CONNECTION TECHNOLOGY SYSTEMS

FOS-5152 Series

48-port 100/1000Base-X SFP + 4-port 1G/10GBase-R SFP+ L2 Managed Fiber Switch

Network Management

User's Manual

Version 1.1

Revision History

Version	F/W	Date	Description
1.0	1.00.00	2020/11/20	First release
1.1	1.00.0D	2021/08/16	**Add:** Event Record Command (Section 2.6.9) Fast Redundancy Command (Section 2.6.10) Fast Redundancy (Section 4.6) Management Authentication (Section 4.16.4) **Revise:** IP Command (Section 2.6.11) MAC Command (Section 2.6.16) Management Command (Section 2.6.17) Show log Command (Section 2.6.35) MAC Address Table (Section 4.7.3) IGMP/MLD Setup (Section 4.9.1.1) IGMP Group Table (Section 4.9.1.7) DHCP Snooping Setup (Section 4.11.1.1) DHCP Snooping Table (Section 4.11.1.3) Event Log (Section 4.15.7) RADIUS/TACACS+ (Section 4.16.3)

Trademarks

CTS is a registered trademark of Connection Technology Systems Inc..
Contents are subject to revision without prior notice.
All other trademarks remain the property of their owners.

Copyright Statement

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

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.

CTS Contact Information

■ Headquarters/Manufacturer:

Connection Technology Systems Inc.

18F-6, No.79, Sec.1, Xintai 5th Rd.,

Xizhi Dist., New Taipei City 221, Taiwan(R.O.C.)

Tel: +886-2-2698-9661

Fax: +886-2-2698-3960

Sales Direct Line:+886-2-2698-9201

www.ctsystem.com

■ Global Offices:

Connection Technology USA

40538 La Purissima Way,

Fremont, CA 94539, USA

Tel: +1-510-509-0304

Sales Direct Line: +1-510-509-0305

E-mail:cts_us@ctsystem.com

Connection Technology Systems Japan

Higobashi Bldg. No.3 R201, 1-23-13,

Edobori, Nishi-ku, Osaka 550-0002, Japan

Tel: +81-6-6450-8890

E-mail: cts_japan@ctsystem.com

Connection Technology Systems NE AB

August Barks Gata 21,

421 32 Västra Frölunda, Sweden

Tel: +46-31-221980

E-mail: info@ctsystem.se

Connection Technology Systems Central Europe (COMPONET Handels GmbH)

Hirschstettner Straße 19-21/Stiege I

A-1220 Vienna, Austria

Tel: +43-1-235 05 66-0

E-mail: cts_ce@ctsystem.com

CTS Connection Technology Systems DE GmbH

An den Bergen 17, 60437 Frankfurt am Main, Germany

Tel: +491711051295

E-mail: cts_de@ctsystem.com

Table of Content

1. INTRODUCTION

Thank you for using the 48 100/1000Base-X SFP ports plus 4 1G/10GBase-R SFP+ uplink ports Managed Switch that is specifically designed for FTTx applications. The Managed Switch provides a built-in management module that enables users to configure and monitor the operational status both locally and remotely. This user's manual will explain how to use command-line interface and web management to configure your Managed Switch. The readers of this manual should have knowledge about their network typologies and about basic networking concepts so as to make the best of this user's manual and maximize the Managed Switch's performance for your personalized networking environment.

1.1 Management Options

Switch management options available are listed below:

- Local Console Management
- Telnet Management
- SNMP Management
- WEB Management
- SSH Management

Local Console Management

Local Console Management is done through the RS-232 RJ-45 Console port located on the front panel of the Managed Switch. Direct RS-232 cable connection between the PC and the Managed switch is required for this type of management.

Telnet Management

Telnet runs over TCP/IP and allows you to establish a management session through the network. Once the Managed switch is on the network with proper IP configurations, you can use Telnet to login and monitor its status remotely.

SNMP Management

SNMP is also done over the network. Apart from standard MIB (Management Information Bases), an additional private MIB is also provided for SNMP-based network management system to compile and control.

Web Management

Web Management is done over the network and can be accessed via a standard web browser, such as Microsoft Internet Explorer. Once the Managed Switch is available on the network, you can login and monitor the status of it through a web browser remotely or locally. Web management in the local site, especially for the first time use of the Managed Switch to set up the needed IP, can be done through one of the SFP/SFP+ ports located on the front panel of the Managed Switch. A converter and direct RJ-45 LAN cable connection between a PC and the Managed Switch are required for Web Management.

SSH Management

SSH Management supports encrypted data transfer to prevent the data from being “stolen” for remote management. You can use PuTTY, a free and open source terminal emulator application which can act as a client for the SSH, to gain access to the Managed Switch.

1.2 Management Software

The following is a list of management software options provided by this Managed Switch:

- Managed Switch CLI interface
- SNMP-based Management Software
- Web Browser Application

Console Program

The Managed Switch has a built-in Command Line Interface called the CLI which you can use to:

- Configure the system
- Monitor the status
- Reset the system

You can use CLI as the only management system. However, other network management options, SNMP-based management system, are also available.

You can access the text-mode Console Program locally by connecting a VT-100 terminal - or a workstation running VT100 emulation software - to the Managed Switch RS-232 RJ-45 Console port directly. Or, you can use Telnet to login and access the CLI through network connection remotely.

SNMP Management System

Standard SNMP-based network management system is used to manage the Managed Switch through the network remotely. When you use a SNMP-based network management system, the Managed Switch becomes one of the managed devices (network elements) in that system. The Managed Switch management module contains an SNMP agent that will respond to the requests from the SNMP-based network management system. These requests, which you can control, can vary from getting system information to setting the device attribute values.

The Managed Switch's private MIB is provided for you to be installed in your SNMP-based network management system.

Web Browser Application

You can manage the Managed Switch through a web browser, such as Internet Explorer or Google Chrome, etc.. (The default IP address of the Managed Switch port can be reached at **"http://192.168.0.1"**.) For your convenience, you can use either this Web-based Management Browser Application program or other network management options, for example SNMP-based management system as your management system.

1.3 Management Preparations

After you have decided how to manage your Managed Switch, you are required to connect cables properly, determine the Managed switch IP address and, in some cases, install MIB shipped with your Managed Switch.

Connecting the Managed Switch

It is very important that the proper cables with the correct pin arrangement are used when connecting the Managed switch to other switches, hubs, workstations, etc..

1000Base-X/100Base-FX SFP Port, 1G/10GBase-R SFP+ Port

The small form-factor pluggable (SFP) or the enhanced small form-factor pluggable (SFP+) transceiver is a compact optical transceiver used in optical data communication applications. It interfaces a network device mother board (for a switch, router or similar device) to a fiber optic or unshielded twisted pair networking cable. It is a popular industry format supported by several fiber optic component vendors. SFP+ transceiver can bring speeds up to 10 Gbit/s.

SFP/SFP+ transceivers are available with a variety of different transmitter and receiver types, allowing users to select the appropriate transceiver for each link to provide the required optical reach over the available optical fiber type.

SFP/SFP+ slot supports hot swappable SFP/SFP+ fiber transceiver. Before connecting the other switches, workstation or Media Converter, make sure both side of the SFP/SFP+ transfer are with the same media type, for example, 1000Base-SX to 1000Base-SX, 1000Base-LX to 1000Base-LX, 10GBASE-LR to 10GBASE-LR, and check the fiber-optic cable type matches the SFP/SFP+ transfer model. To connect to 1000Base-SX transceiver, use the multi-mode fiber cable with male duplex LC connector type for one side. To connect to 1000Base-LX transfer, use the single-mode fiber cable with male duplex LC connector type for one side.

RS-232 RJ-45 Port (Console Port)

The RS-232 RJ-45 port is located at the front of the Managed Switch. This RJ-45 port is used for local, out-of-band management. Since this RJ-45 port of the Managed switch is DTE, a null modem is also required to be connected to the Managed Switch and the PC. By connecting this RJ-45 port, it allows you to configure & check the status of Managed Switch even when the network is down.

IP Addresses

IP addresses have the format n.n.n.n, (The default factory setting is 192.168.0.1).

IP addresses are made up of two parts:

- The first part (for example 192.168.n.n) refers to network address that identifies 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 which intends to connect to the Internet.

- The second part (for example n.n.0.1) 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 with the allocation organization where 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 network, 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 performed.

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 the proper operation of a network with subnets defined.

MIB for Network Management Systems

Private MIB (Management Information Bases) is provided for managing the Managed Switch through the SNMP-based network management system. You must install the private MIB into your SNMP-based network management system first.

The MIB file is shipped together with the Managed Switch. The file name extension is “.mib” that allows SNMP-based compiler can read and compile.

2. Command Line Interface (CLI)

This chapter introduces you how to use Command Line Interface CLI, specifically in:

- Local Console
- Telnet
- Configuring the system
- Resetting the system

The interface and options in Local Console and Telnet are the same. The major difference is the type of connection and the port that is used to manage the Managed Switch.

2.1 Using the Local Console

Local Console is always done through the RS-232 RJ-45 port and requires a direct connection between the switch and a PC. This type of management is useful especially when the network is down and the switch cannot be reached by any other means.

You also need the Local Console Management to setup the Switch network configuration for the first time. You can setup the IP address and change the default configuration to the desired settings to enable Telnet or SNMP services.

Follow these steps to begin a management session using Local Console Management:

Step 1. Attach the serial cable to the RS-232 RJ-45 port located at the front of the Switch.

Step 2. Attach the other end to the serial port of a PC or workstation.

Step 3. Run a terminal emulation program using the following settings:

- **Emulation** VT-100/ANSI compatible
- **BPS** 9600
- **Data bits** 8
- **Parity** None
- **Stop bits** 1
- **Flow Control** None
- **Enable** Terminal keys

Step 4. Press Enter to access the CLI (Command Line Interface) mode.

2.2 Remote Console Management - Telnet

You can manage the Managed Switch via Telnet session. However, you must first assign a unique IP address to the Switch before doing so. Use the Local Console to login the Managed Switch and assign the IP address for the first time.

Follow these steps to manage the Managed Switch through Telnet session:

Step 1. Use Local Console to assign an IP address to the Managed Switch

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

Step 2. Run Telnet

Step 3. Log into the Switch CLI

Limitations: When using Telnet, keep the following in mind:

Only 5 active Telnet sessions can access the Managed Switch at the same time.

2.3 Navigating CLI

When you successfully access the Managed 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, the User mode only provides users with basic functions to operate the Managed Switch. If you would like to configure advanced features of the Managed Switch, such as, VLAN, QoS, Rate limit control, you must enter the Configuration mode. The following table provides an overview of modes available in this Managed Switch.

Command Mode	Access Method	Prompt Displayed	Exit Method
User mode	Login username & password	Switch>	logout, exit
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, Ctrl + Z

NOTE: *By default, the model name will be used for the prompt display. You can change the prompt display to the one that is ideal for your network environment using the hostname command. However, for convenience, the prompt display "Switch" will be used throughout this user's manual.*

2.3.1 General Commands

This section introduces you some general commands that you can use in User, Privileged, and Configuration 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 Console or Telnet session.	User Mode Privileged Mode

2.3.2 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.

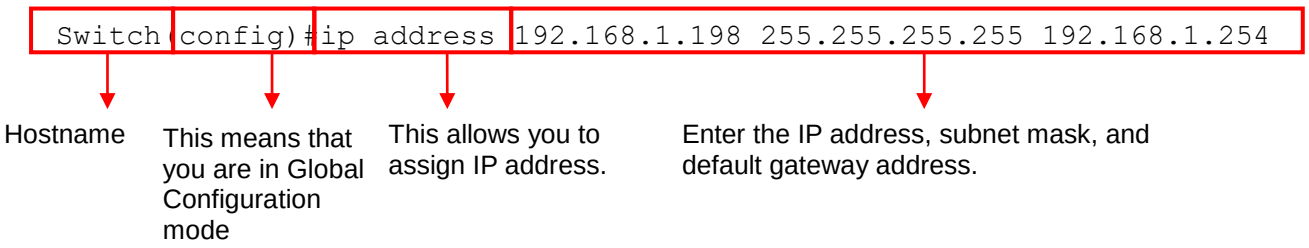
Unfinished command followed by ?	Enter an unfinished command or keyword and press “?” key to complete the command and get command syntax help.
	
	Example: List all available commands starting with the characters that you enter.
	
	`Switch#h?`
	`help  Show available commands`
	`history  Show history commands`

A space followed by ?	Enter a command and then press Spacebar followed by a “?” key to view the next parameter.
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.

2.3.3 Command Format

While in CLI, you will see several symbols very often. As mentioned above, you might already know what ">", "#" and (config)# represent. However, to perform what you intend the device to do, you have to enter a string of complete command correctly. For example, if you want to assign IP address for the Managed 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]`



The following table lists common symbols and syntax that you will see very 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 Global Configuration mode.
Syntax	**Brief Description**
[ ]	Reference parameter.
[-s size] [-r repeat] [-t timeout]	These three parameters are used in ping command and are optional, which means that you can ignore these three parameters if they are unnecessary when executing ping command.
[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]	Enter one port number. See Section 2.6.29 for detailed explanations.
[port_list]	Enter a range of port numbers or several discontinuous port numbers. See Section 2.6.29 for detailed explanations.
[forced_true | forced_false | auto]	There are three 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 value 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 three 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 (separated by a hyphen)
	
	`Switch(config)#qos 802.1p-map 1-3 0`
	
	`Switch(config)#qos dscp-map 10-15 3`

2.3.4 Login Username & Password

Default Login

When you enter Console session, a login prompt for username and password 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 the 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.

Privileged Mode Password

Privileged mode is password-protected. When you try to enter Privileged mode, a password prompt will appear to request the user to provide the legitimate passwords. Privileged mode password is the same as the one entered after login password prompt. By default, no password is required. Therefore, press **Enter** key in password prompt.

Forgot Your Login Username & Password

If you forgot your login username and password, you can use the "reset button" on the front panel to set all configurations back to factory defaults. Once you have performed system reset to defaults, you can login with default username and password. Please note that if you use this method to gain access to the Managed 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 reloaded to the Managed Switch for use when you gain access again to the device.

2.4 User Mode

In User mode, only a limited set of commands are provided. Please note that in User mode, you have no authority to configure advanced settings. You need to enter Privileged mode and Configuration mode to set up advanced functions of the Switch. 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 the User mode or close the terminal connection.
help	Display a list of available commands in User mode.
history	Display the command history.
logout	Logout from the Managed Switch.
loopback	Test whether the connectivity of the networking cable between devices works normally or not.
ping	Test whether a specified network device or host is reachable or not.
traceroute	Trace the route to HOST
enable	Enter the Privileged mode.

2.4.1 Loopback Command

Loopback is used to test the networking cable connectivity between devices. Enter the **loopback** command in User mode. In this command, you need to specify the diagnostic port, accompany port, VLAN ID and the time value for the loopback test.

Command	Parameter	Description
Switch> loopback diagnostic [port_number] accompany [port_number] vid [1-4094] time [1-10]	[port_number]	Specify the diagnostic port for the loopback test.
	[port_number]	Specify the accompany port for the loopback test.
	[1-4094]	Specify the VLAN ID.
	[1-10]	Configure the loopback test time in miniutes.
Example of Loopback Test		
Switch> loopback diagnostic 1 accompany 2 vid 300 time 3		Configure Port 1 as the diagnostic port, Port 2 as the accompany port, VLAN ID as 300 for the loopback test that will last for 3 miniutes.

2.4.2 Ping Command

Ping is used to test the connectivity of end devices and also can be used to self test the network interface card. Enter the **ping** command in User mode. In this command, you can add an optional packet size value and an optional value for the number of counts that PING packets are sent.

Command	Parameter	Description
Switch> ping [A.B.C.D | A:B:C:D:E:F:G:H] [-s 1-20000] [-c 1-99]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IPv4/IPv6 address that you would like to ping.
	[-s 1-20000]	Enter the packet size that would be sent. The allowable packet size is from 1 to 20000 bytes. (optional)
	[-c 1-99]	Enter the counts of PING packets that would be transmitted. The allowable value is from 1 to 99. (optional)
Example		
Switch> ping 8.8.8.8 Switch> ping 8.8.8.8 –s 128 –c 10 Switch> ping 2001:4860:4860::8888 Switch> ping 2001:4860:4860::8888 –s 128 –c 10		

2.4.3 Traceroute Command

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

Command	Parameter	Description
Switch> traceroute [A.B.C.D | A:B:C:D:E:F:G:H] [-m 1-255] [-p 1-5] [-w 1-5]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the target IPv4/IPv6 address of the host that you would like to trace.
	[-m 1-255]	Specify the number of hops between the local host and the remote host. The allowable number of hops is from 1 to 255. (optional)
	[-p 1-5]	Enter the counts of PROBE packets that would be transmitted. The allowable value is from 1 to 5. (optional)
	[-w 1-5]	Specify the response time from the remote host. The allowable time value is from 1 to 5 seconds. (optional)
Example		
Switch> traceroute 8.8.8.8 Switch> traceroute 8.8.8.8 –m 30 Switch> traceroute 2001:4860:4860::8888 Switch> traceroute 2001:4860:4860::8888 -m 30 -p 5 -w 5		

2.5 Privileged Mode

The only place where you can enter the Privileged mode is in User mode. When you successfully enter the Privileged mode (this mode is password protected), 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 via FTP or TFTP server.
disable	Exit Privileged mode and return to User Mode.
exit	Exit Privileged mode and return to User Mode.
firmware	Allow users to update firmware via FTP or TFTP.
help	Display a list of available commands in Privileged mode.
history	Show commands that have been used.
ip	Set up the DHCP recycle.
logout	Logout from the Managed Switch.
loopback	Test whether the connectivity of the networking cable between devices works normally or not.
ping	Test whether a specified network device or host is reachable or not.
reload	Restart the Managed Switch.
traceroute	Trace the route to HOST.
write	Save your configurations to Flash.
configure	Enter Global Configuration mode.
show	Show a list of commands or show the current setting of each listed command.

2.5.1 Copy-cfg Command

Use “copy-cfg” command to backup a configuration file via FTP or TFTP server and restore the Managed Switch back to the defaults or to the defaults but keep IP configurations.

1. Restore a configuration file via FTP or TFTP server.

Command	Parameter	Description
Switch# copy-cfg from ftp [A.B.C.D | A:B:C:D:E:F:G:H] [file name] [user_name] [password]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IPv4/IPv6 address of your FTP server.
	[file name]	Enter the configuration file name that you would like 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 | A:B:C:D:E:F:G:H] [file_name]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IPv4/IPv6 address of your TFTP server.
	[file name]	Enter the configuration file name that you would like 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. Backup a configuration file to FTP or TFTP server.

Command	Parameter	Description
Switch# copy-cfg to ftp [A.B.C.D | A:B:C:D:E:F:G:H] [file name] [running | default | startup] [user_name] [password]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IPv4/IPv6 address of your FTP server.
	[file name]	Enter the configuration file name that you want to backup.
	[running | default | startup]	Specify backup config to be running, default or startup
	[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 | A:B:C:D:E:F:G:H] [file_name] [running | default | startup]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IPv4/IPv6 address of your TFTP server.
	[file name]	Enter the configuration file name that you want to backup.
	[running | default | startup]	Specify backup config to be running, default or startup
Example		
Switch# copy-cfg to ftp 192.168.1.198 HS_0600_file.conf running misadmin1 abcxyz Switch# copy-cfg to tftp 192.168.1.198 HS_0600_file.conf startup		

3. Restore the Managed Switch back to default settings.

Command / Example
Switch# copy-cfg from default Switch# reload

4. Restore the Managed Switch back to default settings but keep IP configurations.

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

2.5.2 Firmware Command

To upgrade firmware via TFTP or FTP server.

Command	Parameter	Description
Switch# firmware upgrade ftp [A.B.C.D | A:B:C:D:E:F:G:H] [file_name] [Image-1| Image-2] [user_name] [password]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IP address of your FTP server.
	[file name]	Enter the firmware file name that you want to upgrade.
	[Image-1| Image-2]	Choose image-1 or image-2 for the firmware to be upgraded to.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
Switch# firmware upgrade tftp	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IP address of your TFTP server.

[A.B.C.D | A:B:C:D:E:F:G:H] [file_name] [Image-1| Image-2]	[file_name]	Enter the firmware file name that you want to upgrade.
	[Image-1| Image-2]	Choose image-1 or image-2 for the firmware to be upgraded to.
Example		
Switch# firmware upgrade ftp 192.168.1.198 HS_0600_file.bin Image-1 edgeswitch10 abcxyz		
Switch# firmware upgrade tftp 192.168.1.198 HS_0600_file.bin Image-2		

2.5.3 IP Command

Command	Parameter	Description
Switch# ip address dhcp recycle		DHCP Release packets and Discover packets will be sent to DHCP server in a manual way. And it will ask for IP address from DHCP server again. **Note 1: Need to enable DHCP mode under the IP global configuration mode before issuing this command. See Section 2.6.9 for more details.** **Note 2: The command is just one-time command, and the setting will not be saved into the configuration file.**

2.5.4 Loopback Command

Loopback is used to test the networking cable connectivity between devices. Enter the loopback command in Privileged mode. In this command, you need to specify the diagnostic port, accompany port, VLAN ID and the time value for the loopback test.

Command	Parameter	Description
Switch# loopback diagnostic [port_number] accompany [port_number] vid [1-4094] time [1-10]	[port_number]	Specify the diagnostic port for the loopback test.
	[port_number]	Specify the accompany port for the loopback test.
	[1-4094]	Specify the VLAN ID.
	[1-10]	Configure the loopback test time in miniutes.
Example of Loopback Test		
Switch# loopback diagnostic 1 accompany 2 vid 300 time 3		Configure Port 1 as the diagnostic port, Port 2 as the accompany port, VLAN ID as 300 for the loopback test that will last for 3 miniutes.

