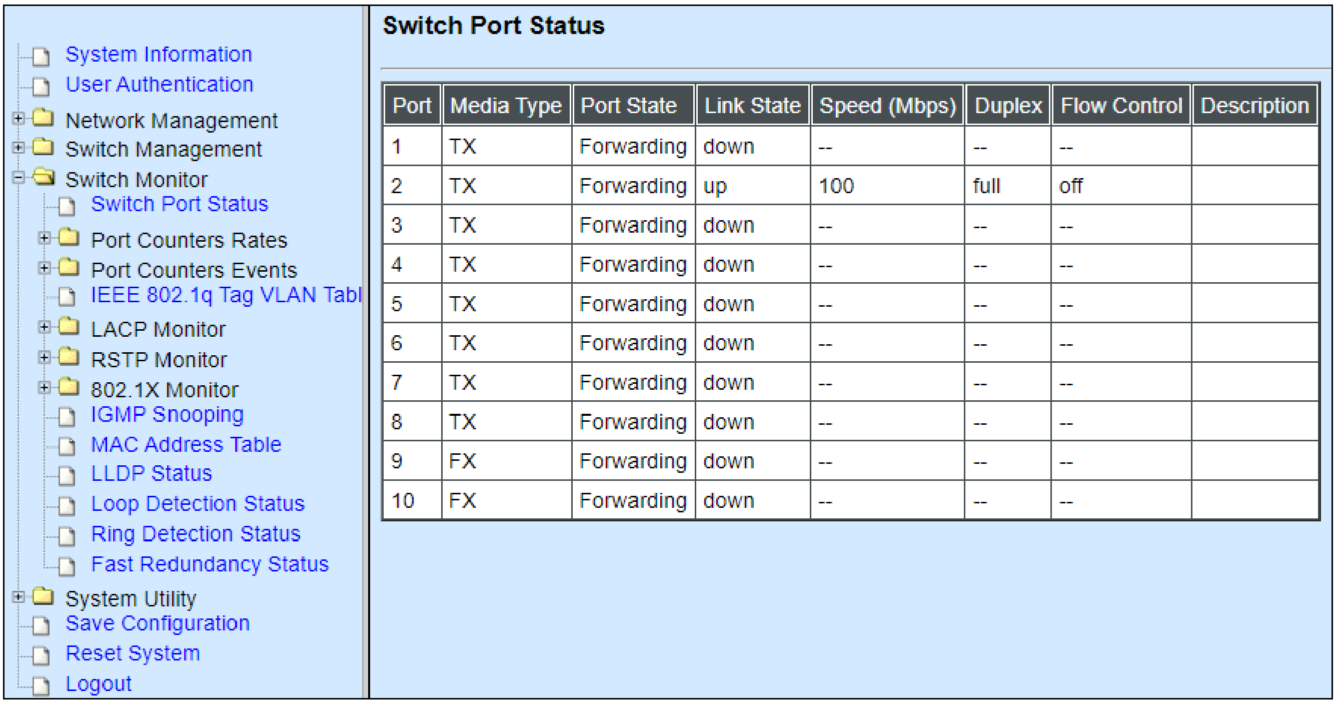
DHCP Snooping	Disabled ▾							
DHCP Server Trust Port	1	2	3	4	5	6	7	8
	□	□	□	□	□	□	□	□
	9				10			
	□				□			

DHCP Snooping: Enable or disable DHCP Snooping function.

DHCP Server Trust Port: Specify designated port to be Trust Port that can give you “offer” from DHCP server. Check any port box to enable it.

3.5 Switch Monitor

Switch Monitor allows users to monitor the real-time operation status of the Managed Industrial 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	up	100	full	off	
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	--	--	--	

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

2. **Port Counters Rates:** This folder includes Port Traffic Statistics (Rates), Port Packet Error Statistics (Rates), and Port Packet Analysis Statistics (Rates).

3. **Port Counters Events:** This folder includes Port Traffic Statistics (Events), Port Packet Error Statistics (Events), and Port Packet Analysis Statistics (Events).

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

5. **LACP Monitor:** View the LACP port status and statistics.

6. **RSTP Monitor:** View RSTP VLAN Bridge, Port Status, and Statistics.

7. **802.1X Monitor:** View the 802.1X port status and statistics.

8. **IGMP Snooping:** View a list of IGMP queries' information in VLAN(s) such as VLAN ID, Querier and reports.

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

10. **LLDP Status:** View the TLV information sent by the connected device with LLDP-enabled.

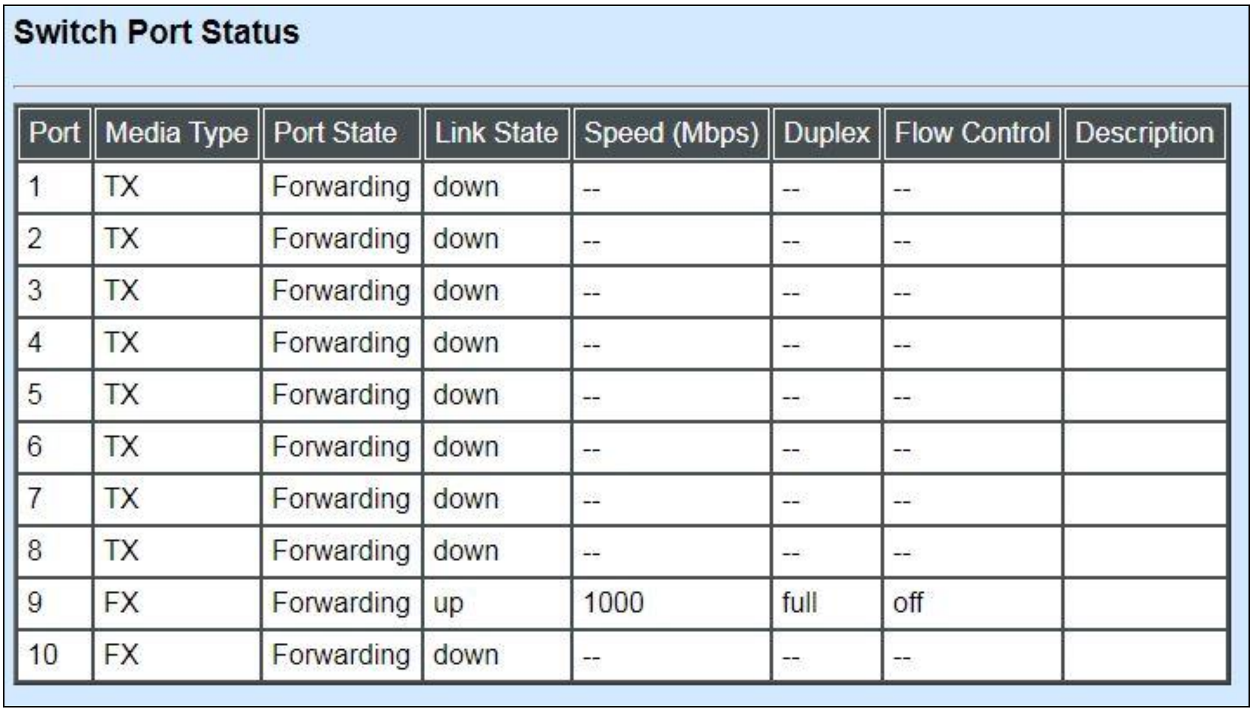
11. **Loop Detection Status:** View the Loop Detection status of each port.

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

13. **Fast Redundancy Status:** View the current Fast Ring v2 and Chain status.

3.5.1 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	up	1000	full	off	
10	FX	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: This shows each port's state which can be Disabled, Blocking/Listening, Learning or Forwarding.

> **Disabled:** A port in this state does not participate in frame relay or the operation of the Spanning Tree Algorithm and Protocol if any.
>
> **Blocking:** A Port in this state does not participate in frame relay; thus, it prevents frame duplication arising from multiple paths existing in the active topology of Bridged LAN.
>
> **Learning:** A port in this state prepares to participate in frame relay. Frame relay is temporarily disabled in order to prevent temporary loops, which may occur in a Bridged

LAN during the lifetime of this state as the active topology of the Bridged LAN changes. Learning is enabled to allow information to be acquired prior to frame relay in order to reduce the number of frames that are unnecessarily relayed.

Forwarding: A port in this state participates in frame relay. Packets can be forwarded only when port state is forwarding.

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.

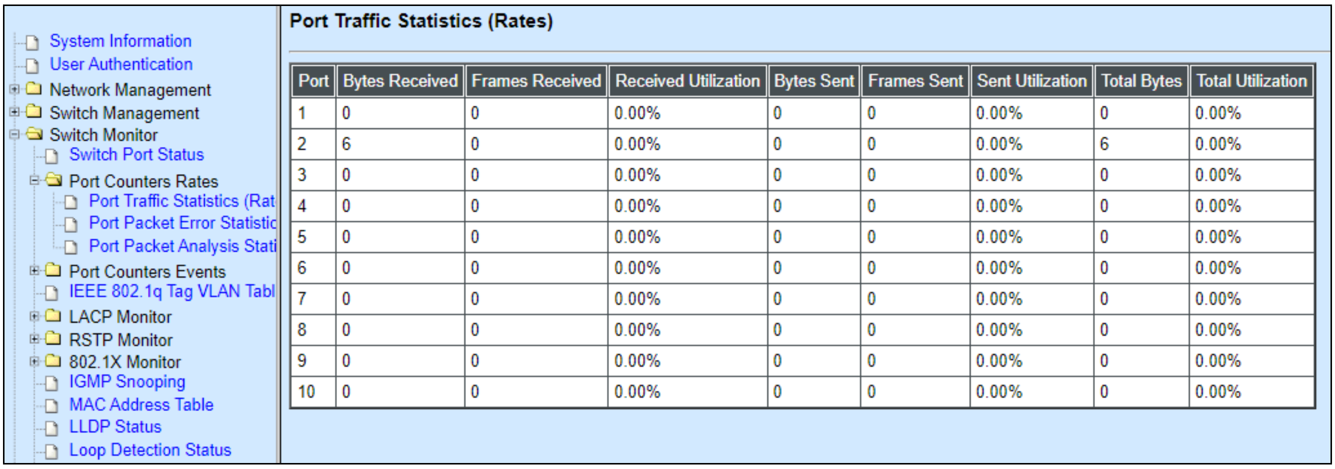
Duplex: It shows the current operation Duplex mode of each port, either Full or Half.

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”.

3.5.2 Port Counters Rates

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



Port Traffic Statistics (Rates)

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	6	0	0.00%	0	0	0.00%	6	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%

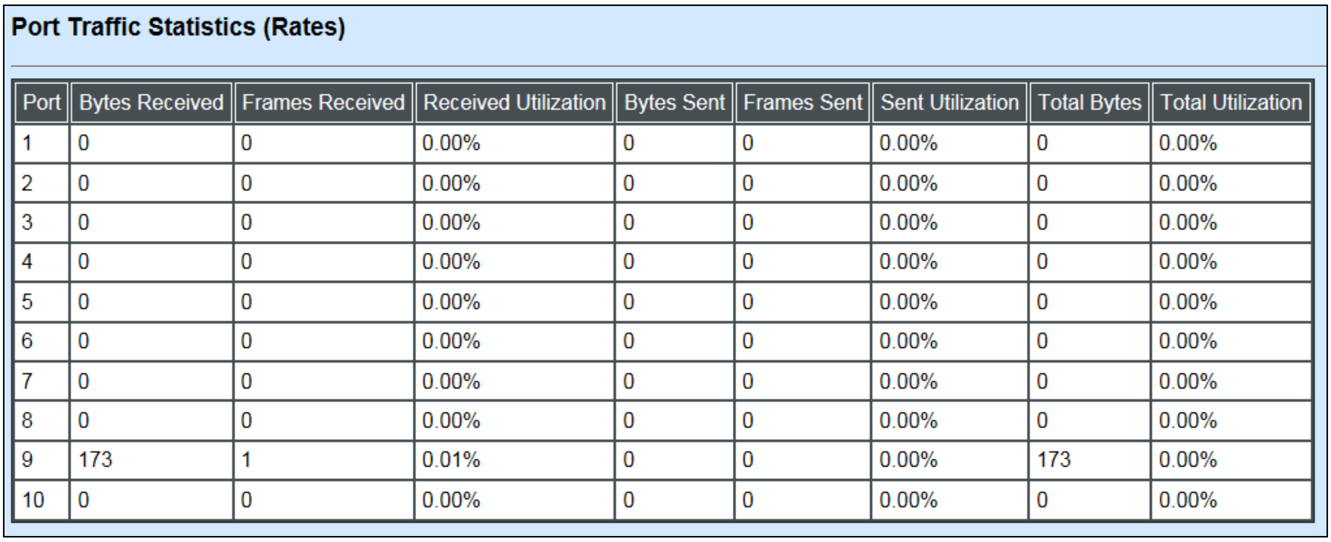
1. **Port Traffic Statistics (Rates):** View the number of bytes received, frames received, bytes sent, frames sent, total bytes, etc.

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.

3.5.2.1 Port Traffic Statistics (Rates)

The following screen page appears if you choose **Port Counters Rates** and then select **Port Traffic Statistics (Rates)**.



Port Traffic Statistics (Rates)

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	173	1	0.01%	0	0	0.00%	173	0.00%
10	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.

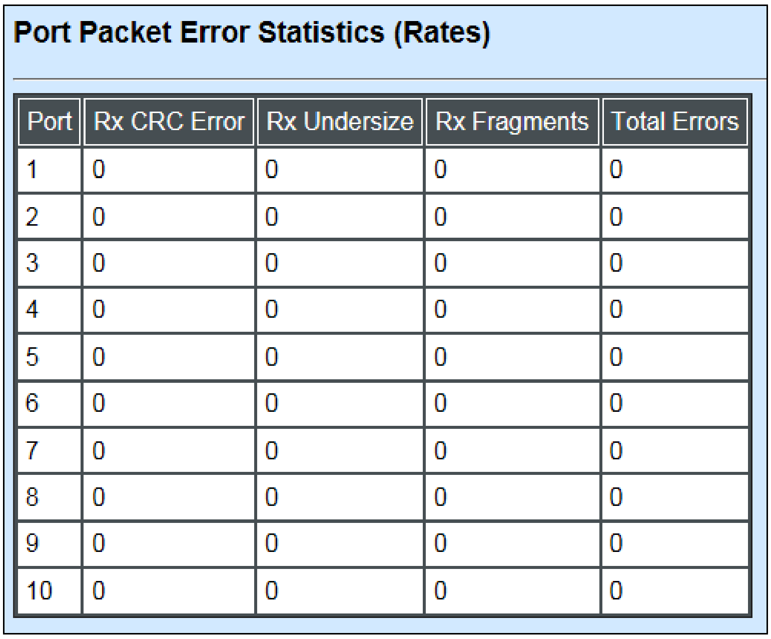
Sent Utilization: The ratio of each port's sending traffic to the port's current bandwidth.

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.

3.5.2.2 Port Packet Error Statistics (Rates)

The following screen page appears if you choose **Port Counters Rates** and then select **Port Packet Error Statistics (Rates)**.



Port Packet Error Statistics (Rates)

Port	Rx CRC Error	Rx Undersize	Rx Fragments	Total Errors
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

RX CRC Error: The number of packets with wrong FCS received.

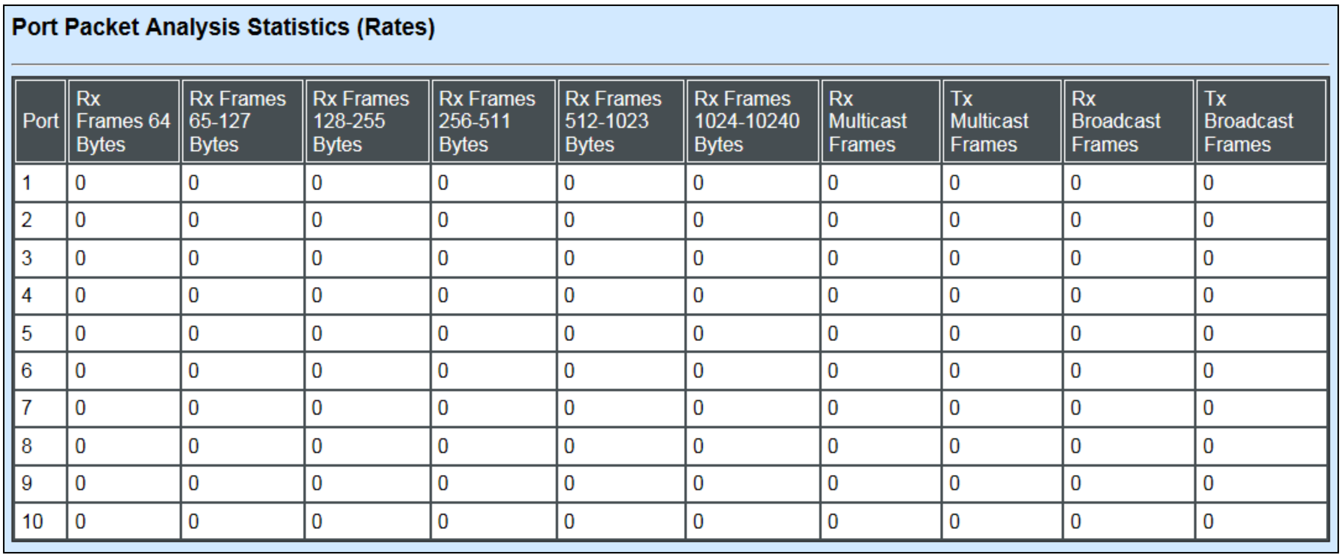
RX Undersize: Undersize frames received.