2.5.5 Ping Command

Command	Parameter	Description
Switch# ping [A.B.C.D | A:B:C:D:E:F:G:H] [-s 1-20000] [-c 1-99]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IPv4/IPv6 address that you would like to ping.
	[-s 1-20000]	Enter the packet size that would be sent. The allowable packet size is from 1 to 20000 bytes. (optional)
	[-c 1-99]	Enter the counts of PING packets that would be transmitted. The allowable value is from 1 to 99. (optional)
Example		
Switch# ping 8.8.8.8 Switch# ping 8.8.8.8 –s 128 –c 10 Switch# ping 2001:4860:4860::8888 Switch# ping 2001:4860:4860::8888 –s 128 –c 10		

2.5.6 Reload Command

1. **To restart the Managed Switch.**

Command / Example
Switch# reload

2. **To specify the image for the next restart before restarting.**

Command / Example
Switch# reload Image-2 OK! Switch# reload

2.5.7 Traceroute Command

Traceroute is used to trace the path between the local host and the remote host. Enter the **traceroute** command in Privileged mode. In this command, you can add an optional maximum hops value for the number of hops that packets are sent and received, an optional value for the number of counts that PROBE packets are sent, or an optional waiting time value of the remote host response.

Command	Parameter	Description
Switch# traceroute [A.B.C.D | A:B:C:D:E:F:G:H] [-m 1-255] [-p 1-5] [-w 1-5]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the target IPv4/IPv6 address of the host that you would like to trace.
	[-m 1-255]	Specify the number of hops between the local host and the remote host. The allowable number of hops is from 1 to 255. (optional)
	[-p 1-5]	Enter the counts of PROBE packets that would be transmitted. The allowable value is from 1 to 5. (optional)
	[-w 1-5]	Specify the response time from the remote host. The allowable time value is from 1 to 5 seconds. (optional)
Example		
Switch# traceroute 8.8.8.8 Switch# traceroute 8.8.8.8 –m 30 Switch# traceroute 2001:4860:4860::8888 Switch# traceroute 2001:4860:4860::8888 -m 30 -p 5 -w 5		

2.5.8 Write Command

To save running configurations to startup configurations, please enter the command of “write”. All unsaved configurations will be lost when you restart the Managed Switch.

Command / Example
Switch# write Save Config Succeeded!

2.5.9 Configure Command

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

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

2.5.10 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. It can be used in Privileged or Configuration mode. The following describes different uses of “show” command.

1. Display system information

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

Company Name: Display a company name for this Managed Switch. Use “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 Switch. Use “switch-info system-contact [sys_contact]” command to edit this field.

System Name: Display a descriptive system name for this Managed Switch. Use “switch-info system-name [sys_name]” command to edit this field.

System Location: Display a brief location description for this Managed Switch. Use “switch-info system-location [sys_location]” command to edit this field.

DHCP/DHCPv6 Vendor ID: Display the Vendor Class Identifier used for DHCP/DHCPv6 relay agent function. Use “switch-info dhcp-vendor-id [dhcp_vendor_id]” command to edit this field.

Model Name: Display the product’s model name.

Host Name: Display the product’s host name. Use “switch-info host-name [host_name]” command to edit this field.

Current Boot Image: The image that is currently using.

Configured Boot Image: The image you would like to use after rebooting.

Image-1 Version: Display the firmware version 1 (image-1) used in this device.

Image-2 Version: Display the firmware version 2 (image-2) used in this device.

M/B Version: Display the main board version.

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

Date Code: Display the date code of the Managed Switch firmware.

Up Time: Display the up time since last restarting.

Local Time: Display the local time of the system.

FAN State: Display the status of FAN1, FAN2 and FAN3.

Power A/B: Display the installation status, the type of power source and state of Power A/B.

CPU Temperature: Display the current CPU temperature of this device.

2. Display or verify currently-configured settings

Refer to the following sub-sections. “Interface command”, “IP command”, “MAC command”, “QoS command”, “Security command”, “SNMP-Server command”, “User command”, “VLAN command” sections, etc.

3. Display interface information or statistics

Refer to “Show interface statistics command” and “Show sfp command” sections.

4. Show default, running and startup configurations

Refer to “Show default-config command”, “Show running-config command” and “Show start-up-config command” sections.

5. Show CPU & Memory Statistics

Show CPU utilization and memory usage rate. Refer to “Switch-info command” section.

6. Show the fan speed

Show the detailed information about of FAN1, FAN2 and FAN3. It includes the current fan speed and state. Refer to “Switch-info command” section.

7. Show the system voltage

Show the current internal system powers’ voltage and state. Refer to “Switch-info command” section.

8. Show Event Log

Show the log of all events information. Refer to “Show log command” section.

2.6 Configuration Mode

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

Command	Description
acl	Set up access control entries and lists.
archive	Manage archive configuration files.
channel-group	Configure static link aggregation groups or enable LACP function.
dot1x	IEEE 802.1X global configuration commands.
digital	Global Digital Input configuration commands.
event record	Configure the Event Record function.
exit	Exit the global configuration mode.
fast-redundancy	Set up the Fast Redundancy function.
help	Display a list of available commands in the global configuration mode.
history	Show commands that have been used.
ip	Set up the IPv4 address and enable DHCP mode & IGMP snooping.
ipv6	To enable ipv6 function and set up IP address.
lldp	LLDP global configuration mode.
loop-detection	Configure loop-detection to prevent loop between switch ports by locking them.
l2protocol-tunnel	Set up Layer 2 protocol tunnel function.
mac	Set up MAC learning function of each port.
management	Set up console/telnet/web/SSH access control and timeout value, RADIUS/TACACS+, and authentication method management.
mirror	Set up target port for mirroring.
mvr	Configure MVR (Multicast VLAN Registration) settings.
ntp	Set up required configurations for Network Time Protocol.
qos	Set up the priority of packets within the Managed Switch.
security	Configure broadcast, unknown multicast, unknown unicast 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	Set up acceptable frame size and address learning, etc.
switch-info	Edit the system information.
syslog	Set up required configurations for Syslog server.
terminal	Set up Terminal functions.
user	Create a new user account.
vlan	Set up VLAN mode and VLAN configuration.
no	Disable a command or reset it back to its default setting.
interface	Select a single interface or a range of interfaces.
show	Show a list of commands or show the current setting of each listed command.

2.6.1 Entering Interface Numbers

In the Global Configuration mode, you can configure a command that only applies to interfaces specified. For example, you can set up each interface’s VLAN assignment, speeds, or duplex modes. To configure, 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 a command or commands.

Commands	Description
Switch(config)# interface 1 Switch(config-if-1)#	Enter a single interface. Only interface 1 will apply commands entered.
Switch(config)# interface 1,3,5 Switch(config-if-1,3,5)#	Enter three discontinuous interfaces, separated by commas. Interface 1, 3, 5 will apply 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 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 comma and hypen to signify the combination of different interface numbers. In this example, interface 1, 3, 4, 5 will apply commands entered.

2.6.2 No Command

Almost every command that you enter in Configuration mode can be negated using “no” command followed by the original or similar command. The purpose of “no” command is to disable a function, remove a command, or reset the setting back to the default value. In each sub-section below, the use of no command to fulfill different purposes will be introduced.

2.6.3 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. It can be used in Privileged or Configuration mode. The following describes different uses of “show” command.

1. Display system information

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

Company Name: Display a company name for this Managed Switch. Use “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 Switch. Use “switch-info system-contact [sys_contact]” command to edit this field.

System Name: Display a descriptive system name for this Managed Switch. Use “switch-info system-name [sys_name]” command to edit this field.

System Location: Display a brief location description for this Managed Switch. Use “switch-info system-location [sys_location]” command to edit this field.

DHCP/DHCPv6 Vendor ID: Display the Vendor Class Identifier used for DHCP/DHCPv6 relay agent function. Use “switch-info dhcp-vendor-id [dhcp_vendor_id]” command to edit this field.

Model Name: Display the product’s model name.

Host Name: Display the product’s host name. Use “switch-info host-name [host_name]” command to edit this field.

Current Boot Image: The image that is currently using.

Configured Boot Image: The image you would like to use after rebooting.

Image-1 Version: Display the firmware version 1 (image-1) used in this device.

Image-2 Version: Display the firmware version 2 (image-2) used in this device.

M/B Version: Display the main board version.

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

Date Code: Display the date code of the Managed Switch firmware.

Up Time: Display the up time since last restarting.

Local Time: Display the local time of the system.

FAN State: Display the status of FAN1, FAN2 and FAN3.

Power A/B: Display the installation status, the type of power source and state of Power A/B.

CPU Temperature: Display the current CPU temperature of this device.

2. Display or verify currently-configured settings

Refer to the following sub-sections. “Interface command”, “IP command”, “MAC command”, “QoS command”, “Security command”, “SNMP-Server command”, “User command”, “VLAN command” sections, etc.

3. Display interface information or statistics

Refer to “Show interface statistics command” and “Show sfp information command” sections.

4. Show default, running and startup configurations

Refer to “Show default-config copmmand”, “Show running-config command” and “Show start-up-config command” sections.

5. Show CPU & Memory Statistics

Show CPU utilization and memory usage rate. Refer to “Switch-info command” section.

6. Show the fan speed

Show the detailed information about of FAN1, FAN2 and FAN3. It includes the current fan speed and state. Refer to “Switch-info command” section.

7. Show the system voltage

Show the current internal system powers’ voltage and state. Refer to “Switch-info command” section.

8. Show Event Log

Show the log of all events information. Refer to “Show log command” section.

2.6.4 ACL Command

ACL Command	Parameter	Description
Switch(config)# acl ipv4 [1-64]	[1-64]	The total number of IPv4 ACL rule can be created is 64. Use this command to enter ACL configuration mode for each ACL rule. When you enter each ACL rule, you can further configure detailed settings for this rule.
Switch(config)# acl ipv6 [1-32]	[1-32]	The total number of IPv6 ACL rule can be created is 32. Use this command to enter ACL configuration mode for each ACL rule. When you enter each ACL rule, you can further configure detailed settings for this rule.
Switch(config-acl-ipv4(6)-RULE)# action [deny | copy(mirror) | permit | redirect]	[deny | copy(mirror) | permit | redirect]	Specify the action to the ACL-matched packet.
Switch(config-acl-ipv4(6)-RULE)# action-port [port]	[port]	Specify copy(mirror)-to/redirect-to port (1~28).
Switch(config-acl-ipv4(6)-RULE)# apply		Enable the specified ACL rule.
Switch(config-acl-ipv4-RULE)# destination-ipv4 any		Specify destination IPv4 address as “ANY”.
Switch(config-acl-ipv4-RULE)# destination-ipv4 address [A.B.C.D] [0-255.X.X.X]	[A.B.C.D]	Specify destination IPv4 address.
	[0-255.X.X.X]	Specify destination IPv4 mask.
Switch(config-acl-ipv6-RULE)# destination-ipv6 any		Specify destination IPv6 address as “ANY”.
Switch(config-acl-ipv6-RULE)# destination-ipv6 address [A:B:C:D:E:F:G:H] [10~128]	[A:B:C:D:E:F:G:H]	Specify destination IPv6 address.
	[10~128]	Specify destination IPv6 prefix-length.
Switch(config-acl-ipv4(6)-RULE)# destination-l4-port any		Specify destination Layer4 port as “ANY”.
Switch(config-acl-ipv4(6)-RULE)# destination-l4-port [1-65535] [0xWXYZ]	[1-65535]	Specify destination Layer4 port.
	[0xWXYZ]	Specify destination Layer4 mask. (Range:0x0000~FFFF)
Switch(config-acl-ipv4(6)-RULE)# destination-mac		Specify destination MAC as “ANY”.

any		
Switch(config-acl-ipv4(6)-RULE)# destination-mac mac [xx:xx:xx:xx:xx:xx] [ff:ff:ff:00:00:00]	[xx:xx:xx:xx:xx:xx]	Specify destination MAC.
	[ff:ff:ff:00:00:00]	Specify destination MAC mask.
Switch(config-acl-ipv4(6)-RULE)# ethertype [any | 0xWXYZ]	[any | 0xWXYZ]	Specify Ethertype (Range: 0x0000 ~FFFF) or “ANY”.
Switch(config-acl-ipv4(6)-RULE)# ingress-port [any | port-list]	[any | port-list]	Specify ingress port(s) or “ANY”.
Switch(config-acl-ipv4(6)-RULE)# name [name]	[name]	Specify the name to the specified ACL rule.
Switch(config-acl-ipv4(6)-RULE)# protocol [any | 0xWX]	[any | 0xWX]	Specify IPv4 protocol and IPv6 next header (Range: 0x00~FF) or “ANY”.
Switch(config-acl-ipv4(6)-RULE)# rate-limit [0,16-1048560]	[0,16-1048560]	Specify rate limitation from 16 to 1048560 kbps. (0:Disable)
Switch(config-acl-ipv4(6)-RULE)# sequence [1-65536]	[1-65536]	Specify the sequence for the specified ACL rule. (Range: 1-65536, 1 will be processed first.)
Switch(config-acl-ipv4-RULE)# source-ipv4 any		Specify source IPv4 address as “ANY”.
Switch(config-acl-ipv4-RULE)# source-ipv4 address [A.B.C.D] [0-255.X.X.X]	[A.B.C.D]	Specify source IPv4 address.
	[0-255.X.X.X]	Specify source IPv4 mask.
Switch(config-acl-ipv6-RULE)# source-ipv6 any		Specify source IPv6 address as “ANY”.
Switch(config-acl-ipv6-RULE)# source-ipv6 address [A:B:C:D:E:F:G:H] [10~128]	[A:B:C:D:E:F:G:H]	Specify source IPv6 address.
	[10~128]	Specify source IPv6 prefix-length.
Switch(config-acl-ipv4(6)-RULE)# source-l4-port any		Specify source Layer4 port as “ANY”.
Switch(config-acl-ipv4(6)-RULE)# source-l4-port [1-65535] [0xWXYZ]	[1-65535]	Specify source Layer4 port.
	[0xWXYZ]	Specify source Layer4 mask. (Range:0x0000~FFFF)
Switch(config-acl-ipv4(6)-RULE)# source-mac any		Specify source MAC as “ANY”.
Switch(config-acl-ipv4(6)-RULE)# source-mac mac [xx:xx:xx:xx:xx:xx] [ff:ff:ff:00:00:00]	[xx:xx:xx:xx:xx:xx]	Specify source MAC.
	[ff:ff:ff:00:00:00]	Specify source MAC mask.
Switch(config-acl-ipv4(6)-RULE)# tos [any | 0xWX]	[any | 0xWX]	Specify IPv4 TOS and IPv6 traffic class (Range: 0x00~FF) or “ANY”.
Switch(config-acl-ipv4(6)-RULE)# vid [any | 1-4094]	[any | 1-4094]	Specify packet classification 802.1q VLAN ID (Range: 1~4094) or “ANY”.

No command		
Switch(config)# no acl ipv4 [1-64]	[1-64]	Remove the specified IPv4 ACL rule.
Switch(config)# no acl ipv6 [1-32]	[1-32]	Remove the specified IPv6 ACL rule.
Switch(config-acl-ipv4(6)-RULE)# no action		Reset action back to the default (permit).
Switch(config-acl-ipv4(6)-RULE)# no action-port		Reset copy(mirror)-to/redirect-to port back to the default (Port 1).
Switch(config-acl-ipv4(6)-RULE)# no apply		Disable the specified ACL rule.
Switch(config-acl-ipv4-RULE)# no destination-ipv4		Reset destination IPv4 address back to the default (ANY).
Switch(config-acl-ipv6-RULE)# no destination-ipv6		Reset destination IPv6 address back to the default (ANY).
Switch(config-acl-ipv4(6)-RULE)# no destination-l4-port		Reset destination Layer4 port back to the default (ANY).
Switch(config-acl-ipv4(6)-RULE)# no destination-mac		Reset destination MAC back to the default (ANY).
Switch(config-acl-ipv4(6)-RULE)# no ingress-port		Reset ingress port(s) back to the default (ANY).
Switch(config-acl-ipv4(6)-RULE)# no ethertype		Reset Ethertype back to the default (ANY).
Switch(config-acl-ipv4(6)-RULE)# no name		Remove the name from the specified ACL rule.
Switch(config-acl-ipv4(6)-RULE)# no protocol		Reset IPv4 protocol and IPv6 next header back to the default “ANY”.
Switch(config-acl-ipv4(6)-RULE)# no rate-limit		Disable rate limitation.
Switch(config-acl-ipv4(6)-RULE)# no sequence		Reset the sequence back to the default (100) for the specified ACL rule.
Switch(config-acl-ipv4-RULE)# no source-ipv4		Reset source IPv4 address back to the default (ANY).
Switch(config-acl-ipv6-RULE)# no source-ipv6		Reset source IPv6 address back to the default (ANY).
Switch(config-acl-ipv4(6)-RULE)# no source-l4-port		Reset source Layer4 port back to the default (ANY).
Switch(config-acl-ipv4(6)-RULE)# no source-mac		Reset source MAC back to the default (ANY).
Switch(config-acl-ipv4(6)-RULE)# no tos		Reset IPv4 TOS and IPv6 traffic class back to the default (ANY).
Switch(config-acl-ipv4(6)-RULE)# no vid		Reset packet classification 802.1q VLAN ID back to the default (ANY).
Show command		**Description**
Switch# show acl ipv4		Display all valid IPv4 ACL rules.
Switch# show acl ipv6		Display all valid IPv6 ACL rules.

Switch# show acl ipv4 [1-64]	[1-64]	Display the specified IPv4 ACL rule configuration.
Switch# show acl ipv6[1-32]	[1-32]	Display the specified IPv6 ACL rule configuration.
Switch# show acl ipv4 [index | sequence]	[index | sequence]	Display all valid IPv4 ACL rules sorted by specific option.
Switch# show acl ipv6 [index | sequence]	[index | sequence]	Display all valid IPv6 ACL rules sorted by specific option.
Switch(config)# show acl ipv4		Display all valid IPv4 ACL rules.
Switch(config)# show acl ipv6		Display all valid IPv6 ACL rules.
Switch(config)# show acl ipv4 [1-64]	[1-64]	Display the specified IPv4 ACL rule configuration.
Switch(config)# show acl ipv6 [1-32]	[1-32]	Display the specified IPv6 ACL rule configuration.
Switch(config)# show acl ipv4 [index | sequence]	[index | sequence]	Display all valid IPv4 ACL rules sorted by specific option.
Switch(config)# show acl ipv6 [index | sequence]	[index | sequence]	Display all valid IPv6 ACL rules sorted by specific option.
Switch(config-acl-ipv4(6)-RULE)# show		Display the specified ACL rule configuration.

2.6.5 Archive Command

Archive 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 | A:B:C:D:E:F:G:H] [file_directory] [user_name] [password]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the IPv4/IPv6 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 | A:B:C:D:E:F:G:H] [file_directory]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the IP/ IPv6 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.

2.6.6 Channel-group Command

1. Configure a static link aggregation group (LAG).

Channel-group Command	Parameter	Description
Switch(config)# channel-group trunking [group_name]	[group_name]	Specify a name for this link aggregation group. Up to 15 alphanumeric characters can be accepted.
Switch(config)# interface [port_list] Switch(config-if-PORT-PORT)# channel-group trunking [group_name]	[port_list] [group_name]	Use "interface" command to configure a group of ports' link aggregation link membership. Assign the selected ports to the specified link aggregation group.
Switch(config)# channel-group distribution-rule destination-ip		Load-balancing depending on destination IP address.
Switch(config)# channel-group distribution-rule destination-L4-port		Load-balancing depending on destination L4 port.
Switch(config)# channel-group distribution-rule destination-mac		Load-balancing depending on destination MAC address.
Switch(config)# channel-group distribution-rule source-ip		Load-balancing depending on source IP address.
Switch(config)# channel-group distribution-rule source-L4-port		Load-balancing depending on source L4 port.
Switch(config)# channel-group distribution-rule source-mac		Load-balancing depending on source MAC address.
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.
Switch(config)# no channel-group distribution-rule destination-ip		Disable load-balancing based on destination IP address.
Switch(config)# no channel-group distribution-rule destination-L4-port		Disable load-balancing based on destination L4 port.
Switch(config)# no channel-group type destination-mac		Disable load-balancing based on destination MAC address.

Switch(config)# no channel-group distribution-rule source-ip		Disable load-balancing based on source IP address.
Switch(config)# no channel-group distribution-rule source-L4-port		Disable load-balancing based on source L4 port.
Switch(config)# no channel-group type source-mac		Disable load-balancing based on source MAC address.
Show command		
Switch(config)# show channel-group trunking		Show link aggregation settings and distribution rule information.
Switch(config)# show channel-group trunking [trunk_name]	[trunk_name]	Show a specific link aggregation group's settings including aggregated port numbers and distribution rule information.

Below is an example of creating a static link aggregation group (port trunking group) using Channel-group commands to have the users realize the commands we mentioned above in this section.

	Command	Purpose
STEP1	**configure** **Example:** FOS-5152# config FOS-5152(config)#	**Enter the global configuration mode.**
STEP2 *(Optional)*	**channel-group distribution-rule source-ip** **Example:** FOS-5152(config)# channel-group distribution-rule source-ip OK !	**Enable Source IP Address in Distribution Rule.**
STEP3 *(Optional)*	**channel-group distribution-rule destination-ip** **Example:** FOS-5152(config)# channel-group distribution-rule destination-ip OK !	**Enable Destination IP Address in Distribution Rule.**
STEP4 *(Optional)*	**channel-group distribution-rule source-L4-port** **Example:** FOS-5152(config)# channel-group distribution-rule source-L4-port OK !	**Enable Source L4 Port in Distribution Rule.**
STEP5 *(Optional)*	**channel-group distribution-rule destination-L4-port** **Example:** FOS-5152(config)# channel-group distribution-rule destination-L4-port OK !	**Enable Destination L4 Port in Distribution Rule.**
STEP6 *(Optional)*	**channel-group distribution-rule source-mac** **Example:** FOS-5152(config)# channel-group distribution-rule source-mac OK !	**Enable Source Mac Address in Distribution Rule.**

STEP7 *(Optional)*	**channel-group distribution-rule destination-mac** **Example:** FOS-5152(config)# channel-group distribution-rule destination-mac OK !	**Enable Destination Mac Address in Distribution Rule.**
STEP8	**channel-group trunking** *group_name* **Example:** FOS-5152(config)# channel-group trunking CTSGROUP OK !	**In this example, it configures the name of the Trunking Group as "CTSGROUP".**
STEP9	**interface** *port_list* **Example:** FOS-5152(config)# interface 1,3 FOS-5152(config-if-1,3)#	**Speciy the interface that you would like to set to Trunking Group.**
STEP10	**channel-group trunking** *group_name* **Example:** FOS-5152(config-if-1,3)# channel-group trunking CTSGROUP OK !	**In this example, it configures Port 1 and Port 3 as the link membership of "CTSGROUP"Trunking Group**
STEP11	**exit** **Example:** FOS-5152(config-if-1,3)# exit FOS-5152(config)#	**Return to the global configuration mode.**
STEP12	**exit** **Example:** FOS-5152(config)# exit FOS-5152#	**Return to the Privileged mode.**
STEP13	**write** **Example:** FOS-5152# write Save Config Succeeded! OK !	**Save the running configuration into the startup configuration.**

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

Channel-group & Interface Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# channel-group lacp		Enable LACP on the selected interfaces.
Switch(config-if-PORT-PORT)# channel-group lacp key [0-255]	[0-255]	Specify a key to the selected interfaces. (0: auto)
Switch(config-if-PORT-PORT)# channel-group lacp role [active | passive]	[active | passive]	Specify the selected interfaces as active or passive 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 back to the default.
Switch(config-if-PORT-PORT)# no channel-group lacp role		Reset the LACP role type of the selected interfaces back to passive mode.
Show command		
Switch(config)# show channel-group lacp		Show each interface's LACP settings including current mode, key value and LACP role type.
Switch(config)# show channel-group lacp [port_list]	[port_list]	Show the selected interfaces' LACP settings.
Switch(config)# show channel-group lacp status		Show each interface's current LACP status.
Switch(config)# show channel-group lacp status [port_list]	[port_list]	Show the selected interfaces' current LACP status.
Switch(config)# show channel-group lacp statistics		Show each interface's current LACP traffic statistics.
Switch(config)# show channel-group lacp statistics [port_list]	[port_list]	Show the selected interfaces' current LACP traffic statistics.
Switch(config)# show channel-group lacp statistics clear		Clear all LACP statistics.

Below is an example of creating a dynamic link aggregation group using Channel-group commands to have the users realize the commands we mentioned above in this section.

	Command	Purpose
STEP1	**configure** **Example:** FOS-5152# config FOS-5152(config)#	**Enter the global configuration mode.**
STEP2 *(Optional)*	**channel-group distribution-rule source-ip** **Example:** FOS-5152(config)# channel-group distribution-rule source-ip OK !	**Enable Source IP Address in Distribution Rule.**
STEP3 *(Optional)*	**channel-group distribution-rule destination-ip** **Example:** FOS-5152(config)# channel-group distribution-rule destination-ip OK !	**Enable Destination IP Address in Distribution Rule.**
STEP4 *(Optional)*	**channel-group distribution-rule source-L4-port** **Example:** FOS-5152(config)# channel-group distribution-rule source-L4-port OK !	**Enable Source L4 Port in Distribution Rule.**
STEP5 *(Optional)*	**channel-group distribution-rule destination-L4-port** **Example:** FOS-5152(config)# channel-group distribution-rule destination-L4-port	**Enable Destination L4 Port in Distribution Rule.**

	OK !	
STEP6 *(Optional)*	**channel-group distribution-rule source-mac** **Example:** FOS-5152(config)# channel-group distribution-rule source-mac OK !	**Enable Source Mac Address in Distribution Rule.**
STEP7 *(Optional)*	**channel-group distribution-rule destination-mac** **Example:** FOS-5152(config)# channel-group distribution-rule destination-mac OK !	**Enable Destination Mac Address in Distribution Rule.**
STEP8	**interface** *port_list* **Example:** FOS-5152(config)# interface 5-7 FOS-5152(config-if-5-7)#	**Speciy the interfaces that you would like to set to LACP Group.**
STEP9	**channel-group lacp** **Example:** FOS-5152(config-if-5-7)# channel-group lacp OK !	**Enable Port 5~Port 7 to LACP Port.**
STEP10	**channel-group lacp role active** **[no channel-group lacp role]** **Example 1:** FOS-5152(config-if-5-7)# channel-group lacp role active OK ! **Example 2:** FOS-5152(config-if-5-7)# no channel-group lacp role OK !	**In the Example 1, it configures LACP Port 5~7 as "Active" in LACP Role.** **In the Example 2, it configures LACP Port 5~7 as "Passive" in LACP Role.**
STEP11	**channel-group lacp key** *LACP_key* **[no channel-group lacp key]** **Example 1:** FOS-5152(config-if-5-7)# channel-group lacp key 10 OK ! **Example 2:** FOS-5152(config-if-5-7)# no channel-group lacp key OK !	**In the Example 1, it configures a key value "10" as the LACP Key of LACP Port 5~7.** **In the Example 2, it configures a key value "0" (default value) as the LACP Key of LACP Port 5~7.**
STEP12	**exit** **Example:** FOS-5152(config-if-5-7)# exit FOS-5152(config)#	**Return to the global configuration mode.**
STEP13	**exit** **Example:** FOS-5152(config)# exit FOS-5152#	**Return to the Privileged mode.**

STEP14	**write** **Example:** FOS-5152# write Save Config Succeeded!	**Save the running configuration into the startup configuration.**

2.6.7 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 [port_list]	[port_list]	Show 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)# 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.

2.6.8 Digital Input Command

Digital Input Command	Parameter	Description
Switch(config)# digital input [1]	[1]	Specify the digital input number.
Switch(config-input-1)# normal [open | close]	[open | close]	Specify the normal digital input type between open and close status for the digital input 1.
No command		
Switch(config)# no digital input 1		Reset all digital input settings back to the default.
Switch(config-input-1)# no normal		Reset the normal digital input type back to the default. (Open)
Show command		**Description**
Switch# show digital input		Display the current digital input configuration.
Switch# show digital input status		Display the digital input status.
Switch(config)# show digital input		Display the current digital input configuration.
Switch(config)# show digital input status		Display the digital input status.
Switch(config-input-1)# show		Display the current normal status of the specified Digital Input.

2.6.9 Event Record Command

Event Record is designed to make it simpler for network administrators to trace the root cause of technical issues and to monitor the Managed Switch's status. When it's enabled, every occurred event will be fully preserved after the Managed Switch is rebooted, while every event will be removed after reboot if the function is disabled. In this sense, Event Record delivers greater control over log data management and allows for easy future troubleshooting.

Event Record Command	Parameter	Description
Switch(config)#event-record		Enable the Event Record function.
No Command		
Switch(config)# no event-record		Disable the Event Record function.
Show Command		**Description**
Switch(config)# show event-record		Show the Event Record function configuration.

2.6.10 Fast Redundancy Command

Besides RSTP and Ring Detection, the employment of CTS's proprietary 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.

CTS's 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 20 role head chain-port2 disable		Specify the 20th 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 16 role head chain-port2 interface 17 role member		Specify the 16th port of the Managed Switch as the 1st interface and the 17th 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 10 ring-port2 interface 11	Specify the 10th port as the 1st interface of the Fast Ring v2 protocol, and the 11th port as the 2nd interface.

2.6.11 IP Command

1. Set up an IP address of the Managed Switch or configure the Managed Switch to get an IP address automatically from DHCP server.

IP Command	Parameter	Description
Switch(config)# ip enable		Enable IPv4 address processing.
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 your Managed Switch.
	[255.X.X.X]	Enter subnet mask of your IP address.
	[A.B.C.D]	Enter the default gateway IP address.
Switch(config)# ip address dhcp		Enable DHCP mode.
No command		
Switch(config)# no ip enable		Disable IPv4 address processing.
Switch(config)# no ip address		Reset the Managed Switch's IP address back to the default.(192.168.0.1)
Switch(config)# no ip address dhcp		Disable DHCP mode.
Show command		
Switch(config)# show ip address		Show the IP configuration and the current status of the system.
IP command Example		
Switch(config)# ip address 192.168.1.198 255.255.255.0 192.168.1.254		Set up the Managed Switch's IP to 192.168.1.198, subnet mask to 255.255.255.0, and default gateway IP address to 192.168.1.254.
Switch(config)# ip address dhcp		The Managed Switch will obtain an IP address automatically.

2. Enable IPv4 DHCP Auto Recycle function.

IP Auto Recycle Command	Parameter	Description
Switch(config)# ip address dhcp auto-recycle		Enable IPv4 DHCP Auto Recycle function globally.
No command		
Switch(config)# no ip address dhcp auto-recycle		Disable IPv4 DHCP Auto Recycle function globally.

3. Use "Interface" command to configure IPv4 DHCP Auto Recycle function.

IP Auto Recycle & Interface Command	Parameter	Description
Switch(config)# interface [port_list]		Enter several discontinuous port numbers separated by commas or a

		range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# ip address dhcp auto-recycle		Enable IPv4 DHCP Auto Recycle function on the specified ports. Only when one of these specific link-up ports is switched from link-down into link-up status, DHCP release packets and Discover packets will be sent to DHCP server automatically. And it will ask for IP address from DHCP server again.
No command		
Switch(config-if-PORT-PORT)# no ip address dhcp auto-recycle		Disable IPv4 DHCP Auto Recycle function on the specified ports.

4. Enable DHCPv4/DHCPv6 relay function.

DHCP Snooping Command	Parameter	Description
Switch(config)# ip dhcp snooping		Enable DHCPv4/DHCPv6 snooping function.
Switch(config)# ip dhcp snooping dhcp-server-ip		Globally enable DHCPv4/DHCPv6 server trust IPv4/IPv6 address.
Switch(config)# ip dhcp snooping dhcp-server-ip [1-4] ip-address [A.B.C.D | A:B:C:D:E:F:G:H]	[1-4]	Specify DHCPv4/DHCPv6 server trust IPv4/IPv6 address number.
	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify DHCPv4/ DHCPv6 server trust IPv4/IPv6 address.
Switch(config)# ip dhcp snooping initiated [0-9999]	[0-9999]	Specify the DHCPv4/DHCPv6 snooping Initiated Time value (0~9999 seconds) that packets might be received.
Switch(config)# ip dhcp snooping leased [180-259200]	[180-259200]	Specify the DHCPv4/DHCPv6 snooping Leased Time for DHCP clients. (Range:180~259200 seconds).
Switch(config)# ip dhcp snooping link-down-clear		Enable DHCPv4/DHCPv6 snooping entry clear function to delete the recorded entries of DHCPv4/DHCPv6 clients once the link of the learning port is down.
Switch(config)# ip dhcp snooping option		Globally enable DHCPv4 Option 82 / DHCPv6 Option 37 relay agent.
Switch(config)# ip dhcp snooping remote		Globally enable DHCPv4 Option 82 / DHCPv6 Option 37 Manual Remote Id.
Switch(config)# ip dhcp snooping remote formatted		Enable the Formatted DHCPv4 Option 82 / DHCPv6 Option 37 Remote Id.
Switch(config)# ip dhcp snooping remote id [remote_id]	[remote_id]	You can configure the DHCPv4 Option 82 / DHCPv6 Option 37 remote ID to be a string of up to 63 characters. The default remote ID is the switch's MAC address.
No command		
Switch(config)# no ip dhcp snooping		Disable DHCPv4/DHCPv6 snooping function.

Switch(config)# no ip dhcp snooping dhcp-server-ip		Globally disable DHCPv4/DHCPv6 server trust IPv4/IPv6 address.
Switch(config)# no ip dhcp snooping dhcp-server-ip [1-4] ip-address		Remove DHCPv4/DHCPv6 server trust IPv4/IPv6 address from the specified trust IPv4/IPv6 address number.
Switch(config)# no ip dhcp snooping initiated		Reset the initiated time value back to the default. (4 seconds)
Switch(config)# no ip dhcp snooping leased		Reset the leased time value back to the default.(86400 seconds)
Switch(config)# no ip dhcp snooping link-down-clear		Disable the DHCPv4/DHCPv6 snooping entry clear function.
Switch(config)# no ip dhcp snooping option		Disable DHCPv4 Option 82 / DHCPv6 Option 37 relay agent.
Switch(config)# no ip dhcp snooping remote		Globally disable DHCPv4 Option 82 / DHCPv6 Option 37 Manual Remote Id.
Switch(config)# no ip dhcp snooping remote formatted		Disable the Formatted DHCPv4 Option 82 / DHCPv6 Option 37 Remote Id.
Switch(config)# no ip dhcp snooping remote id		Clear Remote ID description.
Show command		
Switch(config)# show ip dhcp snooping		Show DHCPv4/DHCPv6 snooping configuration.
Switch(config)# show ip dhcp snooping clear [port_list]	[port_list]	Clear the DHCPv4/DHCPv6 snooping entry learned from the specified port.
Switch(config)# show ip dhcp snooping interface		Show each port's DHCP Snooping Option 82/Option 37 and trust port settings.
Switch(config)# show ip dhcp snooping interface [port_list]	[port_list]	Show the specified port's DHCP Snooping Option 82/Option 37 and trust port settings.
Switch(config)# show ip dhcp snooping opt82 circuit		Show each port's DHCP snooping opt82 Circuit ID.
Switch(config)# show ip dhcp snooping opt82 circuit [port_list]	[port_list]	Show the specified port's DHCP snooping opt82 Circuit ID.
Switch(config)# show ip dhcp snooping opt82 remote		Show DHCP snooping opt82 Remote ID.
Switch(config)# show ip dhcp snooping status		Show DHCPv4/DHCPv6 snooping current status.
Examples of IP DHCP Snooping		
Switch(config)# ip dhcp snooping		Enable DHCP snooping function.
Switch(config)# ip dhcp snooping initiated 10		Specify the time value that packets might be received to 10 seconds.
Switch(config)# ip dhcp snooping leased 240		Specify packets' expired time to 240 seconds.
Switch(config)# ip dhcp snooping link-down-clear		Enable the DHCPv4/DHCPv6 snooping entry clear function.
Switch(config)# ip dhcp snooping option		Enable DHCP Option 82 Relay Agent.
Switch(config)# ip dhcp snooping remote id 123		The remote ID is configured as "123".

5. Use "Interface" command to configure a group of ports' DHCP Snooping settings.

DHCP Snooping & Interface Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# ip dhcp snooping circuit		Enable the selected interfaces' DHCPv4 Option 82 / DHCPv6 Option 37 Manual Circuit Id.
Switch(config-if-PORT-PORT)# ip dhcp snooping circuit formatted		Enable the Formatted DHCPv4 Option 82 / DHCPv6 Option 37 Circuit Id for the selected interfaces.
Switch(config-if-PORT-PORT)# ip dhcp snooping circuit id [circuit_id]	[circuit_id]	Specify the VLAN and port identifier using a VLAN ID in the range of 1 to 4094 as DHCPv4 Option 82 / DHCPv6 Option 37 Circuit ID. Besides, you can configure the circuit ID to be a string of up to 63 characters. The default circuit ID is the port identifier, the format of which is **vlan-mod-port**.
Switch(config-if-PORT-PORT)# ip dhcp snooping option		Enable the selected interfaces' DHCPv4 Option 82 / DHCPv6 Option 37 relay agent.
Switch(config-if-PORT-PORT)# ip dhcp snooping trust		Enable the selected interfaces as DHCPv4 Option 82 / DHCPv6 Option 37 trust ports.
Switch(config-if-PORT-PORT)# ip dhcp snooping server-trust		Enable the selected interfaces as DHCPv4/DHCPv6 server trust ports. **Note: A port / ports cannot be configured as option 82/option 37 trust and server trust at the same time.**
No command		
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit		Disable the selected interfaces' DHCPv4 Option 82 / DHCPv6 Option 37 Manual Circuit Id.
Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit formatted		Disable the Formatted DHCPv4 Option 82 / DHCPv6 Option 37 Circuit Id for the selected interfaces.
Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit id		Clear DHCPv4 Option 82 / DHCPv6 Option 37 Circuit Id.
Switch(config-if-PORT-PORT)# no ip dhcp snooping option		Disable the selected interfaces' DHCPv4 Option 82 / DHCPv6 Option 37 relay agent.
Switch(config-if-PORT-PORT)# no ip dhcp snooping trust		Reset the selected interfaces back to non-DHCPv4 Option 82 / DHCPv6 Option 37 trust ports.
Switch(config-if-PORT-PORT)# no ip dhcp snooping server-trust		Reset the selected interfaces back to non-DHCPv4/DHCPv6 server trust ports.
Examples of DHCP Snooping & Interface		
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)# ip dhcp snooping option	Enable DHCPv4 Option 82 / DHCPv6 Option 37 relay agent for Port 1~3.
Switch(config-if-1-3)# ip dhcp snooping trust	Configure Port 1~3 as DHCPv4 Option 82 / DHCPv6 Option 37 trust ports.

6. Enable or disable IGMP/MLD snooping globally.

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

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

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

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

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

IGMP/MLD Snooping Command	Parameter	Description
Switch(config)# ip igmp snooping		Enable IGMP/MLD snooping. When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic. This is for IGMPv1, v2 and MLDv1 only.
Switch(config)# ip igmp snooping version-3		Enable IGMPv3/MLDv2 snooping. When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic. This is for IGMPv3 and MLDv2 only.
Switch(config)# ip igmp snooping flooding		Enable Unregistered IPMC Flooding function. Set forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic will flood when enabled. However, the traffic will be forwarded to router-ports only when disabled.
Switch(config)# ip igmp snooping immediate-leave		Enable immediate leave function.

Switch(config)# ip igmp snooping stream-life-time		Enable IGMP/MLD snooping stream life time function. The multicast packet stream will be stopped once reaching the end of its specified lifespan. **Note:** **The length of stream life time is determined by the total amount of the specified query-interval and max-response-time (125 and 10 seconds in default, respectively).**
Switch(config)# ip igmp snooping max-response-time [1-255]	[1-255] (Unit:1/10secs)	Specify the IGMP/MLD querier maximum response time. This determines the maximum amount of time can be allowed before sending an IGMP/MLD response report.
Switch(config)# ip igmp snooping query-interval [1-6000]	[1-6000]	Specify the query time interval of IGMP/MLD querier. This is used to set up the time interval between transmitting IGMP/MLD queries. (Range:1-6000 seconds)
Switch(config)# ip igmp snooping vlan [1-4094]	[1-4094]	Specify a VLAN ID. This enables IGMP/MLD Snooping for the specified VLAN.
Switch(config)# ip igmp snooping vlan [1-4094] query	[1-4094]	Enable a querier for the specified VLAN.
No Command		
Switch(config)# no ip igmp snooping		Disable IGMP/MLD snooping function.
Switch(config)# no ip igmp snooping flooding		Disable Unregistered IPMC Flooding function. The traffic will be forwarded to router-ports only when disabled.
Switch(config)# no ip igmp snooping immediate-leave		Disable immediate leave function.
Switch(config)# no ip igmp snooping stream-life-time		Disable IGMP/MLD snooping stream life time function.
Switch(config)# no ip igmp snooping max-response-time		Reset the IGMP/MLD querier maximum response time back to the default.
Switch(config)# no ip igmp snooping query-interval		Reset the query time interval value back to the default. (100 seconds)
Switch(config)# no ip igmp snooping version-3		Disable IGMPv3/MLDv2 snooping.
Switch(config)# no ip igmp snooping vlan [1-4094]	[1-4094]	Disable IGMP/MLD snooping for the specified VLAN.
Switch(config)# no ip igmp snooping vlan [1-4094] query	[1-4094]	Disable a querier for the specified VLAN.
Show Command		
Switch(config)# show ip igmp snooping		Show the current IGMP/MLD snooping configuration. **Note 1: VLAN ID marked * stands that it is a MVR VLAN ID.**

		Note 2: If the VLAN name belongs to an "Enabled" multicast VLAN ID, it will be automatically changed into the one same as MVR name configured by MVR command. (See Section 2.6.17)
Switch(config)# show ip igmp snooping groups		Show IGMP snooping groups table. **Note: VID marked * stands that it is a MVR VLAN ID.**
Switch(config)# show ip igmp snooping status		Show IGMP Snooping status. **Note: VID marked * stands that it is a MVR VLAN ID.**
Switch(config)# show ip mld snooping groups		Show MLD snooping groups table. **Note: VID marked * stands that it is a MVR VLAN ID.**
Switch(config)# show ip mld snooping status		Show MLD Snooping status. **Note: VID marked * stands that it is a MVR VLAN ID.**

7. Use "Interface" command to configure a group of ports' IGMP/MLD snooping settings.

IGMP/MLD Snooping & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# ip igmp snooping mcast-router		Specify the selected port(s) as the multicast router port.
No command		
Switch(config-if-PORT-PORT)# no ip igmp snooping mcast-router		Remove the selected port(s) from the multicast router port list.
Examples of IP DHCP Snooping & Interface		
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)# ip dhcp snooping option		Configure Port 1~3 as the multicast router port.
Switch(config-if-1-3)# no ip igmp snooping mcast-router		Remove Port 1~3 from the multicast router port list.

8. Configure IGMP filtering policies.

IGMP Filtering Command	Parameter	Description
Switch(config)# ip igmp filter		Globally enable IGMP filtering function.