RX Fragments: Fragment frames received.

Total Errors: The number of total errors.

3.5.2.3 Port Packet Analysis Statistics (Rates)

The following screen page appears if you choose **Port Counters Rates** and then select **Port Packet Analysis Statistics (Rates)**.



Port Packet Analysis Statistics (Rates)

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 1024-10240 Bytes	Rx Multicast Frames	Tx Multicast Frames	Rx Broadcast Frames	Tx Broadcast Frames
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

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.

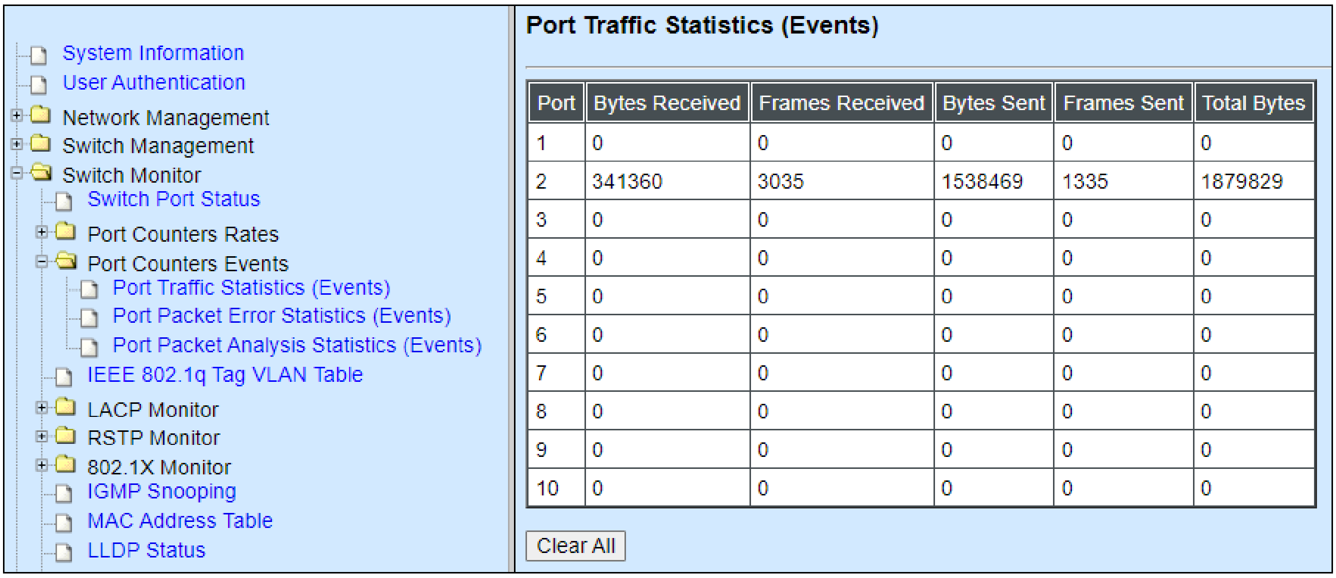
TX Multicast Frames: Good multicast packets sent.

RX Broadcast Frames: Good broadcast frames received.

TX Broadcast Frames: Good broadcast packets sent.

3.5.3 Port Counters Events

To view the accumulated statistics of the Managed Industrial Switch, click **Port Counters Events** folder and then three options appear. The event mode of port counters will be re-calculated when that counter is reset or cleared.



Port Traffic Statistics (Events)

Port	Bytes Received	Frames Received	Bytes Sent	Frames Sent	Total Bytes
1	0	0	0	0	0
2	341360	3035	1538469	1335	1879829
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

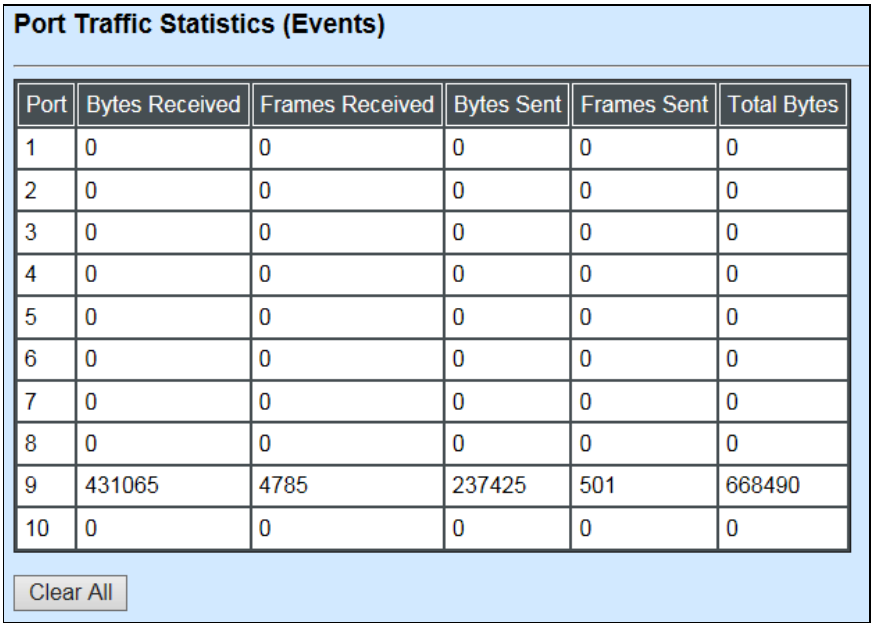
1. **Port Traffic Statistics (Events):** View the number of bytes received, frames received, bytes sent, frames sent, and total bytes.

2. **Port Packet Error Statistics (Events):** View the number of CRC errors, undersize frames, fragment frames, etc.

3. **Port Packet Analysis Statistics (Events):** View each port's frame analysis.

3.5.3.1 Port Traffic Statistics (Events)

The following screen page appears if you choose **Port Counters Events** and then select **Port Traffic Statistics (Events)**.



Port Traffic Statistics (Events)

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	431065	4785	237425	501	668490
10	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 each port.

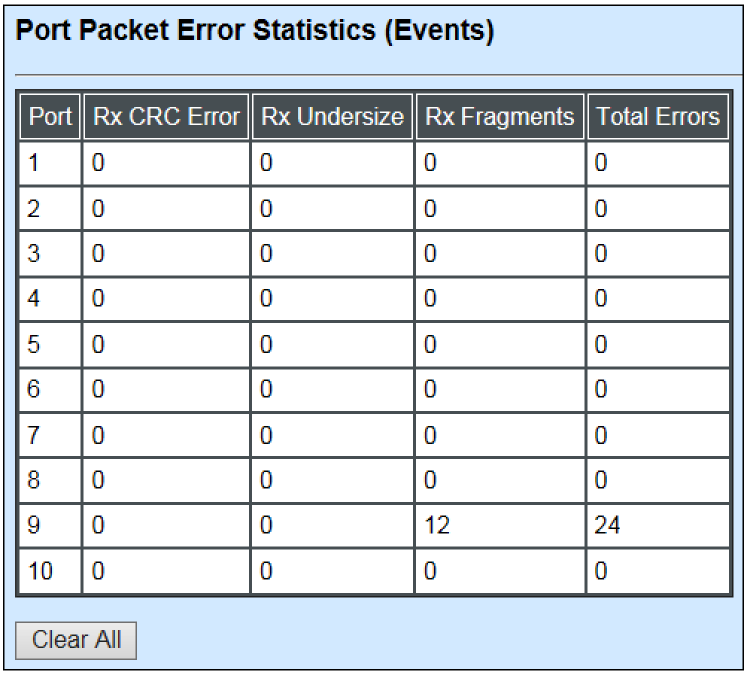
Frames Sent: The total frames sent from each port.

Total Bytes: The total bytes received and sent from each port.

Clear All: Click "**Clear All**" button to clear all ports' statistics.

3.5.3.2 Port Packet Error Statistics (Events)

The following screen page appears if you choose **Port Counters Events** and then select **Port Packet Error Statistics (Events)**.



Port Packet Error Statistics (Events)

Port	Rx CRC Error	Rx Undersize	Rx Fragments	Total Errors
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	12	24
10	0	0	0	0

RX CRC Error: The number of packets with wrong FCS received.

RX Undersize: Undersize frames received.

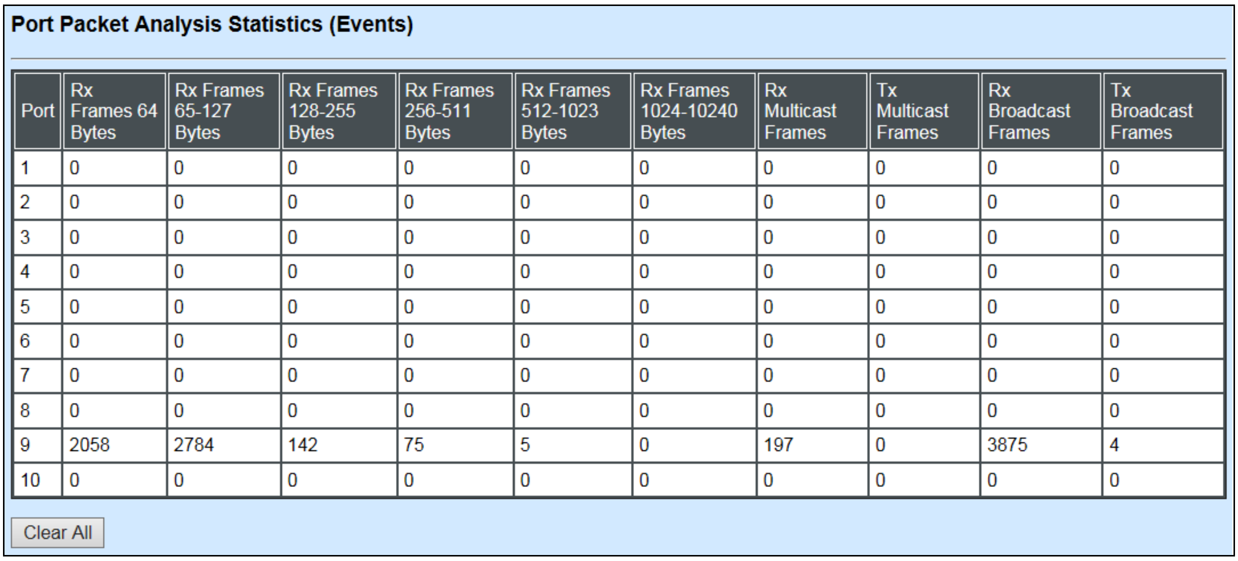
RX Fragments: Fragment frames received.

Total Errors: The number of total errors.

Clear All: Click "**Clear All**" button to clear all ports' statistics.

3.5.3.3 Port Packet Analysis Statistics (Events)

The following screen page appears if you choose **Port Counters Events** and then select **Port Packet Analysis Statistics (Events)**.



Port Packet Analysis Statistics (Events)

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 1024-10240 Bytes	Rx Multicast Frames	Tx Multicast Frames	Rx Broadcast Frames	Tx Broadcast Frames
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	2058	2784	142	75	5	0	197	0	3875	4
10	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.

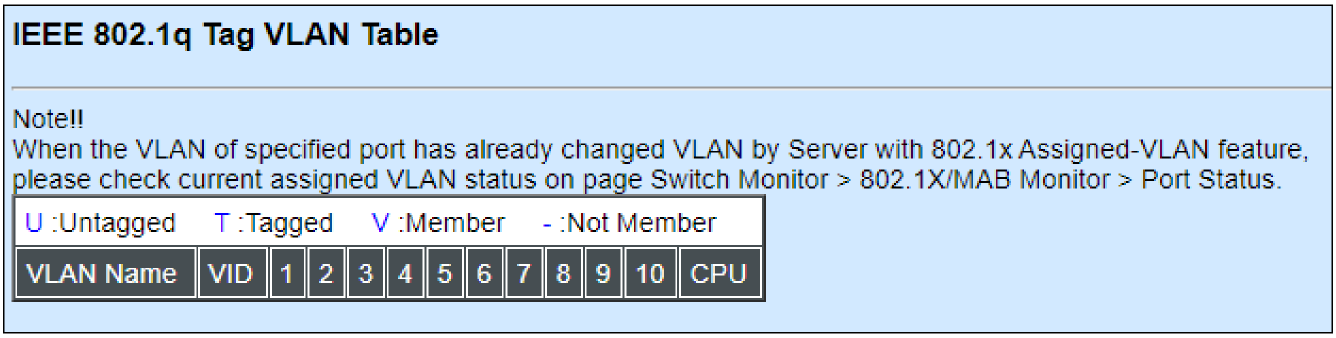
RX Broadcast Frames: Good broadcast frames received.

TX Broadcast Frames: Good broadcast packets sent.

Clear All: Click "**Clear All**" button to clear all ports' statistics.

3.5.4 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 VLAN of specified 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.

U :Untagged T :Tagged V :Member - :Not Member

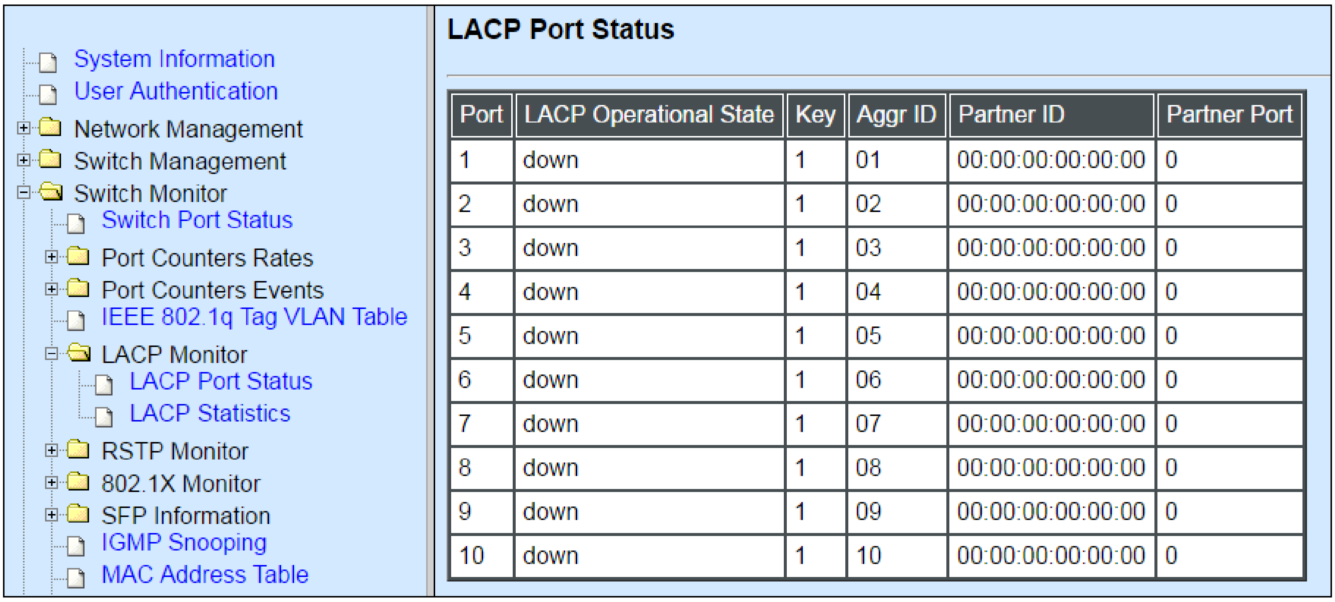
VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	CPU

VLAN Name: View-only filed that shows the VLAN group name.

VID: View-only filed that shows the VID.

3.5.5 LACP Monitor

Click the **LACP Monitor** folder and then the two options will appears.