Switch(config)# ip igmp profile [profile_name]	[profile_name]	Create or modify a profile for IGMP filter. The maximum length of profile name is 20 characters. Up to 60 profiles can be created.
Switch(config-profile-ID)# segment [1-400]	[1-400]	Specify an existing segment ID to the selected profile.
Switch(config)# ip igmp segment [1-400]	[1-400]	Create or modify a segment ID for IGMP filter.
Switch(config-segment-ID)# name [segment_name]	[segment_name]	Specify a name for the selected segment ID. The maximum is 20 characters.
Switch(config-segment-ID)# range [E.F.G.H] [E.F.G.H]	[E.F.G.H] [E.F.G.H]	Specify Low IP multicast address and High IP multicast address for the selected segment ID.
No command		
Switch(config)# no ip igmp filter		Disable IGMP filtering function.
Switch(config)# no ip igmp profile [profile_name]	[profile_name]	Delete the specified profile.
Switch(config)# no ip igmp segment [1-400]	[1-400]	Delete the specified segment ID. Only the segment that does not belong to any profiles can be deleted.
Switch(config-profile-ID)# no segment		Remove all existing segment IDs from the selected profile.
Switch(config-profile-ID)# no segment [1-400]	[1-400]	Remove the specified segment ID(s) from the selected profile.
Switch(config-segment-ID)# no name		Reset a name of the selected segment ID back to the default.
Switch(config-segment-ID)# no range		Reset a multicast IP range of the selected segment ID back to the default.
Show command		
Switch(config)# show ip igmp filter		Show IGMP filter configuration.
Switch(config)# show ip igmp filter interface		Show all ports' IGMP filtering configuration.
Switch(config)# show ip igmp filter interface [port_list]	[port_list]	Show the specified ports' IGMP filtering configuration.
Switch(config)# show ip igmp profile		Show the profile configuration of IGMP filter.
Switch(config)# show ip igmp profile [profile_name]	[profile_name]	Show the specified profile's configuration.
Switch(config)# show ip igmp segment		Show the segment configuration of IGMP filter.
Switch(config)# show ip igmp segment [1-400]	[1-400]	Show the specified segment's configuration.
Switch(config-segment-ID)# show		Show the selected segment's configuration.
Switch(config-profile-ID)# show		Show the selected profile's configuration.
Examples of IGMP Filtering Command		
Switch(config)# ip igmp filter		Enable IGMP filtering function.
Switch(config)# ip igmp segment 50		Create a segment "50".
Switch(config-segment-50)# name Silver		Specify a name "Silver" for this segment 50.

Switch(config-segment-50)# range 224.10.0.2 229.10.0.1	Specify a multicast IP range 224.10.0.2 to 229.10.0.1 to segment 50.
Switch(config)# ip igmp profile Silverprofile	Create or modify a profile named “Silverprofile”.
Switch(config-profile-Silverprofile)# segment 50	Assign the segment 50 to the “Silverprofile” profile.

9. Use “Interface” command to configure a group of ports’ IGMP filtering function.

IGMP Filtering & Interface Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# ip igmp filter		Enable IGMP filter for the selected ports.
Switch(config-if-PORT-PORT)# ip igmp filter profile [profile_name]	[profile_name]	Assign the selected ports to an IGMP filter profile. **Note: Need to create an IGMP filter profile first under the igmp global configuration mode before assigning it.**
Switch(config-if-PORT-PORT)# ip igmp filter max-groups [1-512]	[1-512]	Specify the maximum groups number of multicast streams to the selected ports.
Switch(config-if-PORT)# ip igmp static-multicast-ip [E.F.G.H | E:F:G:H:I:J:K:L] vlan [1-4094]	[E.F.G.H | E:F:G:H:I:J:K:L]	Create/specify a static multicast IP and the specified VLAN entry to the selected port. **Note: Only one port could be assigned at a time.**
	[1-4094]	Specify a VLAN ID.
No command		
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# no ip igmp filter		Disable IGMP filter for the selected ports.
Switch(config-if-PORT-PORT)# no ip igmp filter profile [profile_name]	[profile_name]	Remove the specified profile from the selected ports.
Switch(config-if-PORT-PORT)# no ip igmp max-groups		Reset the maximum number of multicast streams back to the default (512 channels).
Switch(config-if-PORT)# no ip igmp static-multicast-ip [E.F.G.H | E:F:G:H:I:J:K:L] vlan [1-4094]	[E.F.G.H | E:F:G:H:I:J:K:L]	Remove the specific static multicast IP. **Note: Only one port could be assigned at a time.**

	[1-4094]	Remvoe the specified VLAN ID.
Show command		
Switch(config)# show ip igmp static-multicast-ip		Show the static multicast IP table.
Examples of IGMP Filtering & Interface		
Switch(config)# interface1		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)# ip igmp filter		Enable IGMP Filter on port 1.
Switch(config-if-1)# ip igmp filter profile Silverprofile		Assign the selected port to the specified profile “Silverprofile”.
Switch(config-if-1)# ip igmp filter max-groups 400		Set the maximum number of multicast streams to 400.
Switch(config-if-1)# ip igmp static-multicast-ip 224.10.0.5 vlan 50		Create a static multicast IP to VLAN entry.

10. Set Up IP Source Binding Function.

IP Source Binding Command	Parameter	Description
Switch(config)# ip source binding [1-5] ip-address [A.B.C.D | A:B:C:D:E:F:G:H]	[1-5]	Specify the IPv4/IPv6 address security binding number.
	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify IPv4/IPv6 address.
Switch(config)# ip source binding [1-5]	[1-5]	Enable IPv4/IPv6 address security binding for the specified number.
Switch(config)# ip source		Globally enable IPv4/IPv6 address security binding.
No Command		
Switch(config)# no ip source		Globally disable IPv4/IPv6 address security binding.
Switch(config)# no ip source binding [1-5]	[1-5]	Disable IPv4/IPv6 address security binding for the specified number.
Switch(config)# no ip source binding [1-5] ip-address		Remove the IPv4/IPv6 address of the specified number from the IP Source Binding list.
Show command		
Switch(config)# show ip source		Show IPv4/IPv6 Source configuration.

11. Use “Interface” command to configure IP Source Guard for Security.

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

Switch(config-if-PORT-PORT)# ip sourceguard [dhcp | fixed-ip]	[dhcp | fixed-ip]	Specify the authorized access type for the selected ports. **dhcp:** DHCP server assigns IP address. **fixed IP:** Only Static IP (Create Static IP table first). **unlimited:** Non-Limited (Allows both static IP and DHCP-assigned IP). This is the default setting.
Switch(config-if-PORT)# ip sourceguard static-ip [A.B.C.D | A:B:C:D:E:F:G:H] vlan [1-4094]	[A.B.C.D | A:B:C:D:E:F:G:H]	Add a static IPv4/IPv6 address to static IP address table. **Note: Only one port could be assigned at a time.**
	[1-4094]	Specify a VLAN ID. **Note: Static IP can only be configured when IP sourceguard is set to fixed-ip.**
No command		
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# no ip sourceguard		Reset IP sourceguard type setting of the selected ports back to the default (unlimited).
Switch(config-if- PORT)# no ip sourceguard static-ip [A.B.C.D | A:B:C:D:E:F:G:H] vlan [1-4094]	[A.B.C.D | A:B:C:D:E:F:G:H]	Remove the specified IPv4/IPv6 address. **Note: Only one port could be assigned at a time.**
	[1-4094]	Remvoe the specified VLAN ID.
Show command		
Switch# show ip sourceguard interface		Show each interface's IP sourceguard type.
Switch# show ip sourceguard interface [port_list]	[port_list]	Show the specified interface's IP sourceguard type.
Switch# show ip sourceguard static-ip		Show IP souceguard static IP table.
Switch(config)# show ip sourceguard interface		Show each interface's IP sourceguard type.
Switch(config)# show ip sourceguard interface [port_list]	[port_list]	Show the specified interface's IP sourceguard type.
Switch(config)# show ip sourceguard static-ip		Show IP souceguard static IP table.
Examples of IP Source Guard & Interface		
Switch(config)# interface1		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)# ip sourceguard fixed-ip	Set the authorized access type for the selected ports as fixed-ip.
Switch(config-if-1)# ip sourceguard static-ip 192.168.0.100 vlan 20	Create a static IP 192.168.0.100 to VLAN entry 20.

2.6.12 IPv6 Command

Brief Introduction to IPv6 Addressing

IPv6 addresses are 128 bits long and number about 3.4×1038. IPv6 addresses are written in eight groups of four hexadecimal digits separated by colons, such as

2001:0db8:85a3:0000:0000:8a2e:0370:7334

IPv6 unicast addresses other than those that start with binary 000 are logically divided into two parts: a 64-bit network prefix and a 64-bit interface identifier.

Stateless Autoconfiguration

IPv6 lets any host generate its own IP address and check if it's unique in the scope where it will be used. IPv6 addresses consist of two parts. The leftmost 64 bits are the subnet prefix to which the host is connected, and the rightmost 64 bits are the identifier of the host's interface on the subnet. This means that the identifier need only be unique on the subnet to which the host is connected, which makes it much easier for the host to check for uniqueness on its own.

Autoconfigured address format

part	*Subnet prefix*	*Interface identifier*
bits	64	64

Link local address

The first step a host takes on startup or initialization is to form a link-local address from its MAC address and the link-local prefix FE80::/10. This is done by putting the prefix into the leftmost bits and the MAC address (in EUI-64 format) into the rightmost bits, and if there are any bits left in between, those are set to zero.

Global address

This is done in the same fashion as the link-local address, but instead of the link-local prefix FE80:: it will use the prefix supplied by the router and put it together with its identifier (which by default is the MAC address in EUI-64 format).

Some IPv6 addresses are reserved for special purposes, such as loopback, 6to4 tunneling, and Teredo tunneling, as outlined in RFC 5156. Also, some address ranges are considered special, such as link-local addresses for use on the local link only, Unique Local addresses (ULA), as described in RFC 4193, and solicited-node multicast addresses used in the Neighbor Discovery Protocol.

DHCPv6

IPv6 hosts may automatically generate IP addresses internally using stateless address autoconfiguration, or they may be assigned configuration data with DHCPv6.

Set up the IPv6 address of the Managed Switch or configure the Managed Switch to get an IP address automatically from DHCPv6 server.

IPv6 Command	Parameter	Description
Switch(config)# ipv6 address autoconfig		Configuration of IPv6 addresses using stateless autoconfiguration.
Switch(config)# ipv6 address dhcp auto		Configure DHCPv6 function into the auto mode.
Switch(config)# ipv6 address dhcp force		Configure DHCPv6 function into the forced mode.
Switch(config)# ipv6 address dhcp rapid-commit		Allow the two-message exchange for address assignment.
“ipv6 address dhcp” commands are functional only when autoconfiguration is enabled.		
Switch(config)# ipv6 address global [A:B:C:D:E:F:G:H/10~128] [A:B:C:D:E:F:G:H]	[A:B:C:D:E:F:G:H/10~128]	Specify IPv6 global address and prefix-length of the Managed Switch.
	[A:B:C:D:E:F:G:H]	Specify IPv6 default gateway IP address of the Managed Switch.
Switch(config)# ipv6 address link-local [A:B:C:D:E:F:G:H/10~128]	[A:B:C:D:E:F:G:H/10~128]	Specify IPv6 link-local address and prefix-length of the Managed Switch.
Switch(config)# ipv6 enable		Enable IPv6 address processing.
No command		
Switch(config)# no ipv6 address autoconfig		Disable IPv6 stateless autoconfig.
Switch(config)# no ipv6 address dhcp		Disable DHCPv6 function.
Switch(config)# no ipv6 address dhcp rapid-commit		Disable rapid-commit feature.
Switch(config)# no ipv6 address global		Clear IPv6 global address entry.
Switch(config)# no ipv6 address link-local		Clear IPv6 link-local address entry.
Switch(config)# no ipv6 enable		Disable IPv6 address processing.
Show command		
Switch# show ipv6 address		Display IPv6 configuraiton and the current IPv6 status of the Managed Switch.
Switch(config)# show ipv6 address		Display IPv6 configuraiton and the current IPv6 status of the Managed Switch.
Examples of IPv6 command		
Switch(config)# ipv6 address autoconfig		Enable IPv6 autoconfiguration.
Switch(config)# ipv6 address dhcp auto		Enable DHCPv6 auto mode.

2.6.13 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 contain type, length and value descriptions, and are referred to as TLVs. Details such as port description, system name, system description, system capabilities, and management address can be sent and received on this Managed Switch.

LLDP Command	Parameter	Description
Switch(config)# lldp		Enable LLDP function.
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 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 packets.
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		Disable LLDP function.
Switch(config)# no lldp hold-time		Reset the hold-time value back to the default. (120 seconds)
Switch(config)# no lldp interval		Reset the time interval value of sending updated LLDP packets back to the default.(5 seconds)
Switch(config)# no lldp packets		Reset the amount of packets that are sent in each discover back to the default.(1 packet)
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		Disable System Description attribute to be sent.

system-description	
Switch(config)# no lldp tlv-select system-name	Disable System Name attribute to be sent.
Show command	
Switch# show lldp	Show LLDP settings.
Switch# show lldp interface	Show each interface's LLDP configuraiton.
Switch# show lldp interface [port_list]	Show the selected interfaces' LLDP configuration.
Switch# show lldp status	Show the current LLDP status.
Switch(config)# show lldp	Show LLDP settings.
Switch(config)# show lldp interface	Show each interface's LLDP configuraiton.
Switch(config)# show lldp interface [port_list]	Show the selected interfaces' LLDP configuration.
Switch(config)# show lldp status	Show the current LLDP status.
Examples of LLDP command	**Description**
Switch(config)# lldp hold-time 60	Set the hold-time 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.

2.6.14 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 actions:

1. It blocks the relevant port to prevent broadcast storms, and send out SNMP trap to inform the network administrator. In other words, the system stops forwarding all the traffic via the looped port. However, the system will process the Loop Detection, RSTP and LLDP packets 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 receive 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.*

Loop Detection Command	Parameter	Description
Switch(config)# loop-detection		Enable Loop Detection function.
Switch(config)# loop-detection all-vlan		Enable loop detection on all trunk-VLAN-vids configured in VLAN Command (See Section 2.6.28). **NOTE: When this command is issued, it will invalidate the "Specific VLAN"settings of loop detection.**
Switch(config)# loop-detection interval [1-20]	[1-20]	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 20 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]	Enable loop detection on specified VLAN. Up to 4 sets of VLAN ID can be assigned. **NOTE: The configured "Specific VLAN" takes effect when the setting of loop detection on all trunk-VLAN-vids is disabled.**
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-vids.
Switch(config)# no loop-detection interval		Reset Loop Detection time interval back to the default.
Switch(config)# no loop-detection unlock-interval		Reset Loop Detection unlock time interval back to the default.
Switch(config)# no loop-detection vlan-id [1-4094]	[1-4094]	Disable loop detection on a specified VLAN.
Show command		
Switch# show loop-detection		Show Loop Detection configuration.
Switch# show loop-detection status		Show Loop Detection status of all ports.
Switch# show loop-detection status [port_list]	[port_list]	Show Loop Detection status of the specified port(s).
Switch(config)# show loop-detection		Show Loop Detection configuration.
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 specified port(s).
Examples of Loop Detection command		
Switch(config)# loop-detection interval 10		Set the Loop Detection time interval to 10 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		Enable the Loop Detection on VLAN ID 100.

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

Loop Detection & 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 selected port(s).
Switch(config-if-PORT-PORT)# loop-detection unlock		Unlock the selected port(s) that are locked.
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 selected port(s).

2.6.15 l2protocol-tunnel Command

L2PT (Layer 2 protocol tunneling) allows Layer 2 protocol data units (PDUs), including CDP(Cisco Discovery Protocol), LLDP(Link Layer Discovery Protocol), STP(Spanning Tree Protocol), VTP(Vlan Trunking Protocol), LACP(Link Aggregation Control Protocol), PAgP(Port Aggregation Protocol), UDLD(Unidirectional Link Detection), to be tunneled through a network.

GBPT, also referred to as Generic Bridge PDU Tunneling, provides a scalable approach to PDU tunneling by software encapsulating the PDUs in the ingress edge switches and then multicasting them in hardware. All switches inside the service provider network treat these encapsulated frames as data packets and forward them to the other end. The egress edge switch listens for these special encapsulated frames and decapsulates them; they are then forwarded out of the tunnel.

The encapsulation involves the rewriting of the destination media access control (MAC) address in the PDU. An ingress edge switch rewrites the destination MAC address of the PDUs received on a Layer 2 tunnel port with the desired multicast address.

L2PT Command	Parameter	Description
Switch(config)# l2protocol-tunnel		Enable Layer 2 protocol tunneling (L2PT) function on the Managed Switch.
Switch(config)# l2protocol-tunnel cos [0-7]	[0-7]	Specify the priority bit value as L2PT Class of Service (CoS).
Switch(config)# l2protocol-tunnel mac [xx:xx:xx:xx:xx:xx]	[xx:xx:xx:xx:xx:xx]	Specify the destination MAC address for encapsulating layer 2 protocol packets.
No command		
Switch(config)# no l2protocol-tunnel		Disable Layer 2 protocol tunneling function on the Managed Switch.
Switch(config)# no l2protocol-tunnel cos		Reset the priority bit value for L2PT class of service (cos) back to the default (5).
Switch(config)# no l2protocol-tunnel mac		Reset the destination MAC address for encapsulating Layer 2 protocol packets back to the default (01:00:0C:CD:CD:D0).
Show command		
Switch(config)# show l2protocol-tunnel		Show the current Layer 2 Protocol Tunneling configuration, the state of PDUs and each PDU's encapsulation as well as decapsulation counters for all ports.
Switch(config)# show l2protocol-tunnel [port_list]	[port_list]	Show the current Layer 2 Protocol Tunneling configuration, the state of PDUs and each PDU's encapsulation as well as decapsulation counters for the specified port.
Switch(config)# show l2protocol-tunnel [port_list] clear	[port_list]	Clear each PDU's encapsulation and decapsulation counters of the specified port.
Switch(config)# show l2protocol-tunnel clear		Clear each PDU's encapsulation and decapsulation counters of all ports.
Examples of L2PT command		
Switch(config)# l2protocol-tunnel		Enable L2PT function.
Switch(config)# l2protocol-tunnel cos 3		Specify the priority bit value "3" to L2PT Class of Service (CoS).

Use "Interface" command to configure Layer 2 protocol data units (PDUs) settings.

L2PT & 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)# l2protocol-tunnel		Enable layer 2 protocol tunneling for CDP, LLDP, STP and VTP packets on the selected port(s).
Switch(config-if-PORT-PORT)# l2protocol-tunnel cdp		Enable layer 2 protocol tunneling for CDP packets on the selected port(s).

Switch(config-if-PORT-PORT)# l2protocol-tunnel lldp		Enable layer 2 protocol tunneling for LLDP packets on the selected port(s).
Switch(config-if-PORT-PORT)# l2protocol-tunnel point-to-point		Enable point-to-point layer 2 protocol tunneling for LACP, PAgP and UDLD packets on the selected port(s).
Switch(config-if-PORT-PORT)# l2protocol-tunnel point-to-point lacp		Enable point-to-point layer 2 protocol tunneling for LACP packets on the selected port(s).
Switch(config-if-PORT-PORT)# l2protocol-tunnel point-to-point pagp		Enable point-to-point layer 2 protocol tunneling for PAgP packets on the selected port(s).
Switch(config-if-PORT-PORT)# l2protocol-tunnel point-to-point udld		Enable point-to-point layer 2 protocol tunneling for UDLD packets on the selected port(s).
Switch(config-if-PORT-PORT)# l2protocol-tunnel stp		Enable layer 2 protocol tunneling for STP packets on the selected port(s).
Switch(config-if-PORT-PORT)# l2protocol-tunnel vtp		Enable layer 2 protocol tunneling for VTP packets on the selected port(s).
No command		
Switch(config-if-PORT-PORT)# no l2protocol-tunnel		Disable layer 2 protocol tunneling for CDP, LLDP, STP and VTP packets on the selected port(s).
Switch(config-if-PORT-PORT)# no l2protocol-tunnel cdp		Disable layer 2 protocol tunneling for CDP packets on the selected port(s).
Switch(config-if-PORT-PORT)# no l2protocol-tunnel lldp		Disable layer 2 protocol tunneling for LLDP packets on the selected port(s).
Switch(config-if-PORT-PORT)# no l2protocol-tunnel point-to-point		Disable point-to-point layer 2 protocol tunneling for LACP, PAgP and UDLD packets on the selected port(s).
Switch(config-if-PORT-PORT)# no l2protocol-tunnel point-to-point lacp		Disable point-to-point layer 2 protocol tunneling for LACP packets on the selected port(s).
Switch(config-if-PORT-PORT)# no l2protocol-tunnel point-to-point pagp		Disable point-to-point layer 2 protocol tunneling for PAgP packets on the selected port(s).
Switch(config-if-PORT-PORT)# no l2protocol-tunnel point-to-point udld		Disable point-to-point layer 2 protocol tunneling for UDLD packets on the selected port(s).
Switch(config-if-PORT-PORT)# no l2protocol-tunnel stp		Disable layer 2 protocol tunneling for STP packets on the selected port(s).
Switch(config-if-PORT-PORT)# no l2protocol-tunnel vtp		Disable layer 2 protocol tunneling for VTP packets on the selected port(s).

2.6.16 MAC Command

Set up 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 aging time.

MAC Command	Parameter	Description
Switch(config)# mac address-table aging-time [0-900s]	[0-900s]	Specify MAC address table aging time between 0 and 900 seconds. “0” means that MAC addresses will never age out.
No command		

Switch(config)# no mac address-table aging-time		Reset MAC address table aging time back to the default. (300 seconds).
Show command		
Switch(config)# show mac address-table all		Show all of MAC table information.
Switch(config)# show mac address-table all [mac | vid | port]	[mac | vid | port]	Show all learned MAC addresses sorted by specific option.
Switch(config)# show mac address-table clear		Clear MAC address table.
Switch(config)# show mac address-table clear [port_list]	[port_list]	Clear MAC addresses learned by the specified port.
Switch(config)# show mac address-table count		Show the statistics of MAC address table.
Switch(config)# show mac address-table interface [port_list] [mac | vid | port]	[port_list]	Show the MAC addresses learned by the specified port.
	[mac | vid | port]	Show the learned MAC addresses sorted by specific option.
Switch(config)# show mac address-table mac [xx:xx:xx | xx:xx:xx:xx:xx:xx] [mac | vid | port]	[xx:xx:xx]	Show the MAC address that its first 3 bytes starting with the specified MAC.
	[xx:xx:xx:xx:xx:xx]	Show the MAC address that its 6 bytes totally meet the specified MAC.
	[mac | vid | port]	Show the matched MAC addresses sorted by specific option.
Switch(config)# show mac address-table static		Show the created static MAC addresses.
Switch(config)# show mac address-table static [mac | vid | port]	[mac | vid | port]	Show the created static MAC addresses sorted by specific option.
Switch(config)# show mac address-table vlan [vlan_id] [mac | vid | port]	[vlan_id]	Show the MAC addresses that belongs to the specified VLAN ID.
	[mac | vid | port]	Show the specified VLAN's MAC addresses sorted by specific option.
Switch(config)# show mac learning		Show MAC learning setting of each interface.
Switch(config)# show mac static-mac all		Show all information of static MAC address table.
Switch(config)# show mac static-mac interface [port_list]	[port_list]	Show the specific port‘s information of static MAC address table.
Switch(config)# show mac aging-time		Show the current MAC address aging time.

Examples of MAC command	
Switch(config)# mac address-table aging-time 200	Set MAC address aging time to 200 seconds.

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

MAC & 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)# mac address-table static-mac [xx:xx:xx:xx:xx:xx] vlan [1-4094]	[xx:xx:xx:xx:xx:xx]	Specify a MAC address to the VLAN entry. **Note: Only one port could be set at a time.**
	[1-4094]	Specify the VLAN where the packets with the destination MAC address can be forwarded to the selected port.
Switch(config-if-PORT-PORT)# mac learning		Enable MAC address learning function of the selected port(s).
No command		
Switch(config-if-PORT)# no mac address-table static-mac [xx:xx:xx:xx:xx:xx] vlan [1-4094]	[xx:xx:xx:xx:xx:xx]	Remove the specified MAC address from the MAC address table. **Note: Only one port could be set at a time.**
	[1-4094]	Remove the VLAN to which the specified MAC belongs.
Switch(config-if-PORT-PORT)# no mac learning		Disable MAC address learning function of the selected port(s).

Use “Show mac filter” command to view the intended entries in the MAC address table.

Show Mac Filter Command	Parameter	Description
Switch(config)# show mac filter type [static | dynamic] sort-by [mac | port | vlan]	[static | dynamic]	Display the current MAC addresses that are either static or dynamic. **Note:** **To display both static and dynamic MAC addresses at the same time, simply skip this command.**
	[mac | port | vlan]	(Optional) Specify one particular sorting option to arrange the MAC address table. Entries will be displayed in ascending order according to the specified sort-by method.
Switch(config)# show mac filter mac [include | exclude] mac-address [xx:xx:xx:xx:xx:xx] mac-mask [xx:xx:xx:xx:xx:xx] sort-by [mac | port | vlan]	[include | exclude]	Display the intended MAC addresses that (don’t) correspond to the result of the comparison between the specified MAC address and the specified MAC address mask.
	[xx:xx:xx:xx:xx:xx]	Specify a MAC address to allow the filter to compare it against the specified MAC address mask.

	[xx:xx:xx:xx:xx:xx]	Specify a MAC address mask to allow the filter to compare it against the specified MAC address. **mac-mask:** It indicates how many bits, from left to right, the filter checks against the MAC address. To require an exact match with the MAC address (to check all 48 bits), enter FF:FF:FF:FF:FF:FF; to check only the first 32 bits, enter FF:FF:FF:FF:00:00.
	[mac | port | vlan]	(Optional) Specify one particular sorting option to arrange the MAC address table. Entries will be displayed in ascending order according to the specified sort-by method.
Switch#(config) show mac filter port-list [include | exclude] [port-list] sort-by [mac | port | vlan]	[include | exclude]	Display the intended MAC addresses that (don't) correspond to the comparison result between the specified MAC address and the specified MAC address mask.
	[port-list]	Specify the port from which the intended MAC addresses were learned. Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
	[mac | port | vlan]	(Optional) Specify one particular sorting option to arrange the MAC address table. Entries will be displayed in ascending order according to the specified sort-by method.
Switch#(config) show mac filter vlan [include | exclude] [vlan-id] sort-by [mac | port | vlan]	[include | exclude]	Display the MAC addresses that belong to the specified VLAN ID.
	[1-4094]	Specify a single VLAN ID to which the intended MAC addresses belong.
	[mac | port | vlan]	(Optional) Specify one particular sorting option to arrange the MAC address table. Entries will be displayed in ascending order according to the specified sort-by method.
Example of Show Mac Filter Command		**Description**
Switch#(config) show mac filter type static vlan include 5 sort-by port		Only the static MAC addresses that belong to VLAN 5 will be displayed, and the MAC address table will be displayed in a way that MAC addresses learned by the same port are grouped together and arranged in ascending order.
Switch#(config) show mac filter type dynamic mac exclude mac-address 9C:EB:E8:EA:5E:84 mac-		Only the dynamic MAC addresses of which the first 6 digits are not

mask FF:FF:FF:00:00:00 port-list include 5-10 vlan exclude 100	“9C:EB:E8” will be displayed, yet MAC addresses that belong to VLAN 100 and learned not by port 5, 6, 7, 8, 9, and 10 will not be displayed.

2.6.17 Management Command

Configure console/telnet/web/SSH access control and timeout value.

Management Command	Parameter	Description
Switch(config)# management console		Enable Console management. To manage the Managed Switch via Console.
Switch(config)# management console fail-retry [1-10]	[1-10]	Configure the retry times if the console login fails. The allowable value is 1~10 (times).
Switch(config)# management console block-time [1-120]	[1-120]	Configure the coslole block time of the Managed Switch if the console login retry times are more than the console fail-retry value you set up. The allowable value 1-120 (minutes).
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 [http | https | disable]	[http | https | disable]	Enable or disable Web Management. You can enable this management and manage the Managed Switch via the specified web management method between http and https.
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 fail-retry		Reset console fail-retry times back to the default (3 times).
Switch(config)# no management console block-time		Reset console block-time back to the default (5 minutes).
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.
Switch(config)# management web https		Enable Web Management and manage the Managed Switch via “https” web management method.

Configure RADIUS server authentication method.

Management Radius Command	Parameter	Description
Switch(config)# management radius retry-time [0-3]	[0-3]	Specify the retry time value. This is the number of times that the Managed Switch will try to reauthenticate if the RADIUS server is not reachable.
Switch(config)# management radius timeout [1-3]	[1-3]	Specify the timeout value (second). This is the amount of time that the Managed Switch will wait if the RADIUS server is not responding.
Switch(config)# management radius [server_number]	[1-2]	Specify a RADIUS server number to configure.
Switch(config-radius-NUMBER)# enable		Enable the RADIUS server.
Switch(config-radius-NUMBER)# port [1025-65535]	[1025-65535]	Specify the RADIUS server’s port number.
Switch(config-radius-NUMBER)# secret [secret]	[secret]	Specify a secret, up to 32 alphanumeric characters, for the

		RADIUS server. This secret key is used to validate communications with the RADIUS server.
Switch(config-radius-NUMBER)# server-ip [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the RADIUS server's IPv4/IPv6 address.
No Command		
Switch(config)# no management radius retry-time		Reset the RADIUS server retry time setting back to default.
Switch(config)# no management radius timeout		Reset the RADIUS server timeout setting back to default.
Switch(config-radius-NUMBER)# no enable		Disable the RADIUS server.
Switch(config-radius-NUMBER)# no port		Reset the radius port setting back to default (port number 1812).
Switch(config-radius-NUMBER)# no secret		Remove the configured secret value of the RADIUS server.
Switch(config-radius-NUMBER)# no server-ip		Delete the IPv4/IPv6 address of the RADIUS server.
Show Command		
Switch(config)# show management radius		Show the current configuration of both 1st and 2nd RADIUS servers.
Switch(config)# show management radius 1		Show the current configuration of the 1st RADIUS server.
Switch(config)# show management radius 2		Show the current configuration of the 2nd RADIUS server.
Examples of Management Radius Command		
Switch(config)# management radius retry-time 2		Set the retry time value to 2. The Managed Switch will try to authenticate twice if the RADIUS server is not reachable.
Switch(config)# management radius timeout 3		If the RADIUS server is not responding, the Managed Switch will wait 3 seconds before determining the authentication as timeout.
Switch(config)# management radius 2		Entering server number 2 will direct you to the configuration of 2nd RADIUS server
Switch(config-radius-2)# enable		Enable the 2nd RADIUS server.
Switch(config-radius-2)# port 1812		Set the 2nd RADIUS server port number as 1812.
Switch(config-radius-2)# secret abcxyzabc		Set up "abcxyzabc" as the secret key for validating communications with the 2nd RADIUS server.
Switch(config-radius-2)# server-ip 192.180.3.2		Set the 2nd RADIUS server address to 192.180.3.2.

Configure TACACS+ server authentication method.

Management Tacacs Command	Parameter	Description
Switch(config)# management tacacs retry-time [0-3]	[0-3]	Specify the retry time value. This is the number of times that the Managed Switch will try to reauthenticate if the TACACS+ server is not reachable.
Switch(config)# management tacacs timeout [1-3]	[1-3]	Specify the timeout value (second). This is the amount of time that the Managed Switch will wait if the TACACS+ server is not responding.
Switch(config)# management tacacs [1-2]	[1-2]	Specify a TACACS+ server number to configure.
Switch(config-tacacs-NUMBER)# enable		Enable the TACACS+ server.
Switch(config-tacacs-NUMBER)# port [49, 1025-65535]	[49, 1025-65535]	Specify the TACACS+ server's port number.
Switch(config-tacacs-NUMBER)# secret [secret]	[secret]	Specify a secret, up to 32 alphanumeric characters, for the TACACS+ server. This secret key is used to validate communications with the TACACS+ server.
Switch(config-tacacs-NUMBER)# server-ip [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the TACACS+ server's IPv4/IPv6 address.
No Command		
Switch(config)# no management tacacs retry-time		Reset the TACACS+ server retry time setting back to default.
Switch(config)# no management tacacs timeout		Reset the TACACS+ server timeout setting back to default.
Switch(config-tacacs-NUMBER)# no enable		Disable the TACACS+ server.
Switch(config-tacacs-NUMBER)# no port		Reset the radius port setting of the TACACS+ server back to default (port number 1812).
Switch(config-tacacs-NUMBER)# no secret		Remove the configured secret value of the TACACS+ server.
Switch(config-tacacs-NUMBER)# no server-ip		Delete the IPv4/IPv6 address of the TACACS+ server.
Show Command		
Switch(config)# show management tacacs		Show the current configuration of both 1st and 2nd TACACS+ servers.
Switch(config)# show management tacacs 1		Show the current configuration of the 1st TACACS+ server.
Switch(config)# show management tacacs 2		Show the current configuration of the 2nd TACACS+ server.
Examples of Management Tacacs Command		
Switch(config)# management tacacs retry-time 2		Set the retry time value to 2. The Managed Switch will try to authenticate twice if the TACACS+

	server is not reachable.
Switch(config)# management tacacs timeout 3	If the TACACS+ server is not responding, the Managed Switch will wait 3 seconds before determining the authentication as timeout.
Switch(config)# management tacacs 2	Entering server number 2 will direct you to the configuration of the 2nd TACACS+ server
Switch(config-tacacs-2)# enable	Enable the 2nd TACACS+ server.
Switch(config-tacacs-2)# server-ip 192.180.3.2	Set the 2nd TACACS+ server address to 192.180.3.2.
Switch(config-tacacs-2)# secret abcxyzabc	Set up “abcxyzabc” as the secret key for validating communications with the 2nd TACACS+ server.
Switch(config-tacacs-2)# port 1812	Set the 2nd TACACS+ server port number as 1812.

Configure authentication method management.

Management Command	Parameter	Description
Switch(config)# management authentication continue		Enable “Continue to the Next Method” on the authentication method function. Any user accessing the Managed Switch will be authenticated against the specified method scheme. **Note:** **Once this function is enabled, the Managed Switch will continue to the next method if the first authentication fails, say, due to invalid client credentials. It indeed delivers extra flexibility for an ought-to-be-authenticated user, yet at the expense of network security. To fully protect against malicious users, it’s recommended to set this function disabled.**
Switch(config)# management authentication all [method 1] [method 2] [method 3] [method 4] [method 5]	[disable | local | radius1 | radius2 | tacacs1 | tacacs2]	Configure the authentication method scheme for all interfaces, including Telnet, SSH, Web, and Console. **Note:** **Each method can be configured as disable, local, radius1, radius2, tacacs1, or tacacs2. However, local must be set after RADIUS and TACACS+ servers throughout the specified method scheme, and the 1st method cannot be configured as disable.**

No Command	
Switch(config)# no management authentication continue	Disable “Continue to the Next Method” on the authentication method function. **Note:** **Disabling this function means the device will only apply method 1. Access will be denied to those who fail the authentication against the 1st method.**
Switch(config)# no management authentication all	Reset the authencation method scheme back to default (method 1 as local, and the remainder as disable).
Show Command	
Switch(config)# show management authentication	Show the current configuration of the authentication method function.
Examples of Management Command	
Switch(config)# management authentication continue	Enable “Continue to the Next Method” on the authentication method function.
Switch(config)# management authentication all [tacacs2] [radius1] [tacacs1] [radius2] [local]	A user will be first authenticated by the 2nd TACACS+ server which you specified earlier. However, if the authentication fails, the device will move on to the next method (in this case, the 1st RADIUS server), and applies the third method (the 1st TACACS+ server) if the second authentication fails.

2.6.18 Mirror Command

Mirror Command	Parameter	Description
Switch(config)# mirror		Globally enable Port Mirroring function.
Switch(config)# mirror index [1-4]	[1-4]	Specify the index of port mirroring you would like to configure. Up to 4 sets of port mirroring can be set up.
Switch (config-mirror-index)# enable		Enable the specified port mirroring. **NOTE: This command works only when its mirroring-related settings are completed.**
Switch(config-mirror-index)# destination [port_number]	[port_number]	Specify the preferred destination port (1~28) for port mirroring. **NOTE: The destination port of Index 1~4 port mirroring cannot be the same.**
Switch(config-mirror-index)# source [port_list] direction [tx | rx | both]	[port_list] [tx | rx | both]	Specify the source port number(s) and TX/RX/both direction for port mirroring. **NOTE: The port selected as the destination port cannot be the source port.**

No command		
Switch(config)# no mirror		Globally disable Port Mirroring function.
Switch(config)# no mirror index [1-4]	[1-4]	Clear the settings of the specified port mirroring.
Switch (config-mirror-index)# no enable		Disable the specified port mirroring.
Switch(config-mirror-index)# no destination		Reset the mirroring destination port back to the default. (Port 1)
Switch(config-mirror-index)# no source [port_list] direction [tx | rx | both]	[port_list] [tx | rx | both]	Remove the source port number(s) and TX/RX/both direction from the port mirroring list.
Show command		
Switch(config)# show mirror		Show the current port mirroring configuration.
Switch(config-mirror-index)# show		Show the current configuration of the specified port mirroring.
Example of Mirror command		
Switch(config-mirror-3)# destination 8		The selected source ports' data will mirror to Port 8 in the port mirroring of Index No. 3.
Switch(config-mirror-3)# source 1-7 direction tx		Port 1 to 7's transmitting packets will mirror to the destination port in the port mirroring of Index No. 3.

2.6.19 MVR Command

MVR (Multicast VLAN Registration) allows clients receiving multicast stream transmitted from the upstream device to reside in different VLANs, which is particularly suitable for networks with the high demand of bandwidth.

Instead of transmitting multiple copies of multicast traffic to clients in the different VLANs separately, an upstream device merely needs to transmit multicast traffic to a multicast VLAN if the configured MVR is enabled on Managed Switch. Therefore, the network bandwidth can greatly be saved and diminish the load of upstream device(s) without sending several identical multicast data flows downstream to each client VLAN.

MVR also allows a client on a port to subscribe/unsubscribe to a multicast stream on the multicast VLAN. MVR not only provides the ability to continuously send multicast streams to the multicast VLAN, but isolates the multicast streams from the client VLANs for the reasons of bandwidth and security.

1. Set up MVR

MVR Command	Parameter	Description
Switch(config)# mvr		Globally enable the MVR function.
Switch(config)# mvr vlan [1-4094]	[1-4094]	Configure the specified VLAN as a multicast VLAN.
Switch(config-mvr-ID)# active		Enable the specified multicast VLAN.
Switch(config-mvr-ID)# multicast-group ipv4 all		Specify all of IPv4 multicast addresses as the multicast group for the selected

		multicast VLAN.
Switch(config-mvr-ID)# multicast-group ipv4 range from [E.F.G.H] to [E.F.G.H]	[E.F.G.H] [E.F.G.H]	Specify a range of IPv4 multicast addresses as the multicast group for the selected multicast VLAN.
Switch(config-mvr-ID)# multicast-group ipv6 all		Specify all of IPv6 multicast addresses as the multicast group for the selected multicast VLAN.
Switch (config-mvr-ID)# multicast-group ipv6 range from [A:B:C:D:E:F:G:H] to [A:B:C:D:E:F:G:H]	[A:B:C:D:E:F:G:H] [A:B:C:D:E:F:G:H]	Specify a range of IPv6 multicast addresses as the multicast group for the selected multicast VLAN.
Switch (config-mvr-ID)# name [mvr_name]	[mvr_name]	Specify a MVR name for the selected multicast VLAN. Up to 15 characters can be accepted.
No command		
Switch(config)# no mvr		Globally disable the MVR function.
Switch(config)# no mvr vlan [1-4094]	[1-4094]	Remove the specified multicast VLAN.
Switch(config-mvr-ID)# no active		Disable the specified multicast VLAN.
Switch(config-mvr-ID)# no multicast-group ipv4 all		Remove the specific IPv4 multicast group assigned with all IPv4 multicast addresses for the selected multicast VLAN.
Switch(config-mvr-ID)# no multicast-group ipv4 range from [E.F.G.H] to [E.F.G.H]	[E.F.G.H] [E.F.G.H]	Remove the specific IPv4 multicast group assigned with the specified range of IPv4 multicast addresses for the selected multicast VLAN.
Switch(config-mvr-ID)# no multicast-group ipv6 all		Remove the specific IPv6 multicast group assigned with all IPv6 multicast addresses for the selected multicast VLAN.
Switch(config-mvr-ID)# no multicast-group ipv6 range from [A:B:C:D:E:F:G:H] to [A:B:C:D:E:F:G:H]	[A:B:C:D:E:F:G:H] [A:B:C:D:E:F:G:H]	Remove the specific IPv6 multicast group assigned with the specified range of IPv6 multicast addresses for the selected multicast VLAN.
Switch(config-mvr-ID)# no name		Reset the MVR name back to the default for the selected multicast VLAN.
Show command		
Switch# show mvr		Show the current MVR configuration.
Switch# show mvr interface		Show the current MVR port configuration of each port.
Switch# show mvr interface [port_list]	[port_list]	Show the current MVR port configuration of the specific port.
Switch# show mvr multicast-group		Show the current configuration of all IPv4 and IPv6 multicast groups.
Switch# show mvr multicast-group ipv4		Show the current configuration of all IPv4 multicast groups.
Switch# show mvr multicast-group ipv4 from [E.F.G.H] to [E.F.G.H]	[E.F.G.H] [E.F.G.H]	Show the current configuration of the specified IPv4 multicast group.

Switch# show mvr multicast-group ipv6		Show the current configuration of all IPv6 multicast groups.
Switch# show mvr multicast-group ipv6 from [A:B:C:D:E:F:G:H] to [A:B:C:D:E:F:G:H]	[A:B:C:D:E:F:G:H]	Show the current configuration of the specified IPv6 multicast group.
	[A:B:C:D:E:F:G:H]	
Switch# show mvr multicast-group vlan [1-4094]	[1-4094]	Show the current multicast group configuration for the specific multicast VLAN.
Switch# show mvr vlan [1-4094]	[1-4094]	Show the current configuration of the specific multicast VLAN.
Switch(config)# show mvr		Show the current MVR configuration.
Switch(config)# show mvr interface		Show the current MVR port configuration of each port.
Switch(config)# show mvr interface [port_list]	[port_list]	Show the current MVR port configuration of the specific port.
Switch(config)# show mvr multicast-group		Show the current configuration of all IPv4 and IPv6 multicast groups.
Switch(config)# show mvr multicast-group ipv4		Show the current configuration of all IPv4 multicast groups.
Switch(config)# show mvr multicast-group ipv4 from [E.F.G.H] to [E.F.G.H]	[E.F.G.H]	Show the current configuration of the specified IPv4 multicast group.
	[E.F.G.H]	
Switch(config)# show mvr multicast-group ipv6		Show the current configuration of all IPv6 multicast groups.
Switch(config)# show mvr multicast-group ipv6 from [A:B:C:D:E:F:G:H] to [A:B:C:D:E:F:G:H]	[A:B:C:D:E:F:G:H]	Show the current configuration of the specified IPv6 multicast group.
	[A:B:C:D:E:F:G:H]	
Switch(config)# show mvr multicast-group vlan [1-4094]	[1-4094]	Show the current multicast group configuration for the specific multicast VLAN.
Switch(config)# show mvr vlan [1-4094]	[1-4094]	Show the current configuration of the specific multicast VLAN.
Example of MVR command		
Switch(config)# mvr		Enable the MVR function globally on the Managed Switch.
Switch(config)# mvr vlan 500		Configure 500 VLAN ID as a multicast VLAN.
Switch(config-mvr-500)# multicast-group ipv4 range from 239.0.0.1 to 239.0.0.254		Configure IPv4 multicast addresses ranging from 239.0.0.1 to 239.0.0.254 as the multicast group for MVR 500.