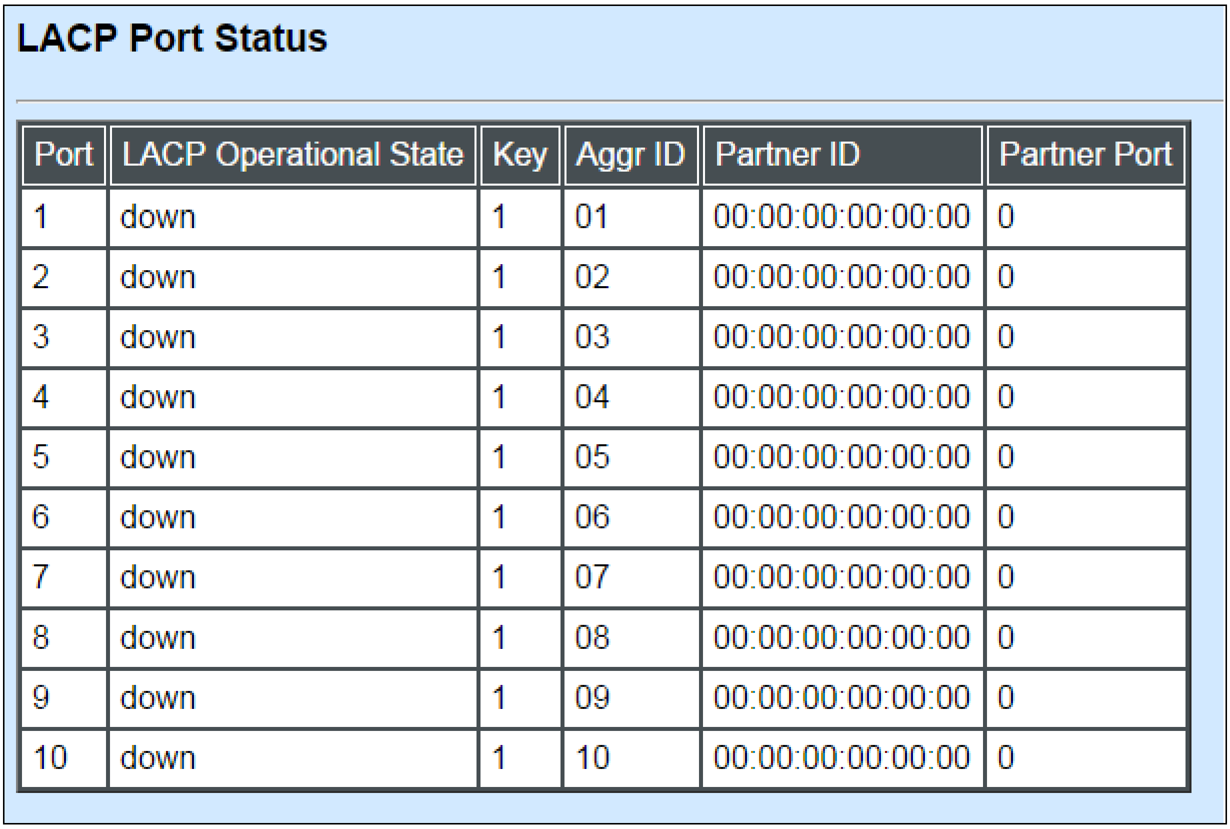


LACP Port Status

Port	LACP Operational State	Key	Aggr ID	Partner ID	Partner Port
1	down	1	01	00:00:00:00:00:00	0
2	down	1	02	00:00:00:00:00:00	0
3	down	1	03	00:00:00:00:00:00	0
4	down	1	04	00:00:00:00:00:00	0
5	down	1	05	00:00:00:00:00:00	0
6	down	1	06	00:00:00:00:00:00	0
7	down	1	07	00:00:00:00:00:00	0
8	down	1	08	00:00:00:00:00:00	0
9	down	1	09	00:00:00:00:00:00	0
10	down	1	10	00:00:00:00:00:00	0

3.5.5.1 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	down	1	01	00:00:00:00:00:00	0
2	down	1	02	00:00:00:00:00:00	0
3	down	1	03	00:00:00:00:00:00	0
4	down	1	04	00:00:00:00:00:00	0
5	down	1	05	00:00:00:00:00:00	0
6	down	1	06	00:00:00:00:00:00	0
7	down	1	07	00:00:00:00:00:00	0
8	down	1	08	00:00:00:00:00:00	0
9	down	1	09	00:00:00:00:00:00	0
10	down	1	10	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.

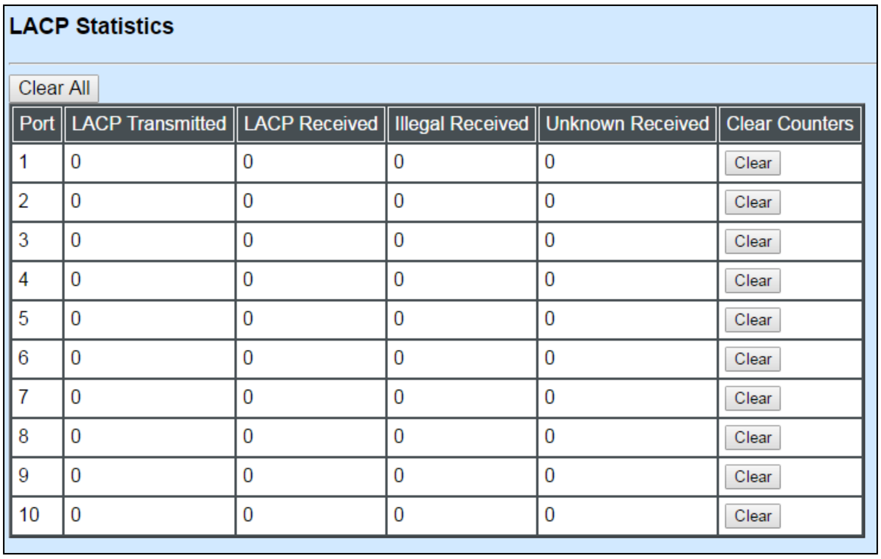
In LACP mode, link aggregation control protocol data unit (LACPDU) is used for exchanging information among LACP-enabled devices. After LACP is enabled on a port, the port sends LACPDUs to notify the remote system of its system LACP priority, system MAC address, port LACP priority, port number and operational 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.

3.5.5.2 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

Port: LACP packets (LACPDU) transmitted or received from current port.

LACP Transmitted: Packets transmitted from current port.

LACP Received: Packets received form current port.

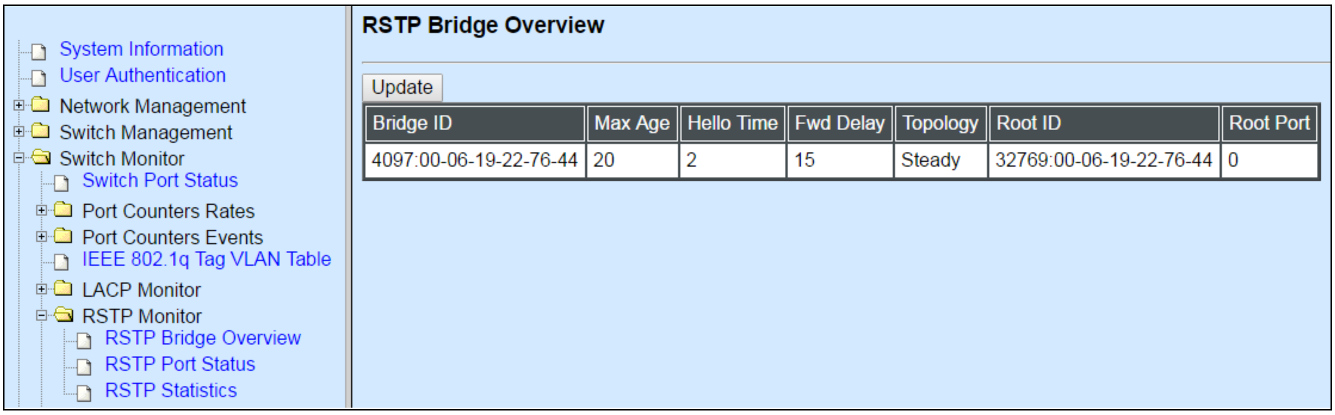
Illegal Received: Illegal packets received from current port.

Unknown Received: Unknown packets received from current port.

Clear Counter: Clear the statistics of the current port.

3.5.6 RSTP Monitor

Click the **RSTP Monitor** folder and then three options appear.

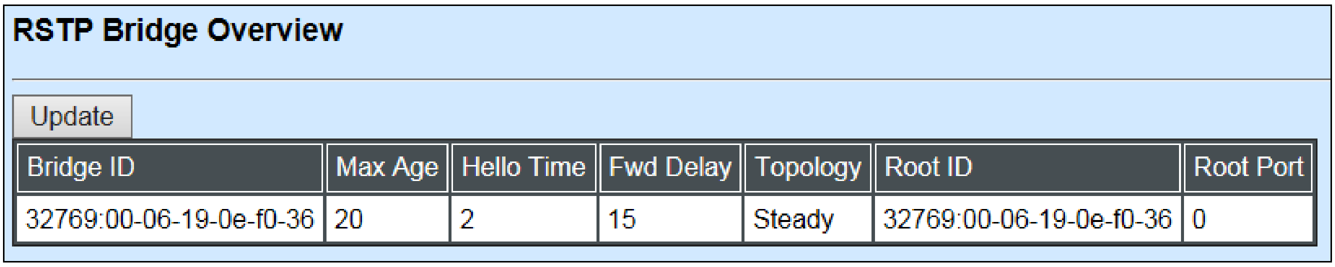


RSTP Bridge Overview

Bridge ID	Max Age	Hello Time	Fwd Delay	Topology	Root ID	Root Port
4097:00-06-19-22-76-44	20	2	15	Steady	32769:00-06-19-22-76-44	0

3.5.6.1 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
32769:00-06-19-0e-f0-36	20	2	15	Steady	32769:00-06-19-0e-f0-36	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.

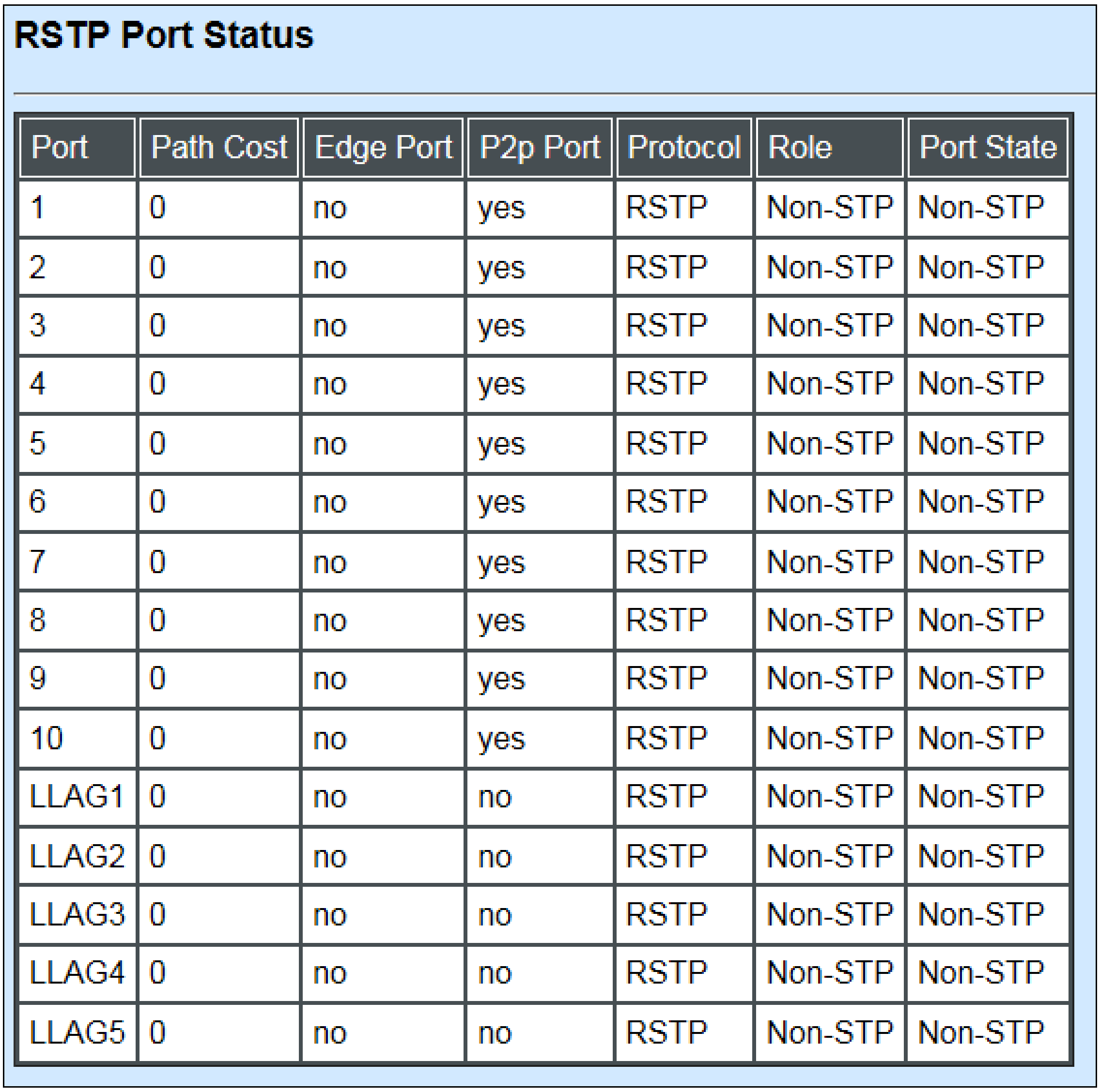
Topology: The state of the topology.

Root ID: Display this Managed Switch's Root ID.

Root port: Display this Managed Switch's Root Port Number.

3.5.6.2 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	no	yes	RSTP	Non-STP	Non-STP
2	0	no	yes	RSTP	Non-STP	Non-STP
3	0	no	yes	RSTP	Non-STP	Non-STP
4	0	no	yes	RSTP	Non-STP	Non-STP
5	0	no	yes	RSTP	Non-STP	Non-STP
6	0	no	yes	RSTP	Non-STP	Non-STP
7	0	no	yes	RSTP	Non-STP	Non-STP
8	0	no	yes	RSTP	Non-STP	Non-STP
9	0	no	yes	RSTP	Non-STP	Non-STP
10	0	no	yes	RSTP	Non-STP	Non-STP
LLAG1	0	no	no	RSTP	Non-STP	Non-STP
LLAG2	0	no	no	RSTP	Non-STP	Non-STP
LLAG3	0	no	no	RSTP	Non-STP	Non-STP
LLAG4	0	no	no	RSTP	Non-STP	Non-STP
LLAG5	0	no	no	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.

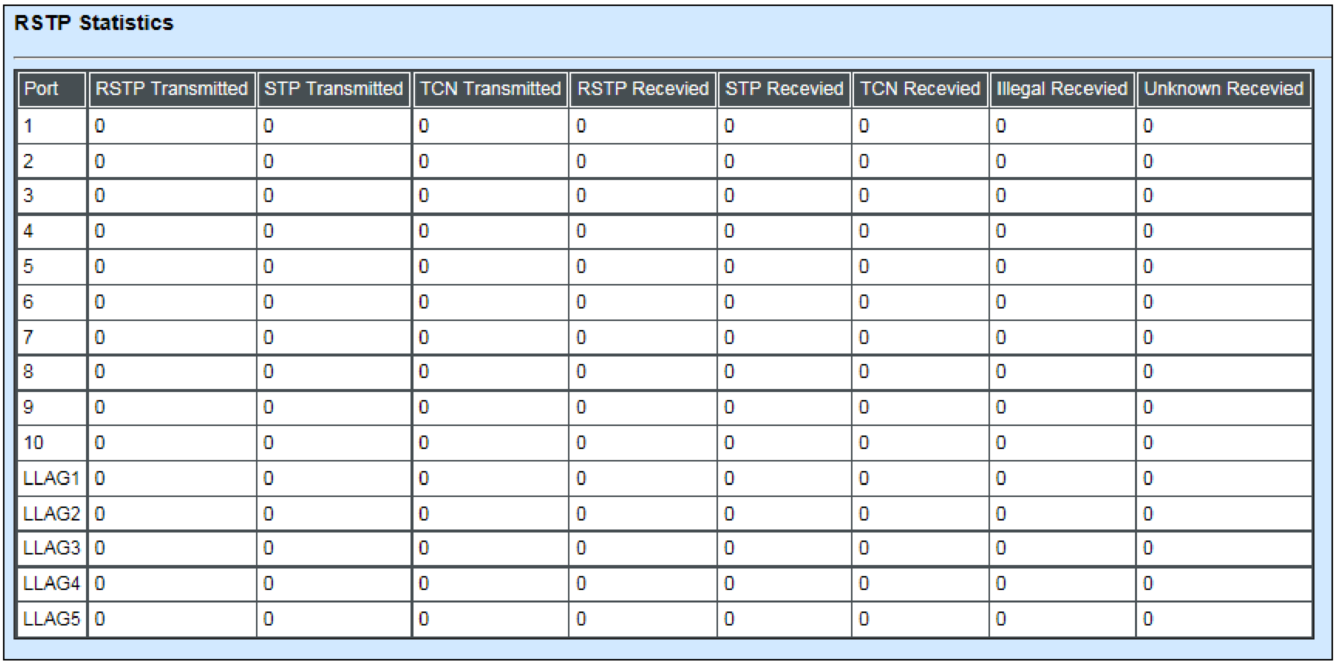
Protocol: Display RSTP or STP.