3. Use “Interface” command to configure the MVR interfaces as Receiver & Sender Port settings.

MVR & 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)# mvr vlan [1-4094] type receiver-port	[1-4094]	Configure the selected port(s) as a receiver port for the specified multicast VLAN. **Receiver port:** Configure a port as a receiver port if it is a client port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages. Receiver ports cannot belong to the multicast VLAN.
Switch(config-if-PORT-PORT)# mvr vlan [1-4094] type sender-port		Configure the selected port(s) as a sender port for the specified multicast VLAN. **Sender port:** The sender port is the multicast server port. Configure uplink ports that receive and send multicast data as sender ports. Clients cannot be directly connected to sender ports. **Note: The port number configured as Receiver port cannot be the Sender port.**
No command		
Switch(config-if-PORT-PORT)# no mvr vlan [1-4094] type receiver-port	[1-4094]	Remvoe the selected port(s) configured as the receiver port for the specified multicast VLAN.
Switch(config-if-PORT-PORT)# no mvr vlan [1-4094] type sender-port	[1-4094]	Remvoe the selected port(s) configured as the sender port for the specified multicast VLAN.

2.6.20 NTP Command

NTP Command	Parameter	Description
Switch(config)# ntp		Enable Network Time Protocol to have Managed Switch's system time synchronize with NTP time server.
Switch(config)# ntp daylight-saving [recurring | date]	[recurring]	Enable daylight saving function with recurring mode.
	[date]	Enable daylight saving function with date mode.
Switch(config)# ntp offset [Mm,w,d,hh:mm-Mm,w,d,hh:mm]	[Mm,w,d,hh:mm-Mm,w,d,hh:mm]	Specify the offset of daylight saving in 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-	Specify the offset of daylight saving in date

[Days,hh:mm-Days,hh:mm]	Days,hh:mm]	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:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the primary NTP time server's IPv4/IPv6 address.
Switch(config)# ntp server2 [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the secondary NTP time server's IPv4/IPv6 address.
Switch(config)# ntp syn-interval [1-8]	[1-8]	Specify the time interval to have Managed Switch synchronize with NTP time server. **1=1hour, 2=2hours, 3=3hours, 4=4hours, 5=6hours, 6=8hours, 7=12hours, 8=24hours**
Switch(config)# ntp time-zone [0-135]	[0-135]	Specify the time zone to which the Managed Switch belongs. Use space and a question mark to view the complete code list of 136 time zones. For example, "Switch(config)# ntp time-zone ?"
No command		
Switch(config)# no ntp		Disable Network Time Protocol to stop Managed Switch's system time synchronizing with NTP time server.
Switch(config)# no ntp daylight-saving		Disable the daylight saving function.
Switch(config)# no ntp offset		Reset the offset value back to the default.
Switch(config)# no ntp server1		Delete the primary time server's IPv4/IPv6 address.
Switch(config)# no ntp server2		Delete the secondary time server's IPv4/IPv6 address.
Switch(config)# no ntp syn-interval		Reset the synchronization time interval back to the default.
Switch(config)# no ntp time-zone		Reset the time-zone setting back to the default.
Show command		
Switch# show ntp		Show the current NTP time server configuration.
Switch(config)# show ntp		Show the current NTP time server configuration.
Examples of NTP command		
Switch(config)# ntp		Enable NTP function for the Managed Switch.
Switch(config)# ntp daylight-saving date		Enable the daylight saving function in date mode.
Switch(config)# ntp offset [100,12:00-101,12:00]		Daylight saving time date start from the 100th day of the year to the 101th day of the year.
Switch(config)# ntp server1 192.180.0.12		Set the primary NTP time server's IP address to 192.180.0.12.

Switch(config)# ntp server2 192.180.0.13	Set the secondary NTP time server's IP address to 192.180.0.13.
Switch(config)# ntp syn-interval 4	Set the synchronization interval to 4 hours.
Switch(config)# ntp time-zone 3	Set the time zone to GMT-8:00 Vancouver.

2.6.21 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 | strict]	[weight | strict]	Specify QoS Queue mode between weight and strict mode.
Switch(config)# qos queue-weighted [1:2:4:8:16:32:64:127]	[1:2:4:8:16:32:64 :127]	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		Globally disable DSCP

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 bit 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 and user priority configuration.
Switch(config)# show qos interface		Show QoS interface overall information.
Switch(config)# show qos interface [port-list]	[port-list]	Show the specific QoS interface information.
Switch(config)# show qos remarking		Show QoS remarking-mapping 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.

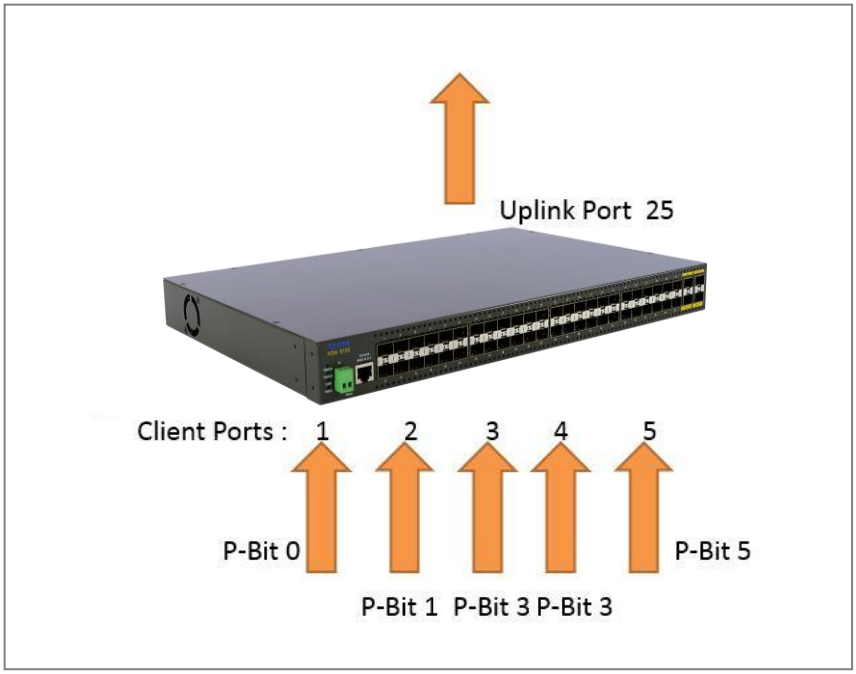
2. Use “interface” command to configure a group of ports’ QoS settings.

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		Enable QoS ingress rate limit settings.
Switch(config-if-PORT-PORT)# qos rate-limit ingress rate [500-1000000 | 1-1000] Kbps/Mbps	[500-1000000 | 1-1000] Kbps/Mbps	Specify the ingress rate limit value. (Valid range is from 500-1000000 in unit of Kbps or 1-1000 in unit of Mbps).
Switch(config-if-PORT-PORT)# qos rate-limit ingress unit [Kbps |	[Kbps | Mbps]	Specify the unit of the ingress rate limit between Kbps and Mbps.

Mbps]		
Switch(config-if-PORT-PORT)# qos rate-limit egress		Enable QoS egress rate limit settings.
Switch(config-if-PORT-PORT)# qos rate-limit egress rate [500-1000000 | 1-1000] Kbps/Mbps	[500-1000000 | 1-1000] Kbps/Mbps	Specify the egress rate limit value. (Valid range is from 500-1000000 in unit of Kbps or 1-1000 in unit of Mbps).
Switch(config-if-PORT-PORT)# qos rate-limit egress unit [Kbps | Mbps]	[Kbps | Mbps]	Specify the unit of the egress rate limit between Kbps and Mbps.
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 settings.
Switch(config-if-PORT-PORT)# no qos rate-limit ingress rate		Reset the ingress rate limit value back to the default.
Switch(config-if-PORT-PORT)# no qos rate-limit ingress unit		Reset the unit of the ingress rate limit back to the default (Kbps).
Switch(config-if-PORT-PORT)# no qos rate-limit egress		Disable QoS egress rate limit settings.
Switch(config-if-PORT-PORT)# no qos rate-limit egress rate		Reset the egress rate limit value back to the default.
Switch(config-if-PORT-PORT)# no qos rate-limit egress unit		Reset the unit of the egress rate limit back to the default (Kbps).
Switch(config-if-PORT-PORT)# no qos user-priority		Reset the user priority value setting back to the default.(0)

For QoS configuration via CLI, we take an FOS-5152 Managed Switch for example to let the users have a clear understanding of these QoS commands.

Under this network environment, FOS-5152 will be configured as Table 2-1. 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; Queue 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 2-1

Below is the complete CLI commands applied to FOS-5152 Managed Switch.

	Command	**Purpose**
STEP1	**configure** **Example:** FOS-5152# config FOS-5152(config)#	**Enter the global configuration mode.**
STEP2	**qos 802.1p** **Example:** FOS-5152(config)# qos 802.1p OK !	**In this example, it configures the QoS Mode to 802.1p.**
STEP3	**qos queuing-mode weight** **Example:** FOS-5152(config)# qos queuing-mode weight **OK !**	**In this example, it configures Queue Mode as "Weight".**
STEP4	**qos queue-weighted** *weighted* **Example:** FOS-5152(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:** FOS-5152(config)# qos 802.1p-map 0 0 FOS-5152(config)# qos 802.1p-map 1 1 FOS-5152(config)# qos 802.1p-map 3 2 FOS-5152(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:** FOS-5152(config)# interface 1 FOS-5152(config-if-1)#	**Specify the Port 1 that you would like to configure P-Bit.**
STEP7	**qos user-priority** *P-Bit* **Example:** FOS-5152(config-if-1)# qos user-priority 0	**In this example, it configures P-Bit value as 0 for Port 1.**

STEP8	**exit** **Example:** FOS-5152(config-if-1)# exit FOS-5152(config)#	**Return to the global configuration mode.**
STEP9	**interface** *port_list* **Example:** FOS-5152(config)# interface 2 FOS-5152(config-if-2)#	**Specify the Port 2 that you would like to configure P-Bit.**
STEP10	**qos user-priority** *P-Bit* **Example:** FOS-5152(config-if-2)# qos user-priority 1	**In this example, it configures P-Bit value as 1 for Port 2.**
STEP11	**exit** **Example:** FOS-5152(config-if-2)# exit FOS-5152(config)#	**Return to the global configuration mode.**
STEP12	**interface** *port_list* **Example:** FOS-5152(config)# interface 3, 4 FOS-5152(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 unit** *kbps/Mbps* **Example:** FOS-5152(config-if-3,4)# qos rate-limit ingress unit Mbps OK !	**In this example, it configures the unit of the ingress rate limit as" Mbps" for Port 3 and Port 4.**
STEP14	**qos rate-limit ingress rate** *limit_rate(kbps/Mbps)* **Example:** FOS-5152(config-if-3,4)# qos rate-limit ingress rate 10 OK !	**In this example, it configures Port 3 and Port 4 with 10M Ingress Rate.**
STEP15	**qos rate-limit egress unit** *kbps/Mbps* **Example:** FOS-5152(config-if-3,4)# qos rate-limit egress unit Mbps OK !	**In this example, it configures the unit of the egress rate limit as" Mbps" for Port 3 and Port 4.**
STEP16	**qos rate-limit egress rate** *limit_rate(kbps/Mbps)* **Example:** FOS-5152(config-if-3,4)# qos rate-limit egress rate 10 OK !	**In this example, it configures Port 3 and Port 4 with 10M Egress Rate.**
STEP17	**qos user-priority** *P-Bit* **Example:** FOS-5152(config-if-3,4)# qos user-priority 3	**In this example, it configures P-Bit value as 3 for Port 3 and Port 4.**
STEP18	**exit** **Example:** FOS-5152(config-if-3,4)# exit	**Return to the global configuration mode.**

	FOS-5152(config)#	
STEP19	**interface** *port_list* **Example:** FOS-5152(config)# interface 5 FOS-5152(config-if-5)#	**Specify the Port 5 that you would like to configure QoS Rate limit.**
STEP20	**qos rate-limit ingress unit** *kbps/Mbps* **Example:** FOS-5152(config-if-5)# qos rate-limit ingress unit Kbps OK !	**In this example, it configures the unit of the ingress rate limit as" Kbps" for Port 5**
STEP21	**qos rate-limit ingress rate** *limit_rate(kbps/Mbps)* **Example:** FOS-5152(config-if-5)# qos rate-limit ingress rate 1000000 OK !	**In this example, it configures Port 5 with 1G Ingress Rate.**
STEP22	**qos rate-limit egress unit** *kbps/Mbps* **Example:** FOS-5152(config-if-5)# qos rate-limit egress unit Kbps OK !	**In this example, it configures the unit of the egress rate limit as" Kbps" for Port 5**
STEP23	**qos rate-limit egress rate** *limit_rate(kbps/Mbps)* **Example:** FOS-5152(config-if-5)# qos rate-limit egress rate 1000000 OK !	**In this example, it configures Port 5 with 1G Engress Rate.**
STEP24	**qos user-priority** *P-Bit* **Example:** FOS-5152(config-if-5)# qos user-priority 5	**In this example, it configures P-Bit value as 5 for Port 5.**
STEP25	**exit** **Example:** FOS-5152(config-if-5)# exit FOS-5152(config)#	**Return to the global configuration mode.**
STEP26	**exit** **Example:** FOS-5152(config)# exit FOS-5152#	**Return to the Privileged mode.**
STEP27	**write** **Example:** FOS-5152# write Save Config Succeeded!	**Save the running configuration into the startup configuration.**

After completing the QoS settings for your FOS-5152 switches, you can issue the commands listed below for checking your configuration.

Example 1,

FOS-5152(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!

Priority   Queue
---------  ----------
       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  Queue   DSCP  Queue   DSCP  Queue   DSCP  Queue
--------  ----------  ---------  ---------  ---------  ---------  ---------  --------
     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
```

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

Port   Priority
------  --------
   1    0
   2    1
   3    3
   4    3
   5    5
   6    0
   7    0
   8    0
   9    0
  10    0

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

  11    0
  12    0
  13    0
  14    0
  15    0
  16    0
  17    0
  18    0
  19    0
  20    0

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

  21    0
  22    0
  23    0
  24    0
  25    0
  26    0
  27    0
  28    0
CPU    0


FOS-5152(config)#
```

Example 2,

FOS-5152(config)# show qos interface

```
==============================================================================
QoS port Information :
==============================================================================
          Ingress Rate                      Egress Rate
      ------------------------------    ------------------------------------
Port   State      Rate       Unit      State       Rate       Unit
------  ---------  ----------  ----------  ----------  ---------- ----------
  1   disable         500  Kbps    disable         500     Kbps
  2   disable         500  Kbps    disable         500     Kbps
  3   disable          10   Mbps   disable          10     Mbps
  4   disable          10   Mbps   disable          10     Mbps
  5   disable     1000000   Kbps    disable     1000000     Kbps
  6   disable         500   Kbps    disable         500     Kbps
  7   disable         500   Kbps    disable         500     Kbps
  8   disable         500   Kbps    disable         500     Kbps

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

  9    disable         500  Kbps    disable         500     Kbps
 10   disable         500  Kbps    disable         500     Kbps
 11   disable         500  Kbps    disable         500     Kbps
 12   disable         500  Kbps    disable         500     Kbps
 13   disable         500  Kbps    disable         500     Kbps
 14   disable         500  Kbps    disable         500     Kbps
 15   disable         500  Kbps    disable         500     Kbps
 16   disable         500  Kbps    disable         500     Kbps

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

 17    disable         500  Kbps    disable         500     Kbps
 18   disable         500  Kbps    disable         500     Kbps
 19   disable         500  Kbps    disable         500     Kbps
 20   disable         500  Kbps    disable         500     Kbps
 21   disable         500  Kbps    disable         500     Kbps
 22   disable         500  Kbps    disable         500     Kbps
 23   disable         500  Kbps    disable         500     Kbps
 24   disable         500  Kbps    disable         500     Kbps

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

 25    disable         500  Kbps    disable         500     Kbps
 26   disable         500  Kbps    disable         500     Kbps
 27   disable         500  Kbps    disable         500     Kbps
 28   disable         500  Kbps    disable         500     Kbps


FOS-5128(config)#
```

2.6.22 Security Command

When a device on the network is malfunctioning or application programs are not well designed or properly configured, broadcast/unknown multicast/unknown unicast 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/unknown multicast/unknown unicast traffic on a per port basis so as to protect network from broadcast/unknown multicast/ unknown unicast storms. Any broadcast/unknown multicast/unknown unicast packets exceeding the specified value will then be dropped.

Port Isolation is used to set up port's communication availability that they can only communicate with a given "uplink". Please note that if the port isolation function is enabled, the Port-based VLAN will be invaild automatically.

As to Mac Limit function, it is to set number of threshold within which MAC address can be learned. After it reaches the threshold, any other incoming MAC address would be dropped or port would be shutdown until the recovery mechanism activates. Please note that mac address table will be erased if the Mac Limit function is enabled.

Besides, the Sticky MAC address function is also provided to keep the event that the packets with the same source MAC address are received by different ports from being taken place. In case this function of the specified port is enabled (the port is also known as the sticky MAC port), then, other ports of the switch cannot receive the packets with the same source MAC address learned by this sticky MAC port anymore. If other ports receive the packets with the same source MAC address again, these packets will be dropped by the switch.

Generally, any auto-learned MAC address from the switch will be a dynamic MAC address. Through this Sticky MAC address function, however, the MAC address learned by the sticky MAC port will automatically be turned into a static one in MAC address table. But, this kind of static MAC address is regarded as a "Sticky" type of MAC address, and it still does not write into the running configuration file. To transfer the MAC address type from "Sticky" into "Manual", and write it into the running configuration file, you may refer to Section 4.6.2 "Static MAC Table Setup".

1. Enable or disable Layer 2 control protocol filter, broadcast/unknown multicast/unknown unicast storm control, port isolation and MAC Limit.

Security Command	Parameter	Description
Switch(config)# security l2control-protocol 00-0F		Enable to filter packets with the destination MAC address ranging from 0180c2000000 to 0180c200000f
Switch(config)# security l2control-protocol 20-2F		Enable to filter packets with the destination MAC address ranging from 0180c2000020 to 0180c200002f.
Switch(config)# security l2control-protocol 10		Enable to filter packets with the destination MAC address 0180c2000010.
Switch(config)# security mac-limit		Globally enable the MAC Limit function on the switch.
Switch(config)# security mac-limit notification threshold interval [120-86400]	[120-86400]	To set up the time interval of sending the alarm trap or system log if the number of source MAC address learned exceeds the limit continuously. The allowable value is

		between 120 and 86400 seconds.
Switch(config)# security port-isolation		Globally enable the port isolation function. If port isolation is set to enabled, the ports cannot communicate with each other. **Note 1: If the port isolation function is enabled, the Port-based VLAN will be invaild automatically.** **Note 2: "Port Isolation" function is not "Private VLAN" fucntion.**
Switch(config)# security storm-protection		Globally enable the storm control function.
Switch(config)# security storm-protection notification threshold interval [120-86400]	[120-86400]	To set up the time interval of sending the alarm trap or system log if broadcast/unknown multicast/unknown unicast packets flood continuously. The allowable value is between 120 and 86400 seconds.
No command		
Switch(config)# no security l2control-protocol 00-0F		Disable to filter packets with the destination MAC address ranging from 0180c2000000 to 0180c200000f
Switch(config)# no security l2control-protocol 20-2F		Disable to filter packets with the destination MAC address ranging from 0180c2000020 to 0180c200002f.
Switch(config)# no security l2control-protocol 10		Disable to filter packets with the destination MAC address 0180c2000010.
Switch(config)# no security mac-limit		Globally disable MAC Limit function on the switch.
Switch(config)# no security mac-limit notification threshold interval		Reset the time interval of sending the alarm trap or system log back to the default if the number of source MAC address learned exceeds the limit continuously. (120 seconds)
Switch(config)# no security port-isolation		Globally disable port isolation function.
Switch(config)# no security storm-protection		Globally disable the storm control function.
Switch(config)# no security storm-protection notification threshold interval		Reset the time interval of sending the alarm trap or system log back to the default if broadcast/unknown multicast/unknown unicast packets flood continuously. (120 seconds)
Show command		
Switch(config)# show security mac-limit		Show the current MAC Limit configuration of all ports.
Switch(config)# show security mac-limit [port_list]	[port_list]	Show the current MAC Limit configuration of specified port(s).

Switch(config)# show security port-isolation		Show the current port isolation configuration.
Switch(config)# show security storm-protection		Show the current storm control global configuration.
Switch(config)# show security storm-protection Interface		Show the current storm control configuration of all ports.
Switch(config)# show security storm-protection Interface [port_list]	[port_list]	Show the current storm control configuration of specified port(s).
Switch(config)# show security l2control-protocol		Show L2 Control Protocol Filter Configuration.
Examples of Security command		
Switch(config)# security mac-limit notification threshold interval 300		Set the time interval as 300 seconds to send the alarm trap or system log if the number of source MAC address learned exceeds the limit continuously.
Switch(config)# security storm-protection notification threshold interval 200		To set the time interval as 200 seconds to send the alarm trap or system log if broadcast/unknown multicast/unknown unicast packets flood continuously.

2. Use "Interface" command to configure broadcast/unknown multicast/unknown unicast storm control, port isolation and Mac Limiter settings for security.

Security & 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)# security mac-limit		Enable MAC Limit function of the selected port(s).
Switch(config-if-PORT-PORT)# security mac-limit action [drop | shutdown]	[drop | shutdown]	Specify the action that would be taken when the number of source MAC address learned exceeds the limit.
Switch(config-if-PORT-PORT)# security mac-limit maximum [1-50]	[1-50]	Specify the maximum number of source MAC address that can be learned for each of the selected port(s). This is to set number of threshold within which MAC address can be learned. After it reaches the threshold, any other incoming MAC address would be dropped or port would be shutdown until the recovery mechanism activates. The valid range of number that can be configured is 1~50.
Switch(config-if-PORT-PORT)# security mac-limit sticky		Enable the function of sticky MAC address on the selected port(s).

Switch(config-if-PORT-PORT)# security mac-limit unlock		Unlock the selected port(s) that are locked because the number of MAC address learned exceeds the threshold and the port action is set as “Shutdown”.
Switch(config-if-PORT-PORT)# security port-isolation up-link-port		Configure the selected port(s) as uplinks that are allowed to communicate with other ports.
Switch(config-if-PORT-PORT)# security storm-protection broadcast [1-256k]	[1-256k]	Specify the maximum broadcast packets per second (pps). Any broadcast packets exceeding the specified threshold will then be dropped. The packet rates that can be specified are listed below: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k NOTE: To view a list of allowable values that can be specified you can press “spacebar” and then followed by “?”. For example, “Switch(config)# security storm-protection broadcast ?”
Switch(config-if-PORT-PORT)# security storm-protection unknown-multicast [1-256k]	[1-256k]	Specify the maximum unknown multicast packets per second (pps). Any unknown multicast packets exceeding the specified threshold will then be dropped. The packet rates that can be specified are listed below: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k ***NOTE:*** *To view a list of allowable values that can be specified you can press “spacebar” and then followed by “?”. For example, “Switch(config)# security storm-protection multicast ?”*
Switch(config-if-PORT-PORT)# security storm-protection unknown-unicast [1-256k]	[1-256k]	Specify the maximum unknown unicast packets per second (pps). Any unknown unicast packets exceeding the specified threshold will then be dropped. The packet rates that can be specified are listed below: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k ***NOTE:*** *To view a list of allowable values that can be specified you can*

		press “spacebar” and then followed by “?”. For example, “Switch(config)# security storm-protection unicast ?”
No command		
Switch(config-if-PORT-PORT)# no security mac-limit		Disable MAC Limit function of the selected port(s).
Switch(config-if-PORT-PORT)# no security mac-limit action		Reset the action that would be taken when the number of source MAC address learned exceeds the limit back to the default. (Drop)
Switch(config-if-PORT-PORT)# no security mac-limit maximum		Reset the maximum number of source MAC address that can be learned for each of the selected port(s) back to the default. (1)
Switch(config-if-PORT-PORT)# no security mac-limit sticky		Disable the function of sticky MAC address on the selected port(s).
Switch(config-if-PORT-PORT)# no security port-isolation up-link-port		Disable the specified port(s) as non-up-link-port.
Switch(config-if-PORT-PORT)# no security storm-protection broadcast		Disable broadcast storm control on the selected ports.
Switch(config-if-PORT-PORT)# no security storm-protection unknown-multicast		Disable unknown-multicast storm control on the selected ports.
Switch(config-if-PORT-PORT)# no security storm-protection unknown-unicast		Disable unknown-unicast storm control on the selected ports.
Examples of Security command		
Switch(config-if-1-3)# security mac-limit		Enable Port 1~Port 3’s MAC Limit function.
Switch(config-if-1-3)# security mac-limit maximum 50		Configure the maximum 50 sets of MAC address that can be learned for Port1~Port 3 respectively.

2.6.23 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		Enable SNMP Management. To manage the Managed Switch via SNMP.
Switch(config)# snmp-server community [community]	[community]	Create/modify a SNMP community name. Up to 20 alphanumeric characters can be accepted.
Switch(config-community-NAME)# active		Enable the specified SNMP community account.
Switch(config-community-NAME)# description [description]	[description]	Enter the description for the specified SNMP community. Up to 35 alphanumerical characters can be accetpted.

Switch(config-community-NAME)# level [admin | rw | ro]	[admin | rw | ro]	Specify the access privilege level for the specified SNMP account. **admin:** Own the full-access right, including maintaining user account, system information, loading factory settings, etc.. **rw:** Read & Write access privilege. Own the partial-access right, unable to modify user account, system information and load factory settings. **ro:** Allow to view only.
No command		
Switch(config)# no snmp-server		Disable SNMP Management.
Switch(config)# no snmp-server community [community]	[community]	Delete the specified community.
Switch(config-community-NAME)# no active		Disable the specified SNMP community account.
Switch(config-community-NAME)# no description		Remove the description of SNMP community.
Switch(config-community-NAME)# no level		Reset the access privilege level back to the default. (Read Only)
Show command		
Switch(config)# show snmp-server		Show SNMP server configuration.
Switch(config)# show snmp-server community		Show SNMP server community configuration.
Switch(config)# show snmp-server community [community]		Show the specified SNMP server community's configuration.
Switch(config-community-NAME)# show		Show the selected community's settings.

Exit command	
Switch(config-community-NAME)# exit	Return to the global configuration mode.
Example of Snmp-server	
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 the access privilege level of "mycomm" community to admin (full-access privilege).

2. Set up a SNMP trap destination.

Trap-destination Command	Parameter	Description
Switch(config)# snmp-server trap-destination [1-3]	[1-3]	Specify the index of SNMP trap destination you would like to modify. Up to 3 sets of SNMP trap destination can be set up.

Switch(config-trap-ID)# active		Enable the specified SNMP trap destination.
Switch(config-trap-ID)# community [community]	[community]	Enter the description for the specified SNMP trap destination.
Switch(config-trap-ID)# destination [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F :G:H]	Specify SNMP server's IPv4/IPv6 address for the specified SNMP trap destination.
No command		
Switch(config)# no snmp-server trap-destination [1-3]	[1-3]	Reset the specified SNMP trap destination configuration back to the default.
Switch(config-trap-ID)# no active		Disable the specified SNMP trap destination.
Switch(config-trap-ID)# no community		Delete the description for the specified SNMP trap destination.
Switch(config-trap-ID)# no destination		Delete SNMP server's IPv4/IPv6 address for the specified SNMP trap destination.
Show command		
Switch(config)# show snmp-server trap-destination		Show all of SNMP trap destination configurations.
Switch(config)# show snmp-server trap-destination [1-3]	[1-3]	Show the specified SNMP trap destination configuration.
Switch(config-trap-ID)# show		Show the configuration of the selected SNMP trap destination.
Exit command		
Switch(config-trap-ID)# exit		Return to the global configuration mode.
Examples of Trap-destination		
Switch(config)# snmp-server trap-destination 1		Specify the trap destination 1 to configure.
Switch(config-trap-1)# active		Activate the trap destination ID 1.
Switch(config-trap-1)# community mycomm		Add the description "mycomm" to this trap destination.
Switch(config-trap-1)# destination 192.168.1.254		Set SNMP server's IP address as "192.168.1.254" for this trap destination.

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 | case-fan | cold-start | cpu-load | cpu-temperature | digital | mac-limit | port-link | power-down| storm-control | system-voltage | warm-start | console-port-link]	[all | auth-fail | auto-backup | case-fan | cold-start | cpu-load | cpu-temperature | digital | mac-limit | port-link | power-down| storm-control | system-voltage	Specify a trap type that will be sent when a certain situation occurs. **all:** A trap will be sent when authentication fails, auto-backup succeeds or fails, the cold/warm starts of the Managed Switch, port link is up or down, cpu is overloaded, power failure occurs, console port link is up or down, and so on. **auth-fail:** A trap will be sent when any

	| warm-start | console-port-link]	unauthorized user attempts to login. **auto-backup:** A trap will be sent when the auto backup succeeds or fails. **case-fan:** A trap will be sent either when the fan speed of FAN1/FAN2/FAN3 is zero or at/under the threshold (**≦** 5040 RPM). **cold-start:** A trap will be sent when the Managed Switch boots up. **cpu-load:** A trap will be sent when the CPU is overloaded. **cpu-temperature:** A trap will be sent when CPU temperature is over High Temperature Threshold value, CPU temperature returns to the normal status (at or under High Temperature Threshold value), CPU temperature exceeds the range of threshold (0~95 degrees centigrade), or the temperature sensor fails to detect CPU temperature. **digital:** A trap will be sent when the alarm occurs. **mac-limit:** A trap will be sent when any port in which the Mac Limit function is enabled exceeds the specified source MAC address limit. And it will keep sending this trap upon the notification threshold interval setup of MAC Limit function once any port exceeds the specified source MAC address limit continuously. **port-link:** A trap will be sent when the link is up or down. **power-down:** A trap will be sent when the Managed Switch's power is down. **storm-control:** A trap will be sent when broadcast/unknown multicast/unknown unicast packets flood. And it will keep sending this trap upon the notification threshold interval setup of Storm Control function once these packets flood continuously. **system-voltage:** A trap will be sent either when the voltage of ASIC system

		power/ASIC core power/Power A/Power B is at/over the High threshold or at/under the Low threshold. **warm-start:** A trap will be sent when the Managed Switch restarts. **console-port-link:** A trap will be sent when console port link up/link down occurs.
No command		
Switch(config)# no snmp-server trap-type [all | auth-fail | auto-backup | case-fan | cold-start | cpu-load | cpu-temperature | digital |mac-limit | port-link | power-down| storm-control | system-voltage | warm-start | console-port-link]	[all | auth-fail | auto-backup | case-fan | cold-start | cpu-load | cpu-temperature | digital | mac-limit | port-link | power-down| storm-control | system-voltage | warm-start | console-port-link]	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.
Examples of Trap-type		
Switch(config)# snmp-server trap-type all		All types of SNMP traps will be sent.

4. Set up detailed configurations for 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.

Note: The SNMPv3 community user account is generated from “User Command”. (See Section 2.6.27.)

Snmp-server Command	Parameter	Description
Switch(config)# snmp-server user [user_name]	[user_name]	Modify an existing username generated in CLI of “User Command” for a SNMPv3 user.
Switch (config-v3-user-user_name)# authentication [md5 | sha]	[md5 | sha]	Specify the authentication method for the specified SNMPv3 user. **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. **sha(Secure Hash Algorithm):** A 160-bit hash function which resembles the said MD5 algorithm.
Switch (config-v3-user-user_name)# authentication password [password]	[password]	Specify the authentication password for the specified SNMPv3 user. Up to 20 alphanumeric characters can be accepted.
Switch (config-v3-user-user_name)# private [des]	[des]	Specify the method to ensure confidentiality of data. **des(data encryption standard):** An algorithm to encrypt critical information such as message text message signatures…etc.
Switch (config-v3-user-user_name)# private password [password]	[password]	Specify the private password for the specified SNMPv3 user. Up to 20 alphanumeric characters can be accepted.
No Command		
Switch (config-v3-user-user_name)# no authentication		Disable the authentication function for the specified SNMPv3 user.
Switch (config-v3-user-user_name)# no authentication password		Delete the configured authentication password.
Switch (config-v3-user-user_name)# no private		Disable data encryption function.
Switch (config-v3-community-user_name)# no private password		Delete the configured private password.
Show Command		
Switch(config)# show snmp-server user		Show SNMPv3 user configuration.
Switch(config)# show snmp-server user [user_name]	[user_name]	Show the specified SNMPv3 user configuration.
Switch(config-v3-user-user_name)# show		Show the specified SNMPv3 user configuration.

A combination of a security event shown 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	Enables authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms.

MD5 or SHA	Data Encryption Standard(DES)	Enables authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms. What's more, enables DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES standard.

2.6.24 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		Globally enable spanning tree protocol function.
Switch(config)# spanning-tree aggregated-port		Enable Spanning Tree Protocl function on aggregated ports.
Switch(config)# spanning-tree aggregated-port cost [0-200000000]	[0-200000000]	Specify aggregated ports' path cost.
Switch(config)# spanning-tree aggregated-port priority [0-15]	[0-15]	Specify aggregated ports' priority. **0=0, 1=16, 2=32, 3=48, 4=64, 5=80 6=96, 7=112, 8=128, 9=144, 10=160 11=176, 12=192, 13=208, 14=224, 15=240**
Switch(config)# spanning-tree aggregated-port edge		Enable aggregated ports to shift to forwarding state when the link is up. If you know a port is directly connected to an end device (that doesn't support RSTP) then set it as an edge port to ensure maximum performance. This will tell the switch to immediately start

		forwarding traffic on the port and not bother trying to establish a RSTP connection. Otherwise, turn it off.
Switch(config)# spanning-tree aggregated-port p2p [forced_true | forced_false | auto]	[forced_true | forced_false | auto]	Set the aggregated ports to point to point ports (forced_true), 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 non-point to point ports (forced_false).
Switch(config)# spanning-tree delay-time [4-30]	[4-30]	Specify the forward delay time value in seconds. The allowable value is between 4 and 30 seconds.
Switch(config)# spanning-tree hello-time [1-10]	[1-10]	Specify the hello interval value in seconds. The allowable value is between 1 and 10 seconds.
Switch(config)# spanning-tree max-age [6-200]	[6-200]	Specify the maximum age time value in seconds. The allowable value is between 6 and 200 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. **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		Globally disable spanning tree protocol function.
Switch(config)# no spanning-tree aggregated-port		Disable STP on aggregated ports.
Switch(config)# no spanning-tree aggregated-port cost		Reset aggregated ports' cost back to the default.
Switch(config)# no spanning-tree aggregated-port priority		Reset aggregated ports' priority back to the 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 back to non-point to point ports (forced_ false).
Switch(config)# no spanning-tree delay-time		Reset the Forward Delay time back to the default.

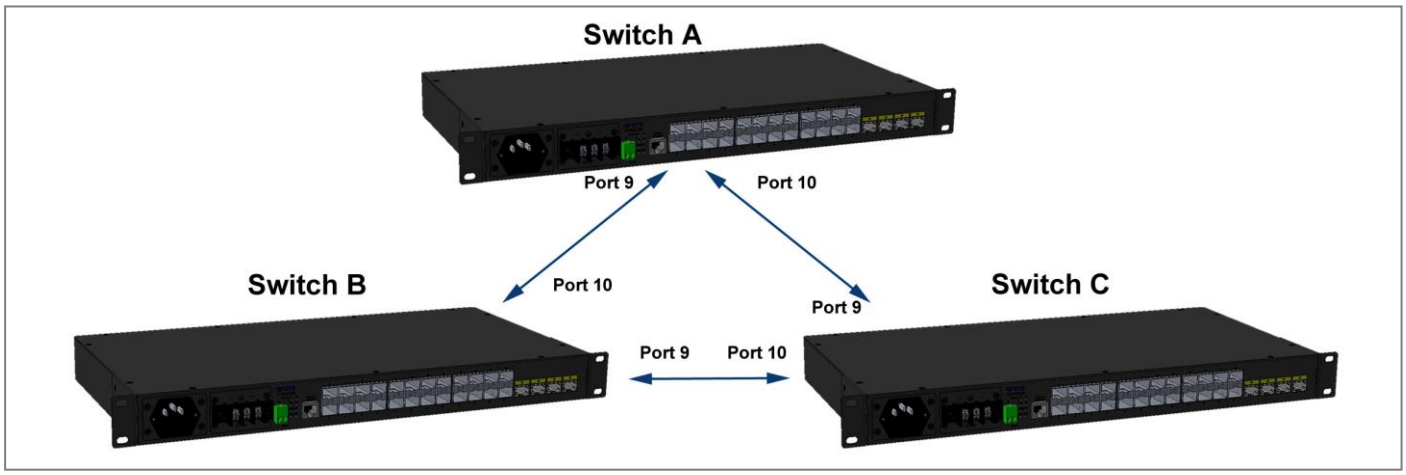
Switch(config)# no spanning-tree hello-time		Reset the Hello Time back to the default.
Switch(config)# no spanning-tree max-age		Reset the Maximum Age back to the default.
Switch(config)# no spanning-tree priority		Reset the priority value on a per switch basis back to the default.
Switch(config)# no spanning-tree version		Reset the RSTP version back to the default.
Show command		
Switch(config)# show spanning-tree		Show RSTP settings on the per switch basis.
Switch(config)# show spanning-tree aggregated-port		Show RSTP settings on aggregated ports.
Switch(config)# show spanning-tree interface		Show each interface's RSTP 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 specified interfaces' RSTP information, including port state, path cost, priority, edge port state, and p2p port state.
Switch(config)# show spanning-tree overview		Show the current root-related information.
Switch(config)# show spanning-tree status		Show each interface and each link aggregation group's (lag) current RSTP port status and 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 [port_list | llag]	[port_list | llag]	Show the specified interface(s) or link aggregation groups' (lag) current RSTP port status and 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..
Examples of Spanning-tree command		**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 10	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 interface(s).
Switch(config-if-PORT-PORT)# spanning-tree cost [0-200000000]	[0-200000000]	Specify the path cost value on the selected interface(s).
Switch(config-if-PORT-PORT)# spanning-tree priority [0-15]	[0-15]	Specify priority value on the selected interface(s). **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		Configure the selected interface(s) as edge port(s).
Switch(config-if-PORT-PORT)# spanning-tree p2p [forced_true| forced_fasle | auto]	[forced_true | forced_fasle | auto]	Set the selected interfaces to non-point to point ports (forced_false) or allow the Managed Switch to detect point to point status automatically (auto). By default, physical ports are set to point to point ports (forced_true).
No command		
Switch(config-if-PORT-PORT)# no spanning-tree		Disable spanning-tree protocol on the selected interface(s).
Switch(config-if-PORT-PORT)# no spanning-tree cost		Reset the cost value back to the default for the selected interface(s).
Switch(config-if-PORT-PORT)# no spanning-tree priority		Reset the priority value back to the default for the selected interface(s).
Switch(config-if-PORT-PORT)# no spanning-tree edge		Reset the selected interface(s) back to non-edge ports.
Switch(config-if-PORT-PORT)# no spanning-tree p2p		Reset the selected interface(s) back to point to point ports (forced_ true).

For RSTP configuration via CLI, we take the following ring network topology composed of 3 sets of FOS-5152 Managed Switches, including Switch A, Switch B and Switch C for example to let the users have a clear understanding of these RSTP commands. Under this network environment, Switch A, Switch B and Switch C will be configured as Table 2-2, and the “Root Switch” will automatically be determined by this network.



Switch	System Priority	Max Age (Secs)	Hello Time (Secs)	Forward Delay (Secs)	Force Version	State	Path Cost	Priority	Edge	P2P
A	4096	6	1	4	Normal	9,10	default	default	default	default
B	4096	6	1	4	Normal	9,10	default	default	default	default
C	4096	6	1	4	Normal	9,10	default	default	default	default

Table 2-2

Below is the complete CLI commands applied to Switch A. Also issue the same commands to Switch B and Switch C accordingly.