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).

3.5.6.3 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
LLAG1	0	0	0	0	0	0	0	0
LLAG2	0	0	0	0	0	0	0	0
LLAG3	0	0	0	0	0	0	0	0
LLAG4	0	0	0	0	0	0	0	0
LLAG5	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.

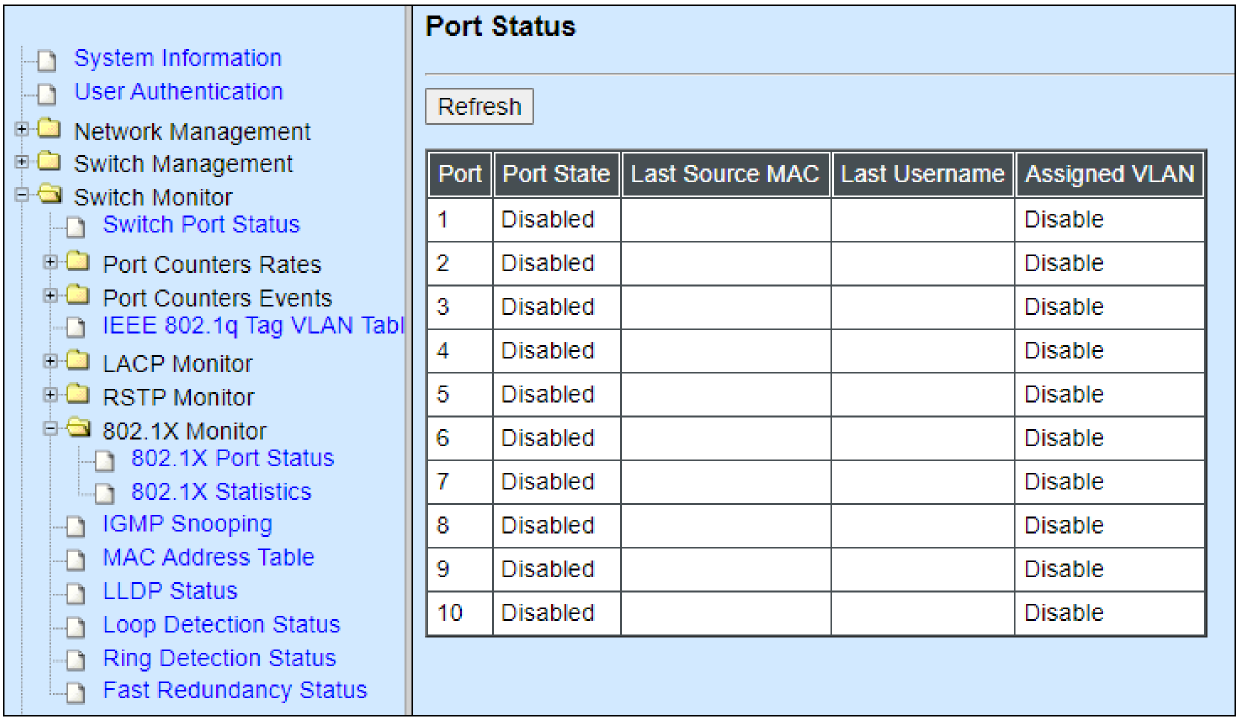
TCN Received: The total received TCN packets from current port.

Illegal Received: The total received illegal packets from current port.

Unknown Received: The total received unknown packets from current port.

3.5.7 802.1X Monitor

Click the **802.1X Monitor** folder and then two options appear.

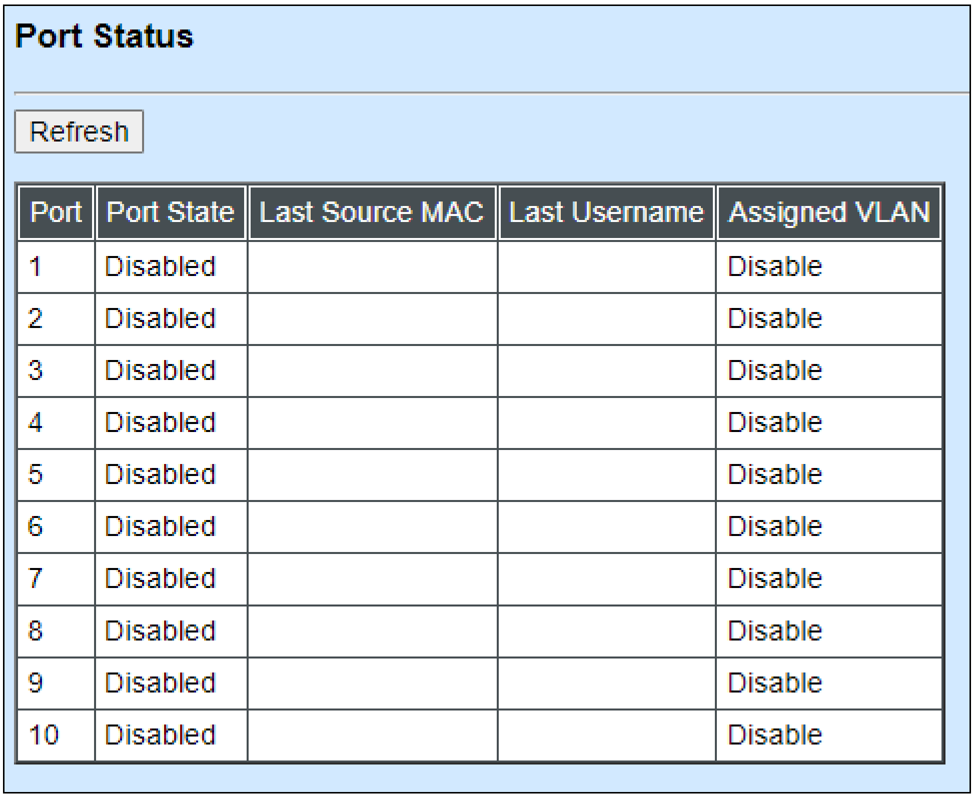


Port Status

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

3.5.7.1 802.1X Port Status

802.1X Port Status allows users to view a list of all 802.1x ports' information. Select **802.1X port status** from the **802.1x 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

In this page, you can find the following information about 802.1X ports:

Port: The number of the port.

Port State: Display the link state “Disabled”, “LinkDown”, “Authorized” or “Unauthorized” of each 802.1x port.

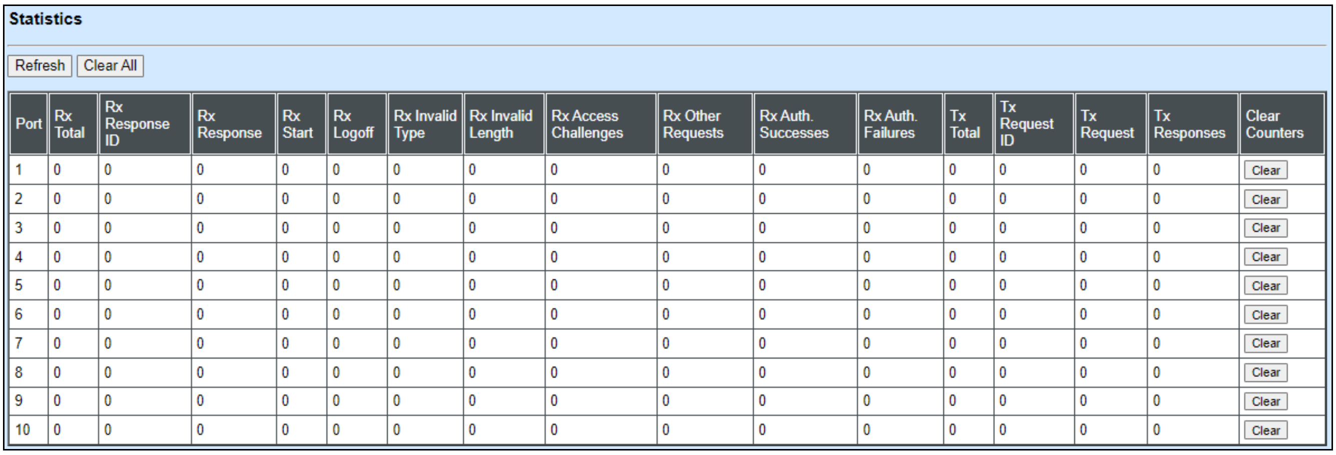
Last Source MAC: Display the MAC address of the port’s last source.

Last Username: Display the username of the port’s last login.

Assigned VLAN: Display the VLAN assigned by 802.1x Server.

3.5.7.2 802.1X Statistics

In order to view the real-time 802.1X port statistics status of the Managed Switch, select **802.1x 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	Clear Counters
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear

Refresh: Click **Refresh** to update the 802.1X port status.

Rx Total: Display the total number of the received EAPOL messages on the port.

Rx Response ID: Display the number of the received EAP-Response/Identity messages on the port.

Rx Response: Display the number of the received EAP-Response messages that were not EAP-Response/Identity.

Rx Start: Display the number of EAPOL-Start messages received on the port.

Rx Logoff: Display the number of EAPOL-Logoff messages received on the port.

Rx Invalid Type: Display the number of received EAPOL messages of the invalid type on the port.

Rx Invalid Length: Display the number of EAPOL messages with incorrect packet body length received on the port.

Rx Access Challenges: Display the number of the received RADIUS Access-Challenge messages on the port.

Rx Auth. Successes: Display the number of the received RADIUS Access-Accept messages on the port.

Rx Auth. Failures: Display the number of the received RADIUS Access-Reject messages on the port.

Tx Total: Display the number of the EAPOL messages transmitted on the port.

Tx Request ID: Display the number of the EAP-Request/Identity messages transmitted on the port.

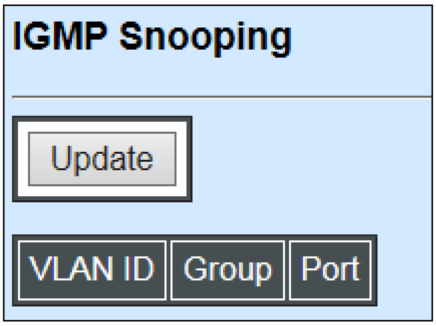
Tx Request: Display the number of the transmitted EAP-Request messages that were not EAP-Request/Identity on the port.

Tx Responses: Display the port's number of the transmitted RADIUS Access-Request messages that encapsulate either EAP-Response packets (that were not EAP-Response/Identity) or EAP-Response/Identity packets.

Clear button in **Clear Counters** field: Clear the statistics of every recorded 802.1X authentication packet transmitted or received on the specified port.

3.5.8 IGMP Snooping

The following screen page appears if you choose **Switch Monitor** and then select **IGMP Snooping**.


IGMP Snooping

VLAN ID	Group	Port

Click **Update** to update the IGMP Table.

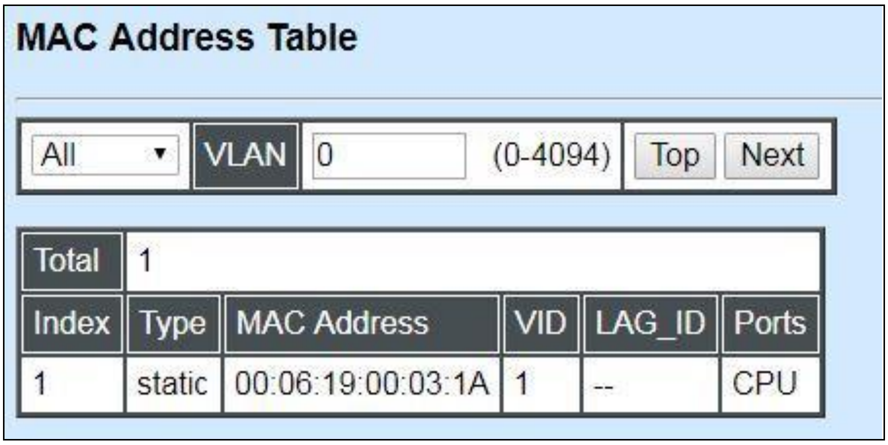
VLAN ID: The VLAN ID associated with the multicast group.

Group: The IP address for the multicast group.

Port: The port(s) grouped in the specific multicast group.

3.5.9 MAC Address Table

MAC Address Table displays MAC addresses learned after the system reset.


MAC Address Table

Total	1				
Index	Type	MAC Address	VID	LAG_ID	Ports
1	static	00:06:19:00:03:1A	1	--	CPU

The table above shows the MAC addresses learned from each port of the Managed Industrial

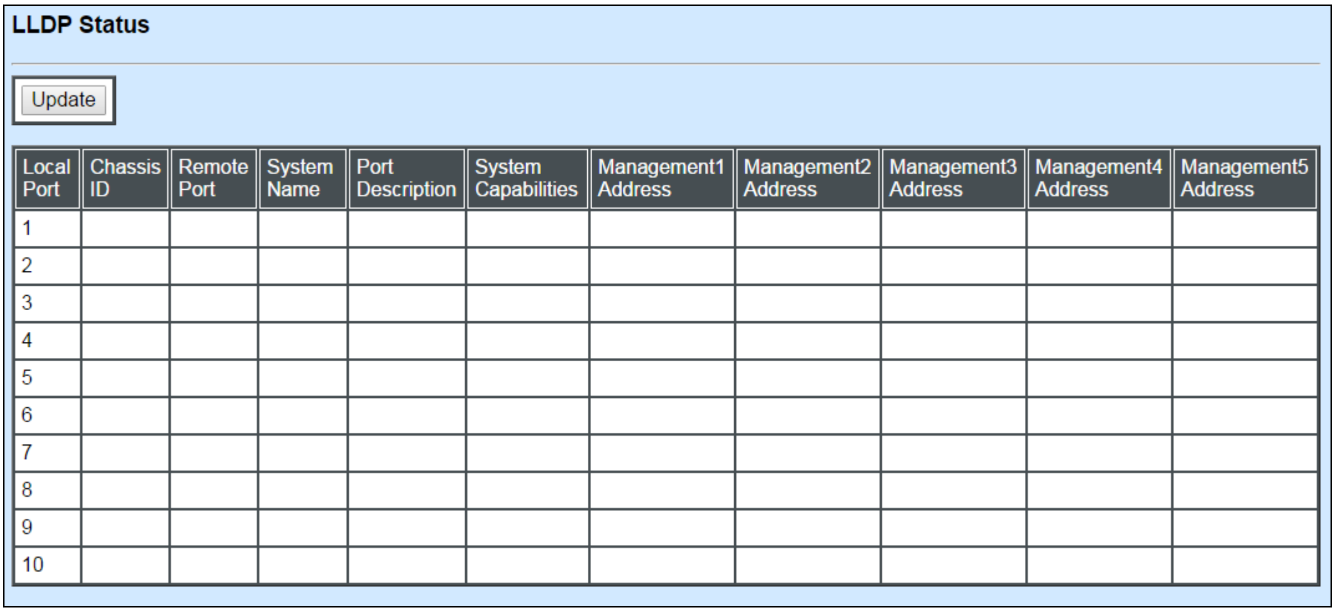
Switch.

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.

3.5.10 LLDP Status

Select **LLDP Status** from the **Switch Monitor** menu and then the following screen page appears.



LLDP Status

Local Port	Chassis ID	Remote Port	System Name	Port Description	System Capabilities	Management1 Address	Management2 Address	Management3 Address	Management4 Address	Management5 Address
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Click **“Update”** to refresh LLDP Status table.

Local Port: View-only field that shows the port number on which LLDP frames are received.

Chassis ID: View-only field that shows the MAC address of the LLDP frames received (the MAC address of the neighboring device).

Remote Port: View-only field that shows the port number of the neighboring device.

System Name: View-only field that shows the system name advertised by the neighboring device.

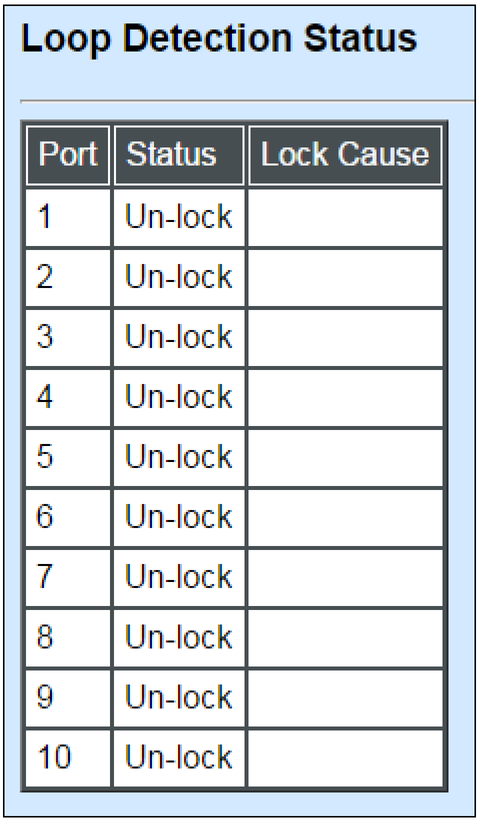
Port Description: View-only field that shows the port description of the remote port.

System Capabilities: View-only field that shows the capability of the neighboring device.

Management Address (1~5): View-only field that shows the IP address (1~5) of the neighboring device.

3.5.11 Loop Detection Status

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



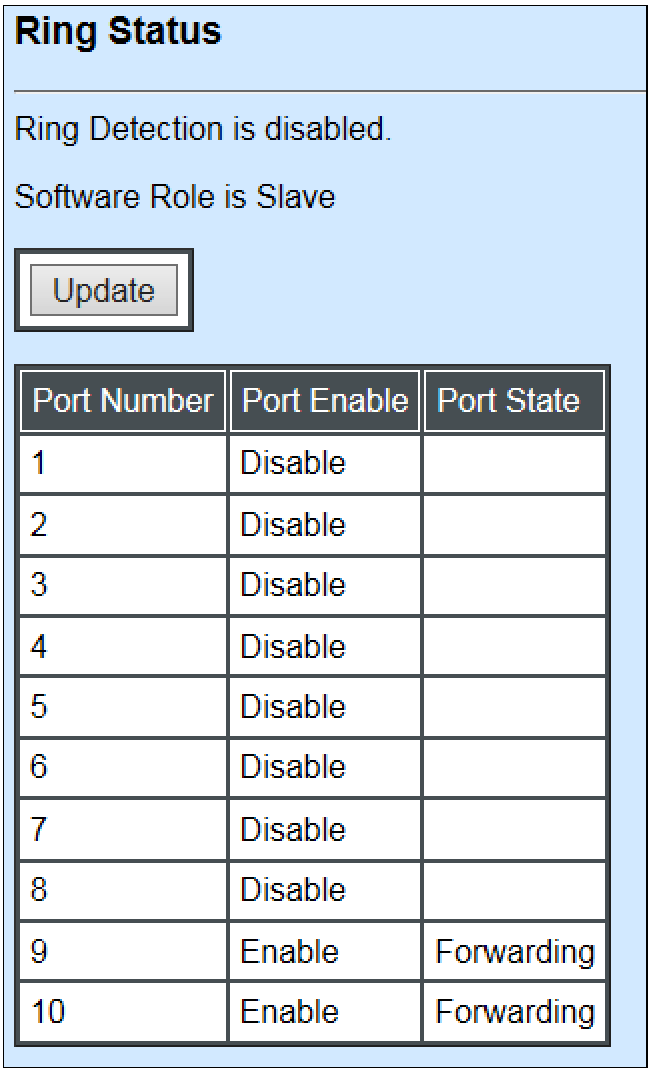
Loop Detection Status

Port	Status	Lock Cause
1	Un-lock	
2	Un-lock	
3	Un-lock	
4	Un-lock	
5	Un-lock	
6	Un-lock	
7	Un-lock	
8	Un-lock	
9	Un-lock	
10	Un-lock	

Status: This shows the status of the port, **Lock** or **Un-lock**.

Lock Cause: This shows the factor that causes the port to be locked.

3.5.12 Ring Detection Status



Ring 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	Enable	Forwarding
10	Enable	Forwarding

Port Enable: The status of whether Ring Detection on ports is enabled or disabled.

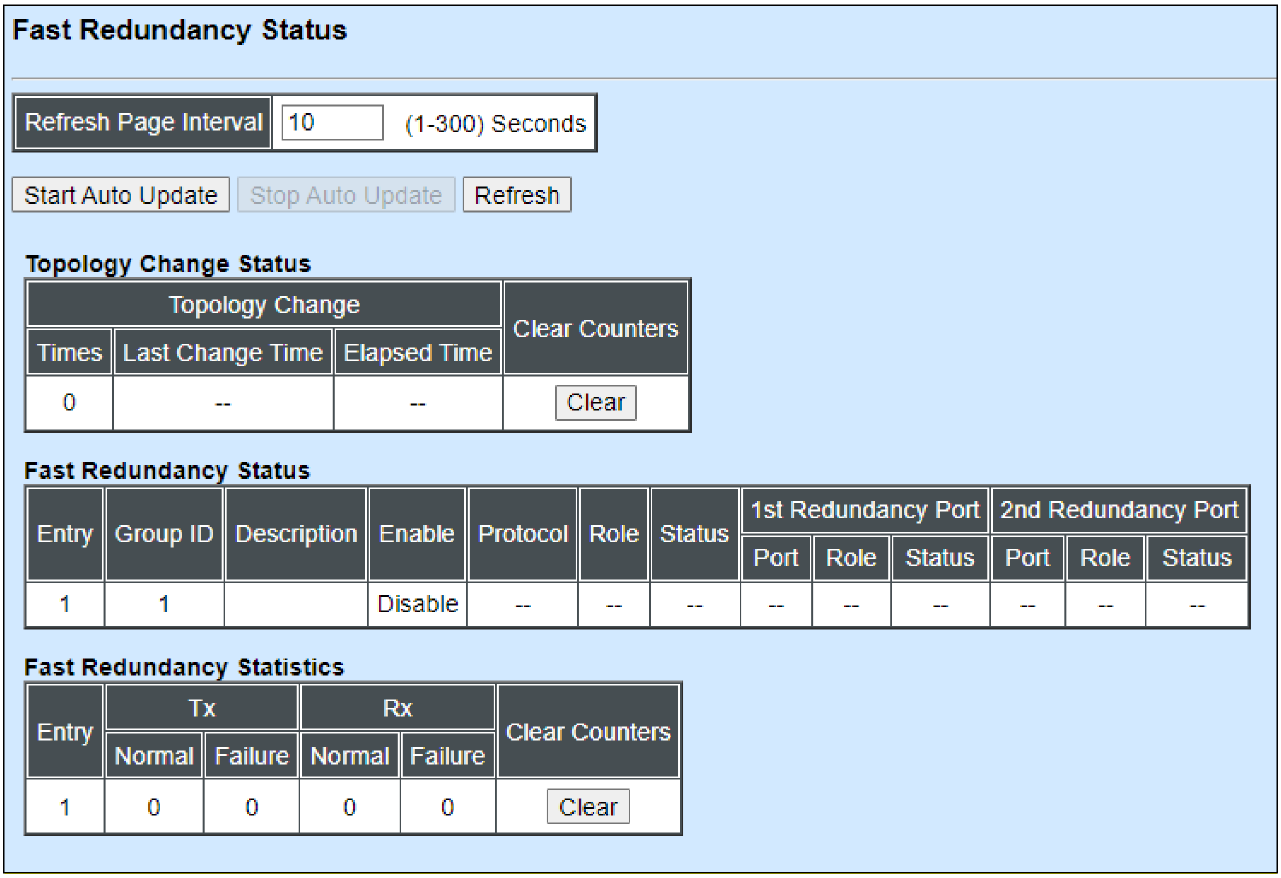
Port State: The status of whether the port is blocking or forwarding.

Blocking: It indicates a port is temporarily blocked and stop sending packet until link down occurs.

Forwarding: It indicates a port keeps sending packets.

3.5.13 Fast Redundancy Status

Fast Redundancy Status is to manually or automatically update the fast redundancy status, the information of topology transformation and the redundant ports' transmitting/receiving statistics for the configured Fast Ring v2 and/or Chain. Select **Fast Redundancy Status** from the **Switch Monitor** menu and then the following screen page appears.



Fast Redundancy Status

Refresh Page Interval	10	(1-300) Seconds

Topology Change Status

Topology Change			Clear Counters
Times	Last Change Time	Elapsed Time	
0	--	--	Clear

Fast Redundancy Status

Entry	Group ID	Description	Enable	Protocol	Role	Status	1st Redundancy Port			2nd Redundancy Port		
							Port	Role	Status	Port	Role	Status
1	1		Disable	--	--	--	--	--	--	--	--	--

Fast Redundancy Statistics

Entry	Tx		Rx		Clear Counters
	Normal	Failure	Normal	Failure	
1	0	0	0	0	Clear

Refresh Page Interval: Automatically updates the related fast redundancy statistics and status at a specified interval in seconds. Please note that the value you assign in this parameter is temporarily used and will not be saved into the configuration file of the Managed Switch. This value will not be applied into the next system boot-up.

Start Auto Update: Click "**Start Auto Update**" to activate auto-update.

Stop Auto Update: Click "**Stop Auto Update**" to deactivate auto-update.

Refresh: Click "**Refresh**" to update the latest statistics and status of fast redundancy at a time.

Times of Topology Change: View-only field that shows the total times of topology transformation for the configured Fast Ring v2 and Chain.

Last Change Time of Topology Change: View-only field that shows the time when the last transformation of topology takes place.

Elapsed Time of Topology Change: The period of time passed by since the last transformation of topology has been taken place.

Clear button in **Clear Counters** field for Topology Change Status**:** The counter value of **Times** will set back to zero and the information related to the last transformation of topology will also be cleared.

Entry: View-only field. This shows the number of each fast redundancy you configured.

Group ID: View-only field. This shows the group ID of each fast redundancy you configured.

Description: View-only field that shows the description of each group you configured.

Enable: View-only field that shows the enabled or disabled status of each fast redundancy you configured.

Protocol: View-only field that shows the redundancy protocol you use for each fast redundancy you configured.

Role: View-only field that shows the role that the Managed Switch plays in each fast redundancy you configured when the "Fast Ring v2" protocol is chosen. It will show "--" when the "Chain" protocol is chosen.

Status: View-only field that shows the connection status of each fast redundancy you configured. Include **Healthy**, **Break** and **Signal Fail** 3 types of state. Each state is described as below.

> **Healthy:** It indicates that the connection of the fast redundancy is in normal status.
>
> **Break:** It indicates that the failure of fast redundancy connection occurs on other switch and its backup link is activated to transmit the data.
>
> **Signal Fail:** It indicates that the failure of fast redundancy connection occurs on the switch itself and its backup link is activated to transmit the data.

1st Redundancy Port: View-only field that shows the port on the Managed Switch acts as the first redundant port.

2nd Redundancy Port: View-only field that shows the port on the Managed Switch acts as the secondary redundant port.

Role of 1st/2nd Redundancy Port: View-only field. It shows the role (Head, Member and Tail) that the port acting as the first/secondary redundant port plays when the Chain protocol is chosen. It will show "--" when the Fast Ring v2 protocol is chosen.

Status of 1st/2nd Redundancy Port: View-only field. It shows the connection status of the port that acts as the first/secondary redundant port. Include **Forwarding**, **Blocked** and **Link down** 3 types of port state. Each state is described as below.

Forwarding: It indicates that the port connection of the fast redundancy is in normal status.

Blocked: It indicates that the port is connected to a backup path and the path is blocked.

Link down: It indicates that no port connection eixsts.

Tx Normal: Total packets transmitted from the specific entry when its configured Fast Ring v2/Chain is at the normal status.

Rx Normal: Total packets received by the specific entry when its configured Fast Ring v2/Chain is at the normal status.

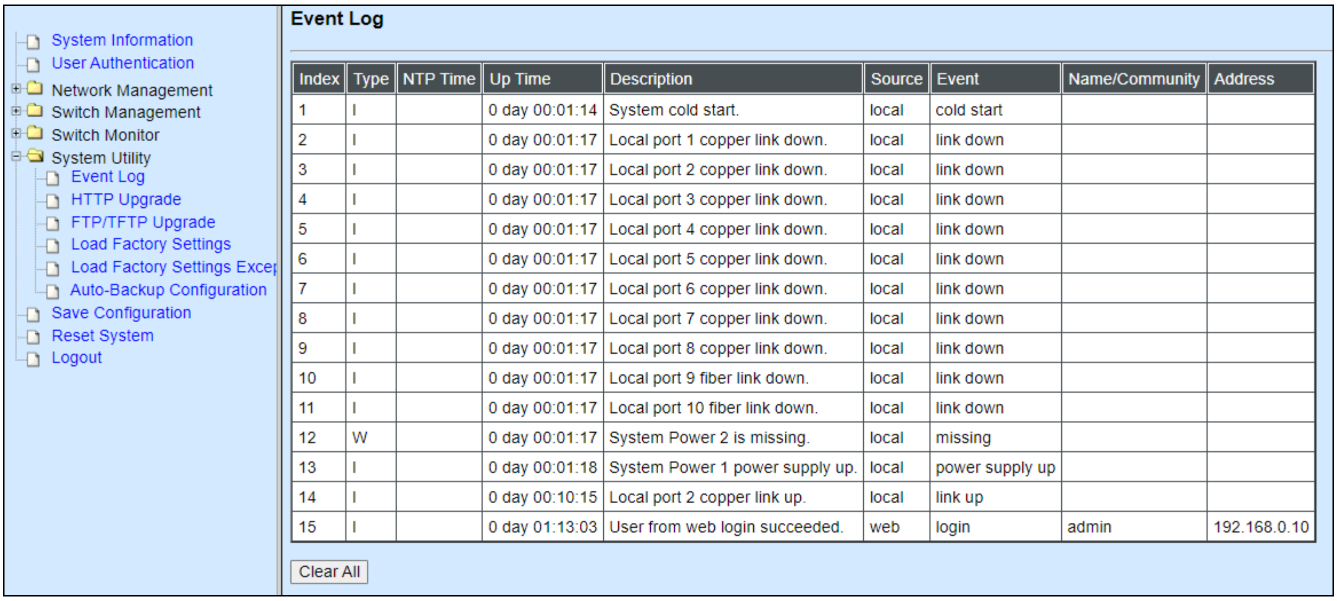
Tx Failure: Total packets transmitted from the specific entry when its configured Fast Ring v2/Chain is at the abnormal status.

Rx Failure: Total packets received by the specific entry when its configured Fast Ring v2/Chain is at the abnormal status.

Clear button in **Clear Counters** field for Fast Redundancy Statistics**:** Clear the fast redundancy Tx/Rx Normal and Tx/Rx Failure statistics of redundant ports for the corresponding entry.

3.6 System Utility

Select the folder **System Utility** from the left column and then the following screen page appears.



Event Log

Index	Type	NTP Time	Up Time	Description	Source	Event	Name/Community	Address
1	I		0 day 00:01:14	System cold start.	local	cold start		
2	I		0 day 00:01:17	Local port 1 copper link down.	local	link down		
3	I		0 day 00:01:17	Local port 2 copper link down.	local	link down		
4	I		0 day 00:01:17	Local port 3 copper link down.	local	link down		
5	I		0 day 00:01:17	Local port 4 copper link down.	local	link down		
6	I		0 day 00:01:17	Local port 5 copper link down.	local	link down		
7	I		0 day 00:01:17	Local port 6 copper link down.	local	link down		
8	I		0 day 00:01:17	Local port 7 copper link down.	local	link down		
9	I		0 day 00:01:17	Local port 8 copper link down.	local	link down		
10	I		0 day 00:01:17	Local port 9 fiber link down.	local	link down		
11	I		0 day 00:01:17	Local port 10 fiber link down.	local	link down		
12	W		0 day 00:01:17	System Power 2 is missing.	local	missing		
13	I		0 day 00:01:18	System Power 1 power supply up.	local	power supply up		
14	I		0 day 00:10:15	Local port 2 copper link up.	local	link up		
15	I		0 day 01:13:03	User from web login succeeded.	web	login	admin	192.168.0.10

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 Switch has both built-in TFTP and FTP clients. Users may save or restore the configuration and update the firmware by FTP/TFTP.

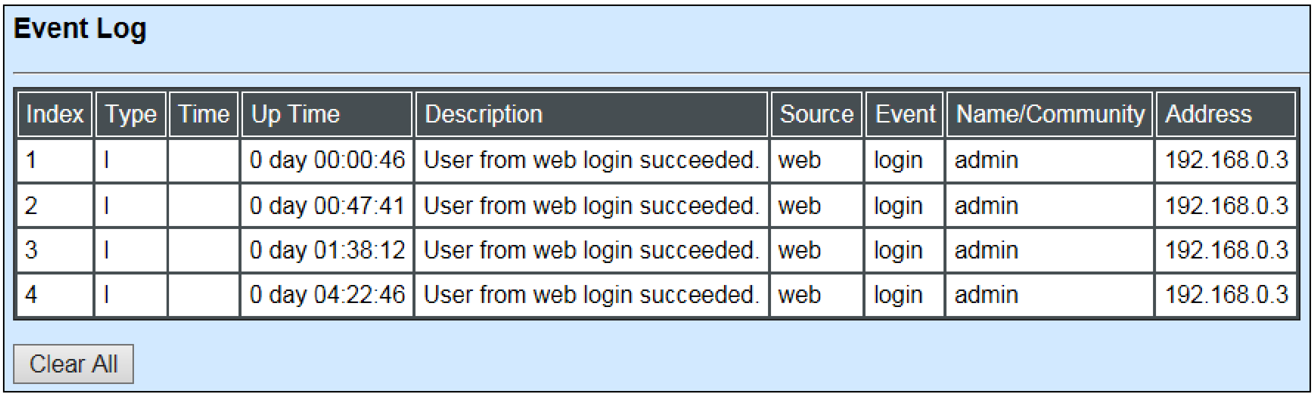
4. **Load Factory Settings:** Load Factory Setting will set the configuration of the Managed Industrial Switch back to the factory default settings. The IP and Gateway addresses will be set to the factory default as well.

5. **Load Factory Settings Except Network Configuration:** Selecting this function will also restore the configuration of the Managed Industrial Switch to its original factory default settings. However, this will not reset the IP and Gateway addresses to the factory default.

6. **Auto-Backup Configuration:** Periodically execute the automatic backup of the start-up configuration files based on the given time you set up.

3.6.1 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.



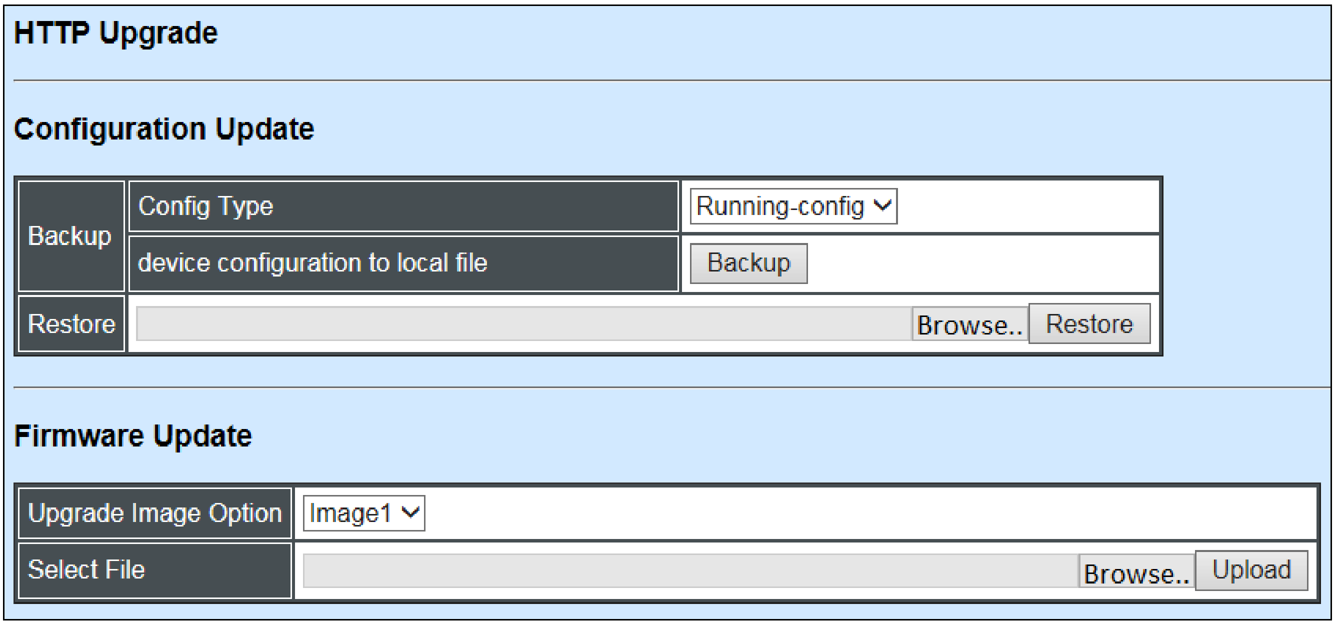
Event Log

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.

3.6.2 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**.

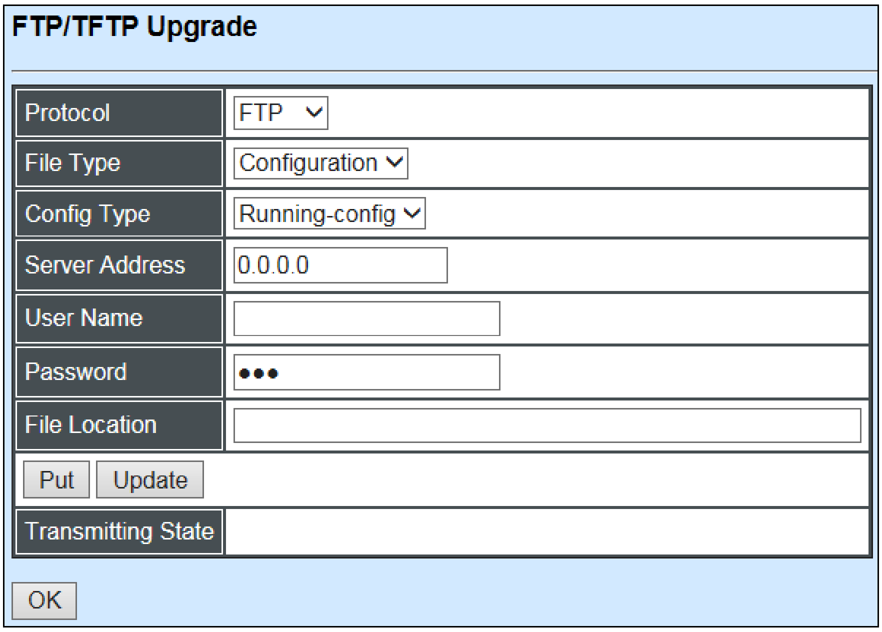
Firmware Update

Upgrade Image Option: Choose the image you want to upgrade.

Select File: Click **Browse**, select the designated file and then click **Upload**.

3.6.3 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	
Transmitting State	

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 Switch to update the firmware or configuration from the File Server. After a successful update, a message will pop up. The Managed Industrial Switch will need a reset to make changes effective.

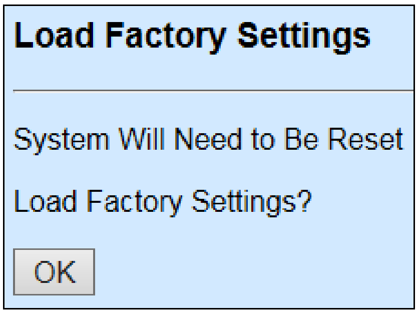
Transmitting State: This field displays the uploading or updating status.

OK: Click **OK** to update the firmware or configuration from the File Server.

3.6.4 Load Factory Settings

Load Factory Settings will set all configurations of the Managed Industrial 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

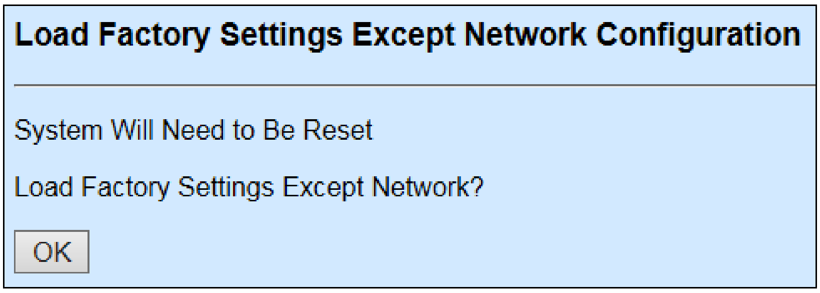
Load Factory Settings?

Click the **"OK"** button to restore the Managed Industrial Switch back to the defaults.

3.6.5 Load Factory Settings Except Network Configuration

Load Factory Settings Except Network Configuration will set all configurations of the Managed Industrial 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

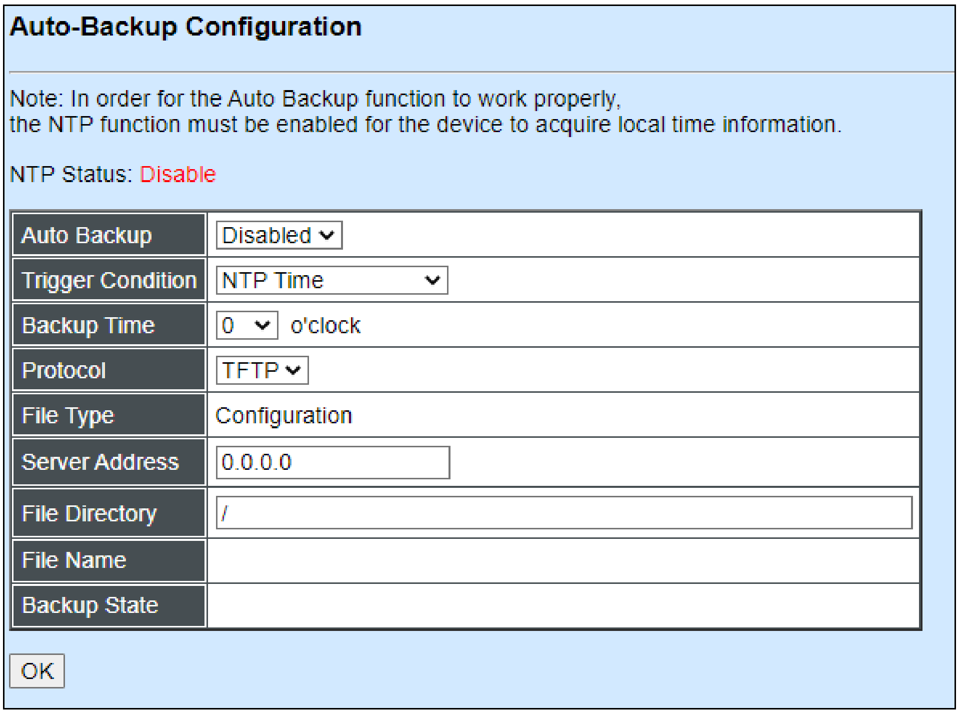
Load Factory Settings Except Network?

Click the **"OK"** button to restore the Managed Industrial Switch back to the defaults excluding network configurations.

3.6.6 Auto-Backup Configuration

The **HTTP Upgrade** and **FTP/TFTP Upgrade** functions are offered for the users to do the manual backup of the start-up configuration. Alternatively, you can choose the **Auto-backup configuration** function to do this backup automatically and periodically. It is useful to prevent the loss of user's important configuration if they forget to do the backup, or help do the file comparison if any error occurs. Please note that the device's NTP function must be enabled as well in order to obtain the correct local time.

To initiate this function, please select **Auto-Backup Configuration** from the **System Utility** menu, the following screen page shows up.



Auto-Backup Configuration

Note: In order for the Auto Backup function to work properly,
the NTP function must be enabled for the device to acquire local time information.

NTP Status: Disable

Auto Backup	Disabled
Trigger Condition	NTP Time
Backup Time	0 o'clock
Protocol	TFTP
File Type	Configuration
Server Address	0.0.0.0
File Directory	/
File Name	
Backup State	

Auto Backup: Enable/Disable the auto-backup function for the start-up configuration files of the device.

Trigger Condition: Select **NTP Time** or **Save Configuration** against which auto-backup will be triggered.

NTP Time: Auto-backup will be triggered against the system's NTP time

Save Configuration: Auto-backup will be triggered whenever you save the current configuration.

Backup Time: Set up the time when the backup of the start-up configuration files will start every day for the system.

Protocol: Either FTP or TFTP server can be selected to back up the start-up configuration files.

File Type: Display the type of files that will be backed up.

Server Address: Set up the IP address of FTP/TFTP server.

User Name and Password: Input the required username as well as password for authentication if FTP is chosen in the Protocol field.

File Directory: Assign the back-up path where the start-up configuration files will be placed on FTP or TFTP server.

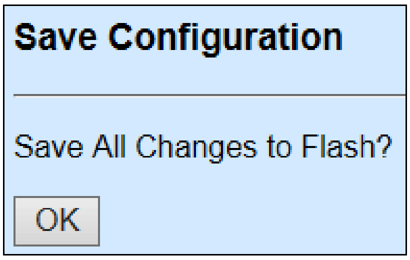
File Name: The filename assigned to the auto- backup configuration files. The format of filename generated automatically is as follows:

ip address_Device Name_Date.txt , for example, 192.168.0.3_IES-3110_20171120.txt

Backup State: Display the status of the auto-backup you execute.

3.7 Save Configuration

To keep the existing configurations permanently, users need to save the configurations first before resetting the Managed Industrial Switch. Select **Save Configuration** from the **Main Menu** and then the following screen page appears.



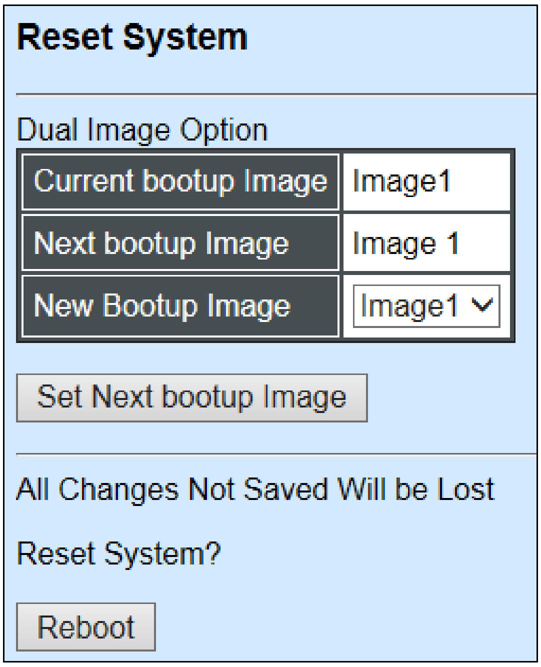
Save Configuration

Save All Changes to Flash?

Click the **"OK"** button to save changes or running configurations to Flash.

3.8 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?

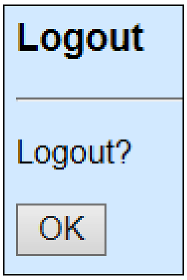
The Managed Industrial Switch supports Dual Image for boot-up, please select the next boot-up image before restarting.

Click the **"Set Next bootup Image"** button to set the designated image for booting up.

Click the **"Reboot"** button to restart the Managed Industrial Switch.

3.9 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 Switch.

APPENDIX A: DHCP Auto-Provisioning Setup

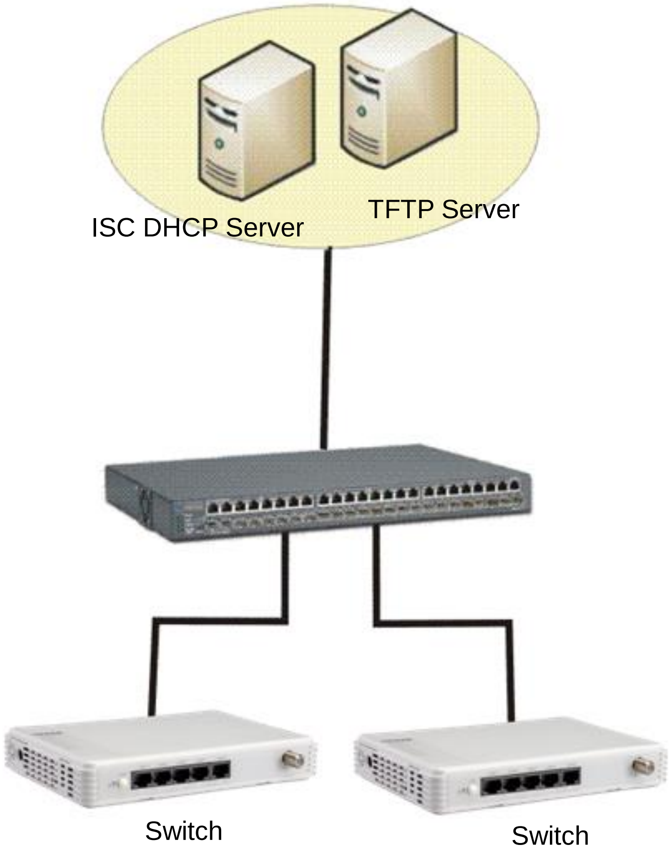
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the Managed Industrial Switch that you 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

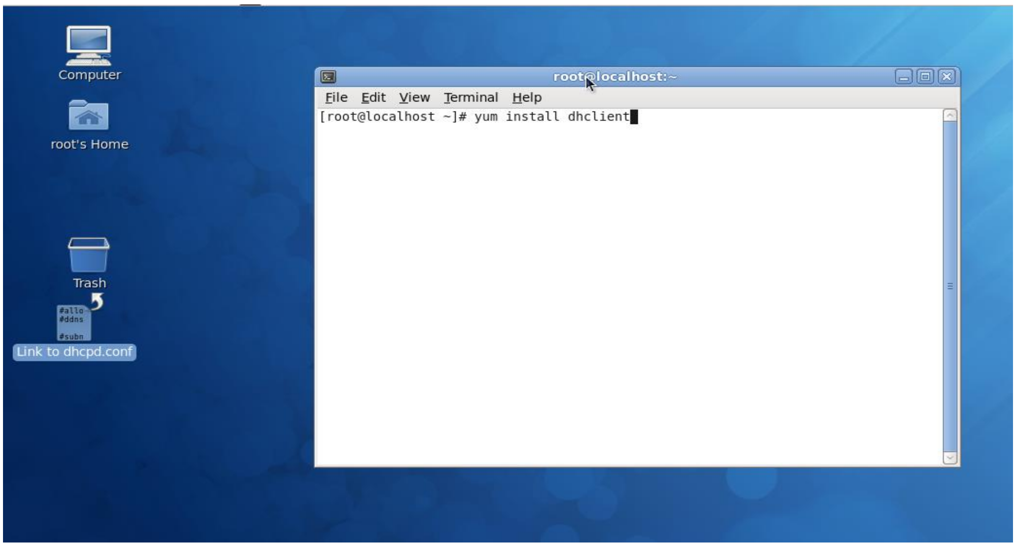
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Topology Example

Step 2. Set Up Auto Provision Server

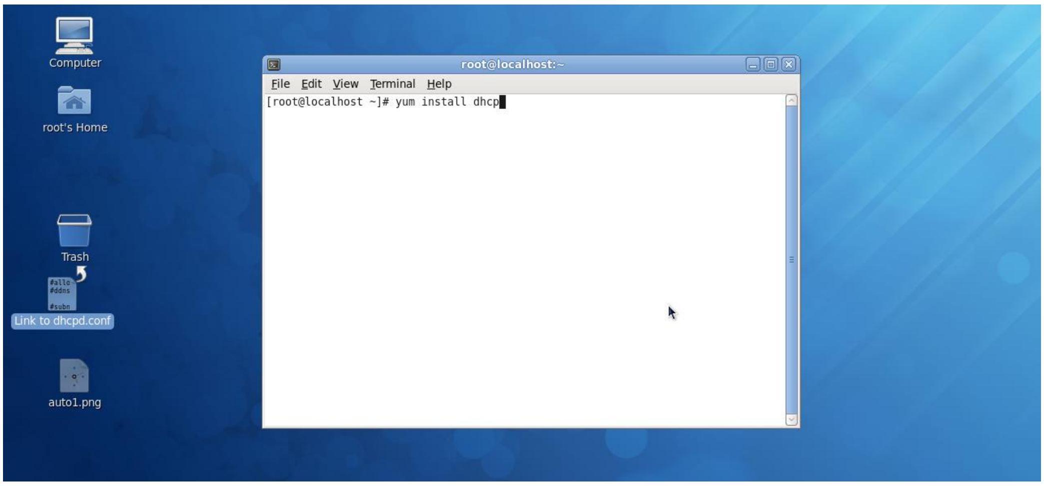
- **Update DHCP client**



```
[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.

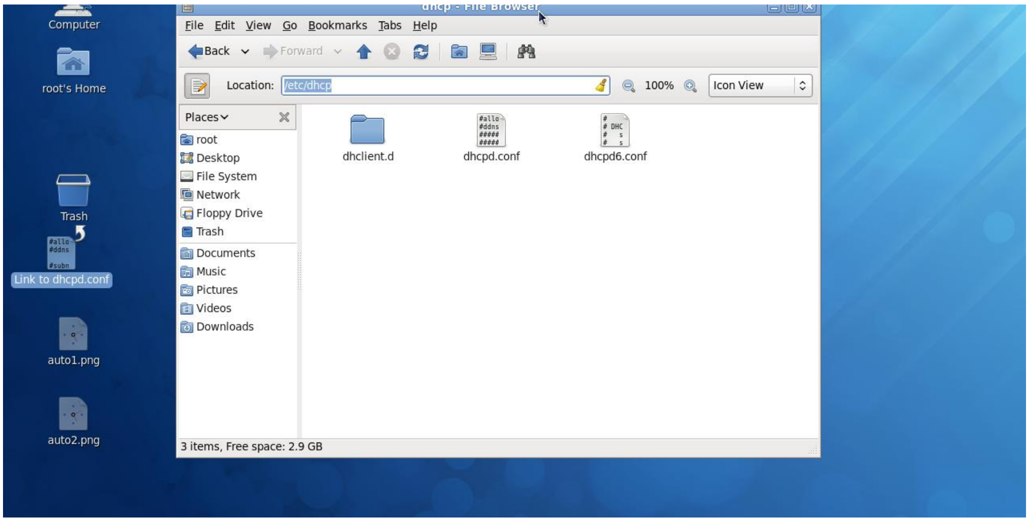
- **Install DHCP server**



```
[root@localhost ~]# yum install dhcp
```

Issue "yum install dhcp" command to install DHCP server.

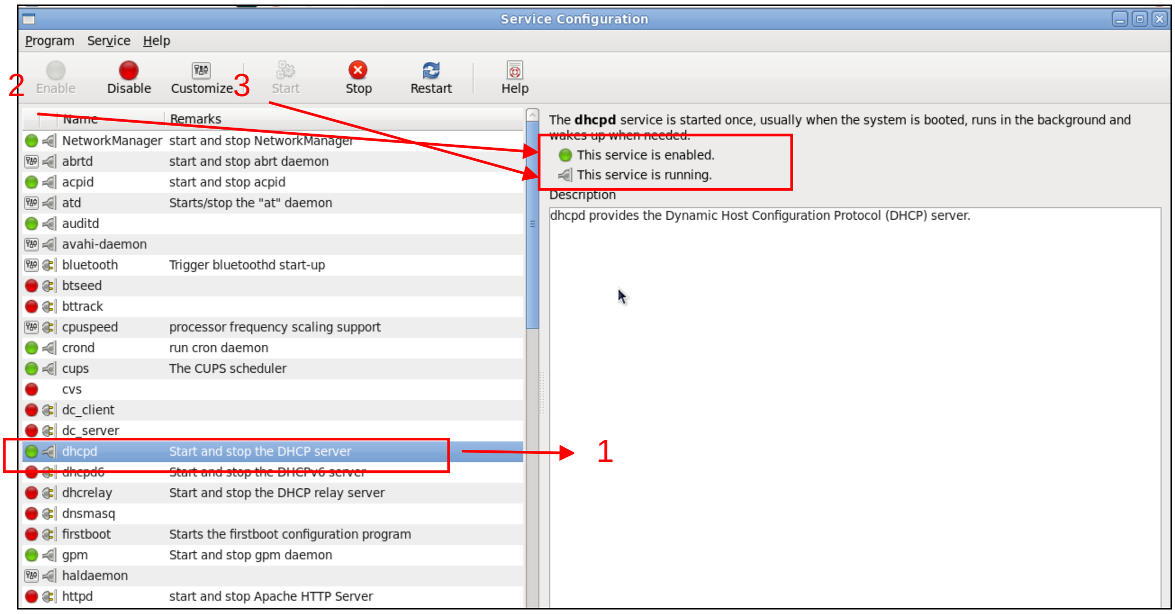
● Copy dhcpd.conf to /etc/dhcp/ directory



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

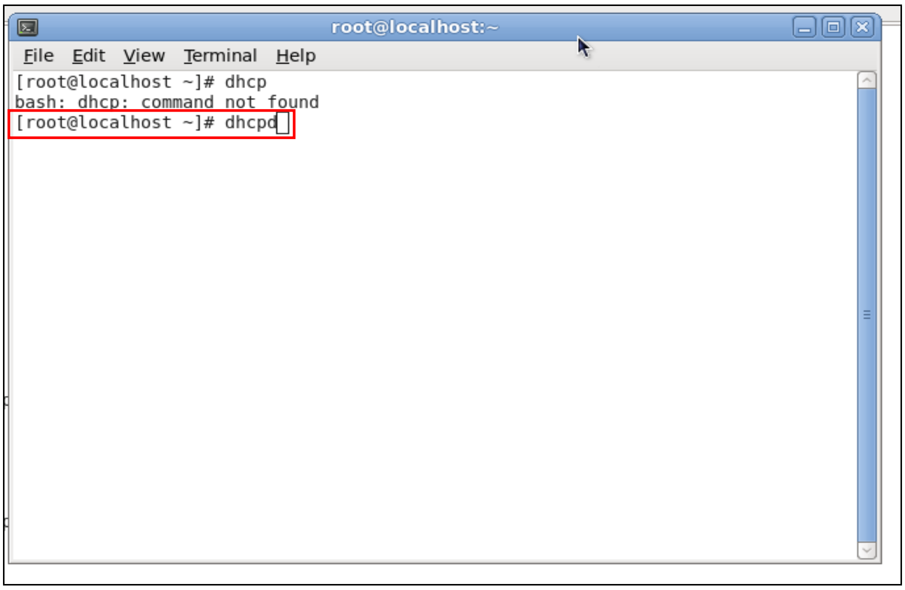
dhcpd provides the Dynamic Host Configuration Protocol (DHCP) server.

1. Choose dhcpd.

2. Enable DHCP service.

3. Start running DHCP service.

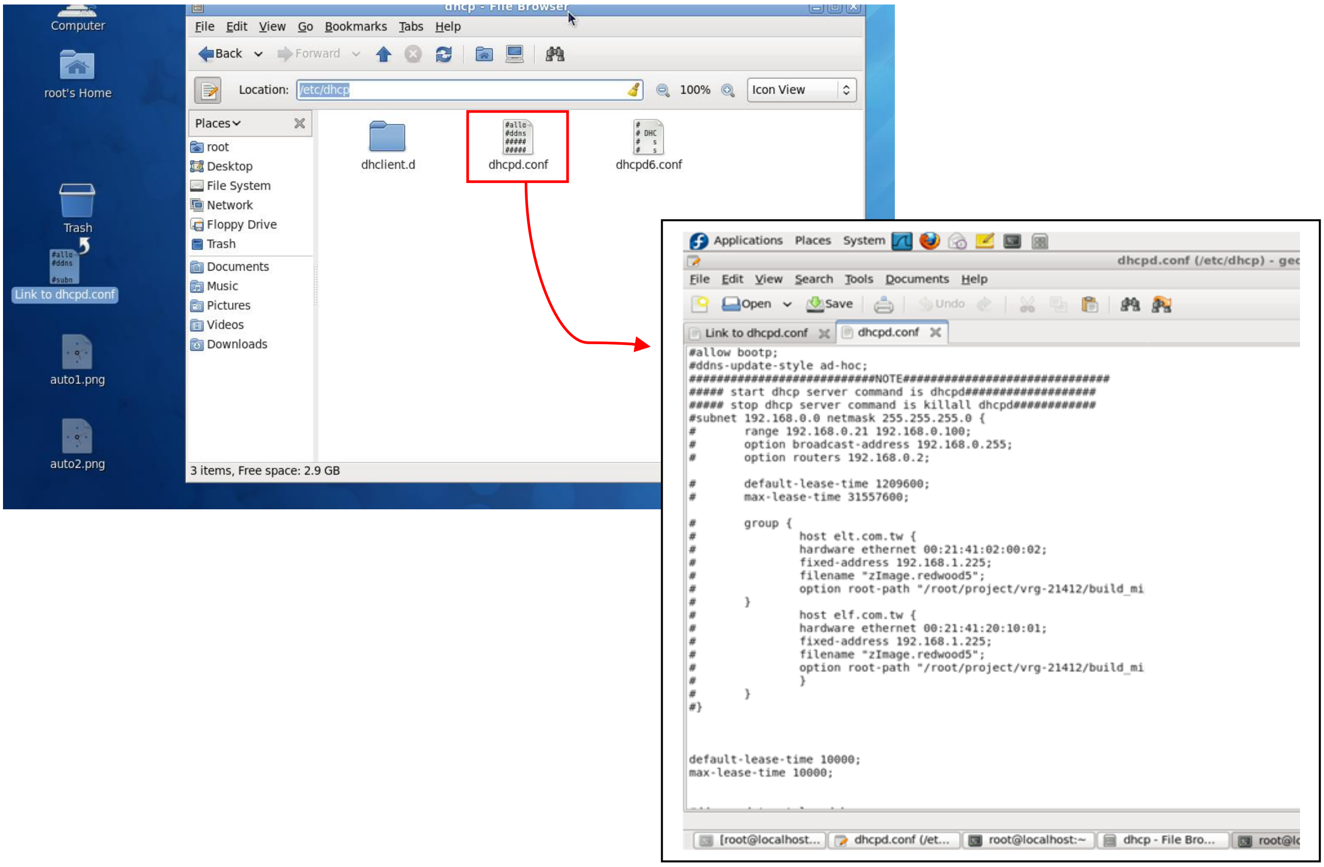
***NOTE:** DHCP service can also be enabled using CLI. Issue “dhcpd” command to enable DHCP service.*



```
[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**

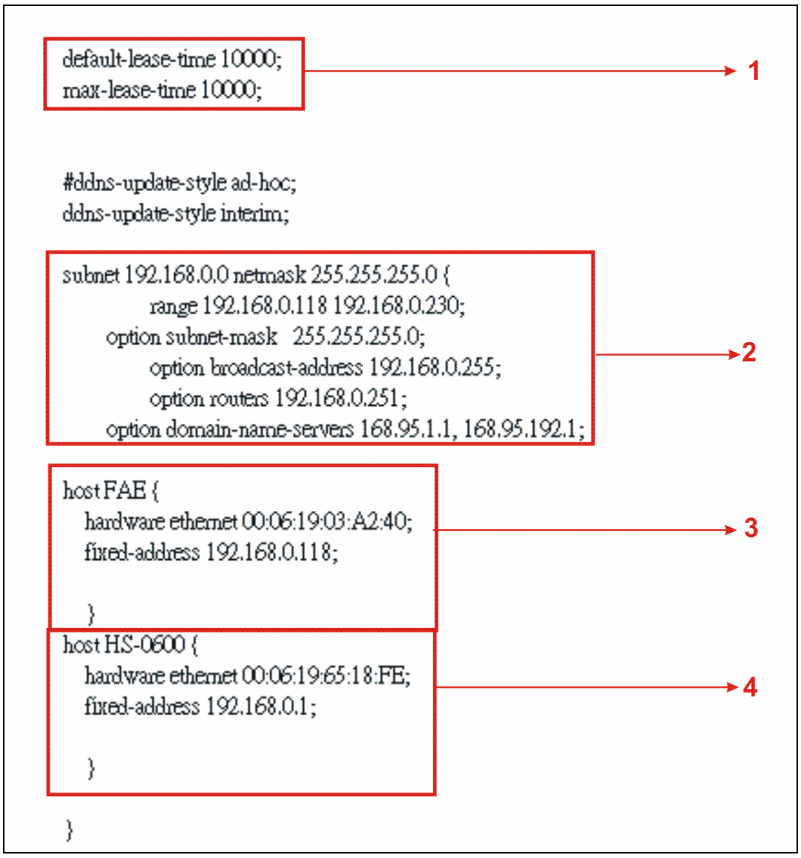


```
#allow bootp;
#ddns-update-style ad-hoc;
###########################NOTE##############################
##### start dhcp server command is dhcpd###################
##### stop dhcp server command is killall dhcpd############
#subnet 192.168.0.0 netmask 255.255.255.0 {
#       range 192.168.0.21 192.168.0.100;
#       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/ directory to open it.

● 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.

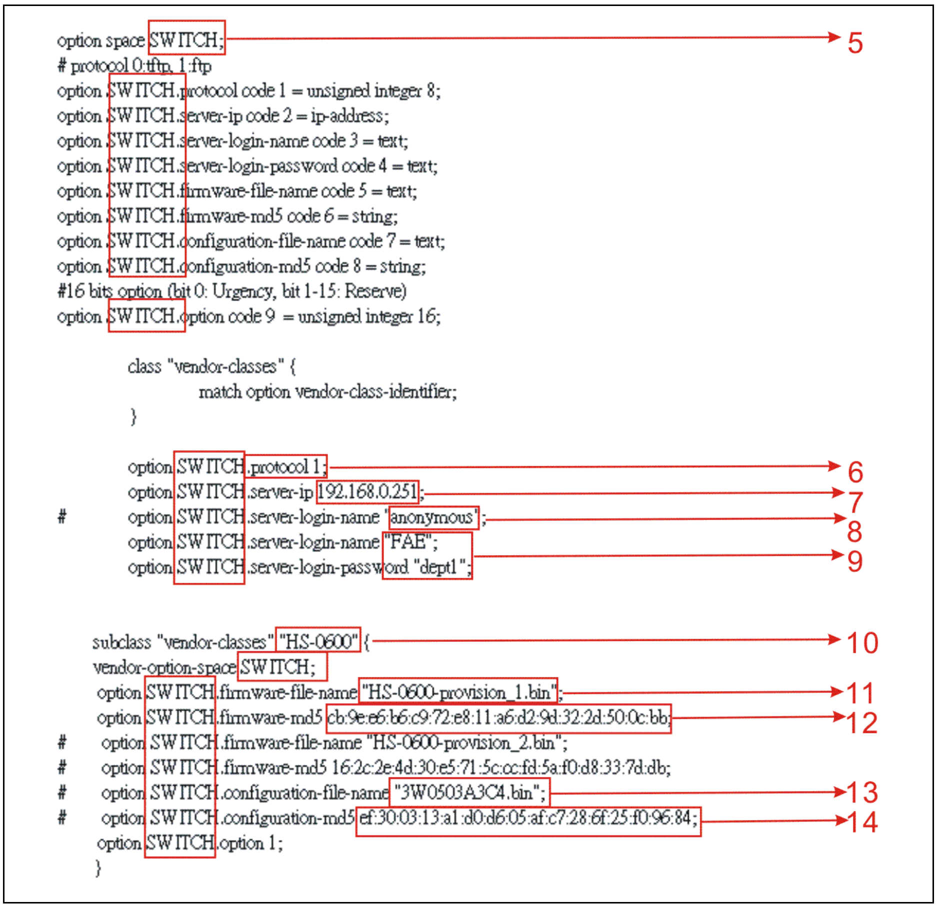
   Default lease time: If a client does not request a specific IP lease time, the server will assign a default lease time value.

   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;
    }
```

5. This value is configurable and can be defined by users.

6. Specify the protocol used (Protocol 1: FTP; Protocol 0: TFTP).

7. Specify the FTP or TFTP IP address.

8. Login TFTP server anonymously (TFTP does not require a login name and password).

9. Specify FTP Server login name and password.

10. Specify the product model name.

11. Specify the firmware filename.

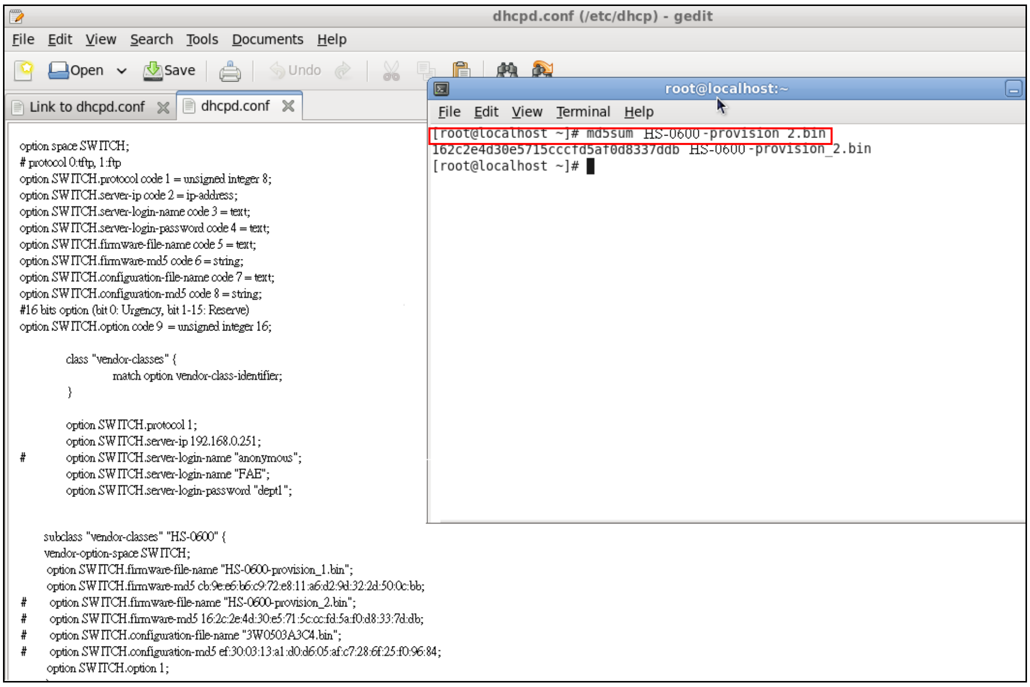
12. Specify the MD5 for firmware image.

13. Specify the configuration filename.

14. 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.*

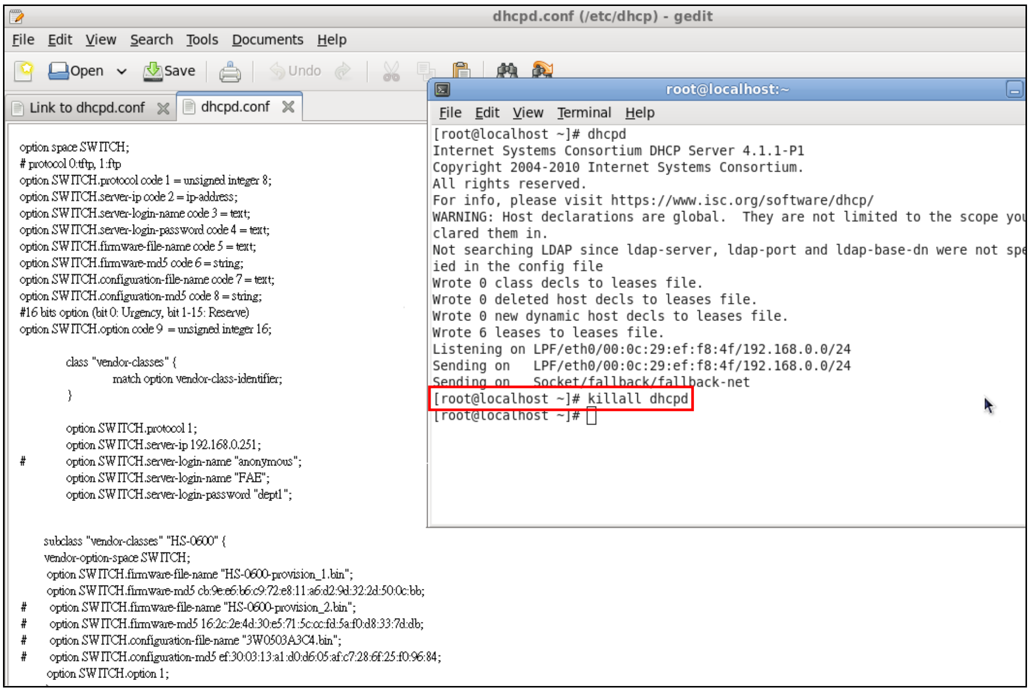


dhcpd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
Link to dhcpd.conf
dhcpd.conf
root@localhost:~
File Edit View Terminal Help

```
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 ~]#
```

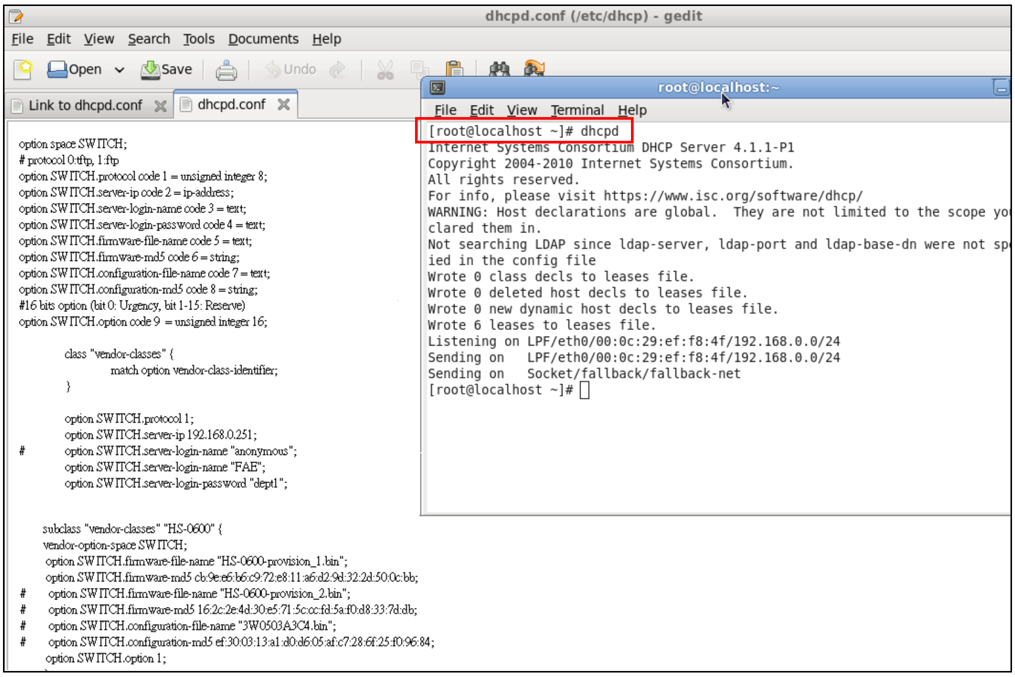
- **Restart DHCP service**



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 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:

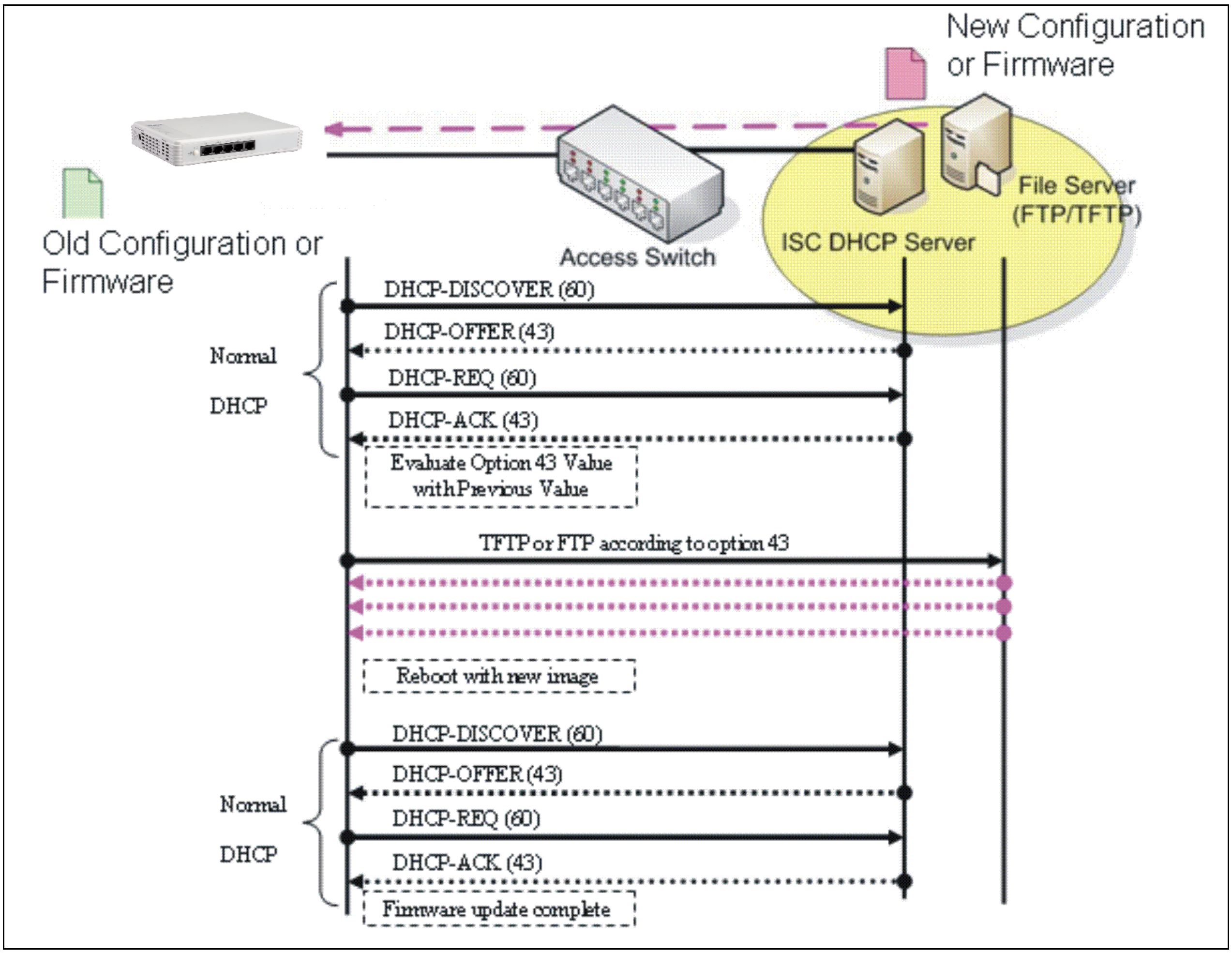
1. ISC DHCP server will recognize the device when it receives an IP address request sent by the device, and it will tell the device how to get a new firmware or configuration.

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: FreeRADIUS Readme

The simple quick setup of FreeRADIUS server for RADIUS Authentication is described below.

On the server-side, you need to 1) create a CTS vendor-specific dictionary and 2) modify three configuration files, “**dictionary**”, “**authorize**”, and “**clients.conf**”, which are already included in FreeRADIUS upon the completed installation.

** Please use any text editing software (e.g. Notepad) to carry out the following file editing works.*

1. Creating a CTS vendor-specific dictionary

Create an empty text file with the filename of “**dictionary.cts”**, copy-and-paste the following defined attributes and values into the document, and move “**dictionary.cts**” to the directory **/etc/raddb**.

```
#
#    dictionary of Connection Technology Systems Inc.
#

VENDOR    cts  9304

#
#    These attributes contain the access-level value.
#

#define ACCOUNT_VALID  0
#define ACCOUNT_STATUS     1
#define DESCRIPTION  2
#define IP_SECURITY  3
#define IP_ADDRESS   4
#define IPMASK       5
#define IPTRAPDEST   6
#define CONSOLE_LEVEL  7
#define SNMP_LEVEL   8
#define WEB_LEVEL    9

BEGIN-VENDOR    cts

ATTRIBUTE    ACCOUNT_VALID       0    integer
ATTRIBUTE    ACCOUNT_STATUS           1    integer
ATTRIBUTE    DESCRIPTION      2    string
ATTRIBUTE    IP_SECURITY      3    integer
ATTRIBUTE    IP_ADDRESS       4    ipaddr
ATTRIBUTE    IPMASK           5    ipaddr
ATTRIBUTE    IPTRAPDEST       6    ipaddr
ATTRIBUTE    CONSOLE_LEVEL       7    integer
ATTRIBUTE    SNMP_LEVEL       8    integer
ATTRIBUTE    WEB_LEVEL        9    integer


VALUE ACCOUNT_VALID  Valid        1
VALUE ACCOUNT_VALID  Invalid      0
VALUE ACCOUNT_STATUS    Valid          1
VALUE ACCOUNT_STATUS    Invalid        0

VALUE IP_SECURITY  Enable       1
VALUE IP_SECURITY  Disable      0

VALUE CONSOLE_LEVEL  Access-Denied  0
VALUE CONSOLE_LEVEL  Read-Only  1
VALUE CONSOLE_LEVEL  Read-Write 2
VALUE CONSOLE_LEVEL  Administrator    3

VALUE SNMP_LEVEL  Access-Denied  0
VALUE SNMP_LEVEL  Read-Only  1
VALUE SNMP_LEVEL  Read-Write 2
VALUE SNMP_LEVEL  Administrator    3

VALUE WEB_LEVEL    Access-Denied  0
VALUE WEB_LEVEL    Read-Only  1
VALUE WEB_LEVEL    Read-Write 2
VALUE WEB_LEVEL    Administrator    3

END-VENDOR  cts
```

2. Modifying three configuration files

** Before editing any of the following files, it’s good practice to read through the official and most-current documentation contained within each file mentioned down below.*

- In the file "**dictionary**" under the directory **/etc/raddb**

Append the following include statement to enable dictionary-referencing:

$INCLUDE dictionary.cts

- In the file "**authorize**", under the directory **/etc/raddb/mods-config/files**

Set up user name, password, and other attributes to specify authentication security and configuration information of each user.

Snippet from within the “**authorize**” file:

```
steve    Password.Cleartext := "testing"
      Service-Type = Framed-User,
      Framed-Protocol = PPP,
      Framed-IP-Address = 172.16.3.33,
      Framed-IP-Netmask = 255.255.255.0,
      Framed-Routing = Broadcast-Listen,
      Framed-Filter-Id = "std.ppp",
      Framed-MTU = 1500,
      Framed-Compression = Van-Jacobsen-TCP-IP
```

- In the file "**clients.conf**", under the directory **/etc/raddb**

Set the valid range of RADIUS client IP addresses to allow permitted clients to send packets to the server.

Snippet from within the “**clients.conf**” file:

```
client localhost {
      ipaddr   = 127.0.0.1
      secret   = testing123
}
```

* The snippet allows packets only sent from 127.0.0.1 (localhost), which mainly serves as a server testing configuration. For permission of packets from the otherwise IP addresses, specify the IP address by following the syntax of the snippets within the “**clients.conf**”.