	Command	Purpose
STEP1	**configure** **Example:** FOS-5152# config FOS-5152(config)#	**Enter the global configuration mode.**
STEP2	**spanning-tree priority** *system_priority* **Example:** FOS-5152(config)# spanning-tree priority 1 OK !	**In this example, it configures the System Priority of Switch A as “1”. It means the value of the real priority is 4096.**
STEP3	**spanning-tree max-age** *max_age_time* **Example:** FOS-5152(config)# spanning-tree max-age 6 OK !	**In this example, it configures the Max. Age Time of Switch A as “6”.**
STEP4	**spanning-tree hello-time** *hello_interval* **Example:** FOS-5152(config)# spanning-tree hello-time 1 OK !	**In this example, it configures the Hello Time of Switch A as “1”.**

STEP5	**spanning-tree delay-time** *forward_delay_time* **Example:** FOS-5152(config)# spanning-tree delay-time 4 OK !	**In this example, it configures the Forward Delay Time of Switch A as 4.**
STEP6	**spanning-tree version** *stp_version* **Example:** FOS-5152(config)# spanning-tree version normal OK !	**In this example, it configures the STP Version of Switch A as "Normal".**
STEP7	**interface** *port_list* **Example:** FOS-5152(config)# interface 9-10 FOS-5152(config-if-9,10)#	**Specify the Port 9 and Port 10 that you would like to configure to RSTP.**
STEP8	**spanning-tree** **Example:** FOS-5152(config-if-9,10)# spanning-tree OK !	**Enable spanning tree protocol on Port 9 and Port 10.**
STEP9	**spanning-tree cost** *path_cost* **Example:** FOS-5152(config-if-9,10)# spanning-tree cost 0 OK !	**In this example, it configure the port path cost for Port 9 and Port 10 as 0.**
STEP10	**spanning-tree priority** *bridge_priority* **Example:** FOS-5152(config-if-9,10)# spanning-tree priority 0 OK !	**In this example, it configure the port priority for Port 9 and Port 10 as 0. It means the value of the real priority is "0".**
STEP11	**spanning-tree edge** **Example:** FOS-5152(config-if-9,10)# no spanning-tree edge OK !	**In this example, it configure Port 9 and Port 10 as the non-edge ports.**
STEP12	**spanning-tree p2p** *type* **Example:** FOS-5152(config-if-9,10)# spanning-tree p2p forced_true OK !	**In this example, it configures the type of Port 9 and Port 10 as point to point ports.**
STEP13	**exit** **Example:** FOS-5152(config-if-9,10)# exit FOS-5152(config)#	**Return to the global configuration mode.**
STEP14	**exit** **Example:** FOS-5152(config)# exit FOS-5152#	**Return to the Privileged mode.**
STEP15	**write** **Example:** FOS-5152# write Save Config Succeeded!	**Save the running configuration into the startup configuration.**

After completing the RSTP Switch settings for your FOS-5152 switches, you can issue the commands listed below for checking your configuration

Example 1,

FOS-5152(config)# show spanning-tree

```
==============================================================================
RSTP Switch Information
==============================================================================
State              : enabled
System Priority : 4096
Max Age          : 6
Hello Time       : 1
Forward Delay  : 4
Force Version   : normal

FOS-5128(config)#
```

Example 2,

FOS-5152(config)# show spanning-tree aggregated-port

```
==============================================================================
RSTP Aggregated Port Information
==============================================================================
Aggregated State         : disable
Aggregated Path Cost  : 1
Aggregated Priority      : 16
Aggregated Edge         : disable
Aggregated Point2point : forced-false

FOS-5128(config)#
```

Example 3,

FOS-5152(config)# show spanning-tree interface

```
================================================================================
RSTP Port Information
================================================================================
Port   State      Path-Cost   Priority    Edge       Point2point
------ ---------- ----------- ----------  ---------- --------------
1      disable    0           128         disable    forced-true
2      disable    0           128         disable    forced-true
3      disable    0           128         disable    forced-true
4      disable    0           128         disable    forced-true
5      disable    0           128         disable    forced-true
6      disable    0           128         disable    forced-true
7      disable    0           128         disable    forced-true
8      disable    0           128         disable    forced-true

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

9      enable     0           0           disable    forced-true
10     enable     0           0           disable    forced-true
11     disable    0           128         disable    forced-true
12     disable    0           128         disable    forced-true
                        :   :
                        :   :
                        :   :
27     disable    0           128         disable    forced-true
28     disable    0           128         disable    forced-true

FOS-5128(config)#
```

Example 4,

FOS-5152(config)# show spanning-tree overview

```
================================================================================
RSTP overview
================================================================================
Bridge ID     : 4097:00-06-19-00-00-00
Max Age       : 6
Hello Time    : 1
Fwd Delay     : 4
Topology      : Steady
Root ID       : 4097:00-06-19-00-00-00
Root Port     : 0

FOS-5128(config)#
```

Example 5,

FOS-5152(config)# show spanning-tree status

```
================================================================================
RSTP Port Status
================================================================================
Port             :1
Path Cost        :0
Edge Cost        :no
P2P Cost         :yes
Protocol         :RSTP
Role             :Non-STP
Port State       :Non-STP
------------------------------------------
Packet Statistics
------------------------------------------
RSTP Received          :0
RSTP Transmitted       :0
STP Received           :0
STP Transmitted        :0
TCN Received           :0
TCN Transmitted        :0
Illegal Received       :0
Unknown Received       :0

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

                  :   :
                  :   :
                  :   :

Port             : 9
Path Cost        : 2000000
Edge Cost        : no
P2P Cost         : yes
Protocol         : RSTP
Role             : Disable
Port State       : Disable
------------------------------------------
Packet Statistics
------------------------------------------
RSTP Received          : 0
RSTP Transmitted       : 0
STP Received           : 0
STP Transmitted        : 0
TCN Received           : 0
TCN Transmitted        : 0
Illegal Received       : 0
Unknown Received       : 0

FOS-5128(config)#
```

```
Port       : 10
Path Cost   : 2000000
Edge Cost   : no
P2P Cost    : yes
Protocol    : RSTP
Role        : Disable
Port State  : Disable
---------------------------------------------
Packet Statistics
---------------------------------------------
RSTP Received    :0
RSTP Transmitted :0
STP Received        :0
STP Transmitted    :0
TCN Received        :0
TCN Transmitted     :0
Illegal Received       :0
Unknown Received  :0
                :   :
                :   :
                :   :


Port           : lag8
Path Cost   : 0
Edge Cost   : no
P2P Cost    : no
Protocol      : RSTP
Role           : Non-STP
Port State    : Non-STP
---------------------------------------------
Packet Statistics
---------------------------------------------
RSTP Received     : 0
RSTP Transmitted  : 0
STP Received        : 0
STP Transmitted    : 0
TCN Received       : 0
TCN Transmitted    : 0
Illegal Received      : 0
Unknown Received : 0


FOS-5128(config)#
```

2.6.25 Switch Command

Switch Command	Parameter	Description
Switch(config)# switch mtu [1518-9600]	[1518-9600]	Specify the maximum frame size in bytes. The allowable MTU value is between 1518 and 9600 bytes.
Switch(config)# switch statistics polling port [1-28]	[1-28]	Specify the number of ports for data acquisition in each polling.
Switch(config)# switch statistics polling interval [1-600]	[1-600] (Unit:1/10secs)	Specify the time interval between each polling.
No command		
Switch(config)# no switch mtu		Reset MTU size back to the default. (9600 bytes)
Switch(config)# no switch statistics polling port		Reset the number of ports for data acquisition in each polling back to the default. (12 ports)
Switch(config)# no switch statistics polling interval		Reset the time interval between each polling back to the default. (60 in 1/10 seconds)
Show command		
Switch(config)# show switch mtu		Show the current the maximum frame size configuration.
Switch(config)# show switch statistics		Show the current configuration of polling port number and time interval between each polling.
Examples of Switch command		
Switch(config)# switch mtu 9600		Set the maximum transmission unit to 9600 bytes.

2.6.26 Switch-info Command

1. Set up the Managed Switch's basic information, including company name, hostname, system name, etc..

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 Managed Switch.
Switch(config)# switch-info cpu-loading-threshold [10-3000]	[10-3000] (Unit: 1/100)	Specify CPU loading threshold.
Switch(config)# switch-info cpu-temperature notification continuous-alarm		Enable the continuous alarm message sending function for CPU temperature of the system.

Switch(config)# switch-info cpu-temperature notification threshold [0-95]	[0-95]	Specify a value as CPU temperature threshold (Vaild Range: 0~95 degrees centigrade).
Switch(config)# switch-info cpu-temperature notification interval [120-86400]	[120-86400]	Specify the time interval of sending cpu-temperature alarm message in seconds.
Switch(config)# switch-info dhcp-vendor-id [dhcp_vendor_id]	[dhcp_vendor_id]	Enter the user-defined DHCP vendor ID, and up to 55 alphanumeric characters can be accepted. Please make sure you have an exact DHCP Vendor ID with the value specified in “vendor-classes” in your dhcpd.conf file. For detailed information, see Appendix B.
Switch(config)# switch-info host-name [host_name]	[host_name]	Enter a new hostname, up to 30 alphanumeric characters, for this Managed Switch. By default, the hostname prompt shows the model name of this Managed Switch. You can change the factory-assigned hostname prompt to the one that is easy for you to identify during network configuration and maintenance.
Switch(config)# switch-info system-contact [sys_contact]	[sys_contact]	Enter the contact information, up to 55 alphanumeric characters, for this Managed switch.
Switch(config)# switch-info system-location [sys_location]	[sys_location]	Enter a brief description of the Managed Switch location, up to 55 alphanumeric characters, for this Managed Switch. Like the name, the location is for reference only, for example, “13th Floor”.
Switch(config)# switch-info system-name [sys_name]	[sys_name]	Enter a unique name, up to 55 alphanumeric characters, for this Managed Switch. Use a descriptive name to identify the Managed Switch in relation to your network, for example, “Backbone 1”. This name is mainly used for reference only.
No command		
Switch(config)# no switch-info company-name		Reset the entered company name back to the default.
Switch(config)# no switch-info cpu-loading-threshold		Reset CPU loading threshold back to the default.
Switch(config)# no switch-info cpu-temperature notification continuous-alarm		Disable the continuous alarm message sending function for CPU temperature of the system.
Switch(config)# no switch-info cpu-temperature notification threshold		Reset CPU temperature threshold back to the default. (80 degrees centigrade)
Switch(config)# no switch-info cpu-temperature notification interval		Reset the time interval of sending cpu-temperature alarm message back to the default. (600 seconds)
Switch(config)# no switch-info dhcp-vendor-id		Reset the entered DHCP vendor ID information back to the default.
Switch(config)# no switch-info host-name		Reset the hostname back to the default.

Switch(config)# no switch-info system-contact	Reset the entered system contact information back to the default.
Switch(config)# no switch-info system-location	Reset the entered system location information back to the default.
Switch(config)# no switch-info system-name	Reset the entered system name information back to the default.
Show command	
Switch(config)# show switch-info	Show the switch-related information including company name, system contact, system location, system name, model name, firmware version and so on.
Switch(config)# show switch-info cpu-mem-statistics	Show the current CPU & memory usage rate of the switch.
Switch(config)# show switch-info cpu-temperature	Show the current cpu-temperature alarm notification configuration and CPU temperature status.
Switch(config)# show switch-info fan-speed	Show the current fan speed in unit of RPM and stauts of FAN1/FAN2/FAN3.
Switch(config)# show switch-info system-voltage	Show the current voltages and status of system's internal powers such as ASIC system power, ASIC core power and Power A & B **Note: Power B is only available in models with two fixed power modules.**
Examples of Switch-info	
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 field to "info@compnay.com".
Switch(config)# switch-info system-location 13thfloor	Set the system location field to "13thfloor".
Switch(config)# switch-info system-name backbone1	Set the system name field to "backbone1".
Switch(config)# switch-info host-name edgeswitch10	Change the Managed Switch's hostname into "edgeswitch10".

2.6.27 Syslog Command

Syslog Command	Parameter	Description
Switch(config)# syslog		Enable the system log function.
Switch(config)# syslog facility [0-7]	[0-7]	Specify a facility code (Local 0~Local 7) to a specific device for classifying the syslog message provided by different devices.
Switch(config)# syslog logging-type terminal-history		Enable Terminal-history log function.
Switch(config)# syslog server1 [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F :G:H]	Specify the primary system log server's IPv4/IPv6 address.
Switch(config)# syslog server2 [A.B.C.D |	[A.B.C.D | A:B:C:D:E:F	Specify the secondary system log server's IPv4/IPv6 address.

A:B:C:D:E:F:G:H]	:G:H]	
Switch(config)# syslog server3 [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F :G:H]	Specify the third system log server's IPv4/IPv6 address.
No command		
Switch(config)# no syslog		Disable the system log function.
Switch(config)# no syslog facility		Reset the facility code back to the default. (Local 0)
Switch(config)# no syslog logging-type terminal-history		Disable Terminal-history log function.
Switch(config)# no syslog server1		Delete the primary system log server's IPv4/IPv6 address.
Switch(config)# no syslog server2		Delete the secondary system log server's IPv4/IPv6 address.
Switch(config)# no syslog server3		Delete the third system log server's IPv4/IPv6 address.
Show command		
Switch(config)# show syslog		Show the current system log configuration.
Examples of Syslog command		
Switch(config)# syslog		Enable the system log function.
Switch(config)# syslog server1 192.180.2.1		Set the primary system log server's IP address to 192.168.2.1.
Switch(config)# syslog server2 192.168.2.2		Set the secondary system log server's IP address to 192.168.2.2.
Switch(config)# syslog server3 192.168.2.3		Set the third system log server's IP address to 192.168.2.3.

2.6.28 Terminal Length Command

Terminal Length Command	Parameter	Description
Switch(config)# terminal length [0-512]	[0-512]	Specify the number of event lines that will show up each time on the screen for "show running-config", "show default-config" and "show start-up-config" commands. ("0" stands for no pausing.)
No Command		
Switch(config)# no terminal length		Reset the terminal length back to the default (20).
Show Command		
Switch(config)# show terminal		Show the current configuration of terminal length.

2.6.29 User Command

Create/modify a new login account to prevent unauthorized operations of the Managed Switch from malicious users.

User Command	Parameter	Description
Switch(config)# user name [user_name]	[user_name]	Create/modify a user account. The authorized user login name is up to 20 alphanumeric characters. Up to 10 users can be registered.
Switch(config)# user password-encryption md5		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. ***NOTE:*** *1. The acquired hashed password from backup config file is not applicable for user login on CLI/Web interface.* *2. We strongly recommend not to alter off-line Auth Method setting in backup configure file.* *3. If Auth-Method is enabled and do firmware downgrade, users must reset default config.*
Switch(config-user-NAME)# active		Activate the specified user account.
Switch(config-user-NAME)# description [description]	[description]	Enter the brief description for the specified user account. Up to 35 alphanumeric characters can be accepted.
Switch(config-user-NAME)# level [admin | rw | ro]	[admin | rw | ro]	Specify this user's access privilege level. **admin (administrator):** Own the full-access right, including maintaining user account & system information, loading factory settings, etc.. **rw (read & write):** Own the partial-access right, unable to modify user account & system information and load factory settings. **ro (read only):** Read-Only access privilege.
Switch(config-user-NAME)# password [password]	[password]	Enter the password, up to 20 alphanumeric characters, for the specified user account.
No command		
Switch(config)# no user name [user_name]	[user_name]	Delete the specified user account.

Switch(config)# no user password-encryption		Disable MD5(Message-Digest Algorithm).
Switch(config-user-NAME)# no active		Deactivate the selected user account.
Switch(config-user-NAME)# no description		Remove the configured description for the specified user account.
Switch(config-user-NAME)# no level		Reset the access privilege level back to the default (Read Only).
Switch(config-user-NAME)# no password		Remove the configured password for the specified user account.
Show command		
Switch(config)# show user		Show user account configuration.
Switch(config)# show user name		List all user accounts.
Switch(config)# show user name [user_name]	[user_name]	Show the specific account's configuration.
Switch(config-user-NAME)# show		Show the specific account's configuration.
Examples of User command		
Switch(config)# user name miseric		Create a new login account "miseric".
Switch(config-user-miseric)# description misengineer		Add a description to this new account "miseric".
Switch(config-user-miseric)# password mis2256i		Set up a password for this new account "miseric"
Switch(config-user-miseric)# level rw		Set this user account's privilege level to "read and write".

2.6.30 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. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

2.6.30.1 Port-Based VLAN

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

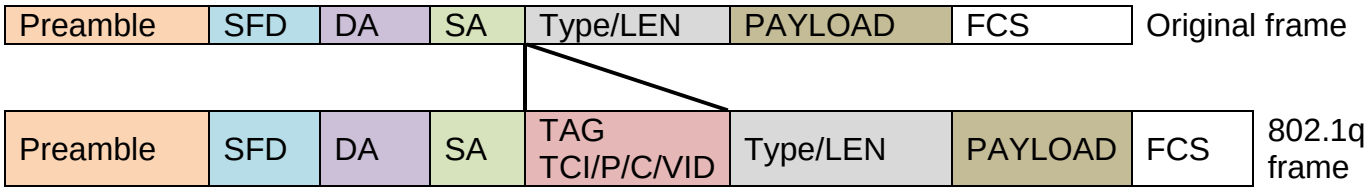
Since source addresses of the packets are listed in MAC address table of specific VLAN (except broadcast/multicast packets), in every VLAN the traffic between two ports will be two-way without restrictions.

2.6.30.2 802.1Q VLAN

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 to 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 8100 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 Canonical format - Ethernet 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 to understand.

- **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**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. 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**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

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

- **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, 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. These types of ports are 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 simultaneously with the 802.1Q tagged packets. 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. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.

- **DOT1Q-Tunnel Mode :**
  Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification.

  Using the IEEE 802.1Q tunneling feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using IEEE 802.1Q tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets. A port configured to support IEEE 802.1Q tunneling is called a *tunnel port*. When you configure tunneling, you assign a tunnel port to a VLAN ID that is dedicated to tunneling. Each customer requires a separate service-provider VLAN ID, but that VLAN ID supports all of the customer’s VLANs.

- **Selective Q-in-Q Mode :**
  Selective Q-in-Q mode is specially designed for the port that enabled Selective Q-in-Q function to separate users & service by encapsulating VLAN ID

- Customer traffic tagged in the normal way with appropriate VLAN IDs comes from an IEEE 802.1Q trunk port on the customer device and into a tunnel port on the service-provider edge

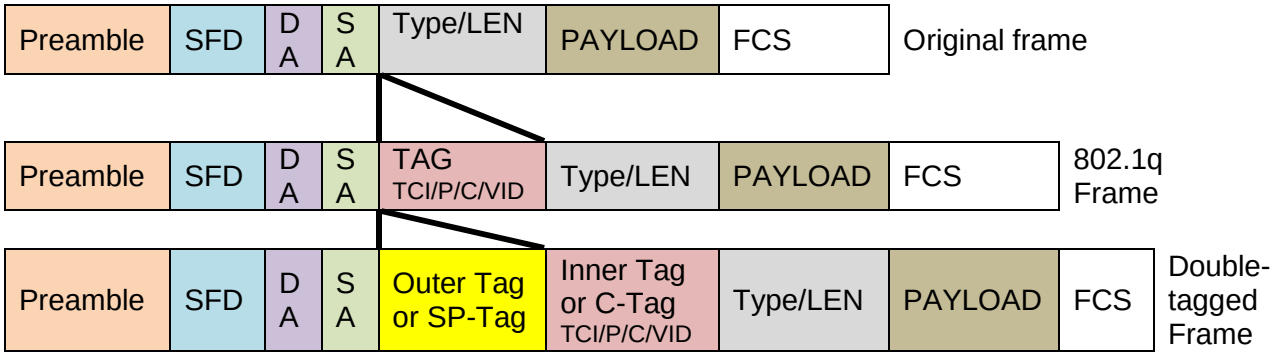
switch. The link between the customer device and the edge switch is asymmetric because one end is configured as an IEEE 802.1Q trunk port, and the other end is configured as a tunnel port. You assign the tunnel port interface to an access VLAN ID that is unique to each customer.

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 VID 10,11 and 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 VID 10,11 and 12 PortX receives **Untagged** packets and add PVID 20
Trunk-VLAN = 10,11,12 Access-VLAN = 20 **Mode = Dot1q-tunnel**	PortX is a **Dot1q-tunnel Port** PortX's **VID** is ignored. PortX's **PVID** is 20 PortX sends **Untagged** or **Tagged** packets VID 20 PortX receives **Untagged** and **Tagged** packets and add PVID 20(outer tag)
Trunk-VLAN = 10,11,12 Access-VLAN = 20 **Mode = Selective Q-in-Q**	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 VID 10,11 and 12 PortX receives **Untagged** packets and add PVID 20

2.6.30.3 Introduction to Q-in-Q (DOT1Q-Tunnel)

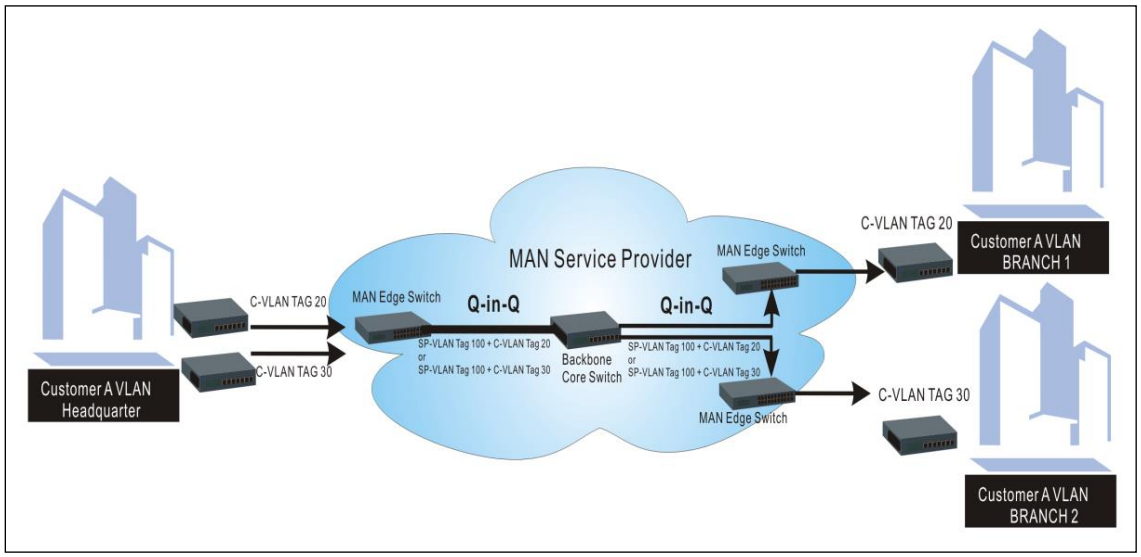
The IEEE 802.1Q double tagging VLAN is also referred to as Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1q VLAN space by tagging the inner tagged packets. In this way, a "double-tagged" frame is created so as to separate customer traffic within a service provider network. As shown below in "Double-Tagged Frame" illustration, an outer tag is added between source destination and inner tag at the provider network's edge. This can support C-VLAN (Customer VLAN) over Metro Area Networks and ensure complete separation between traffic from different user groups. Moreover, the addition of double-tagged space increases the number of available VLAN tags which allow service providers to use a single SP-VLAN (Service Provider VLAN) tag per customer over the Metro Ethernet network.



Double-Tagged Frame Format

As shown below in "Q-in-Q Example" illustration, Headquarter A wants to communicate with Branch 1 that is 1000 miles away. One common thing about these two locations is that they have the same VLAN ID of 20, called C-VLAN (Customer VLAN). Since customer traffic will be routed to service provider's backbone, there is a possibility that traffic might be forwarded insecurely, for example due to the same VLAN ID used. Therefore, in order to get the information from Headquarter to Branch 1, the easiest way for the carrier to ensure security to customers is to encapsulate the original VLAN with a second VLAN ID of 100. This second VLAN ID is known as SP-VLAN (Service Provider VLAN) that is added as data enters the service provider's network and then removed as data exits. Eventually, with the help of SP-Tag, the information sent from Headquarter to Branch 1 can be delivered with customers' VLANs intactly and securely.

Q-in-Q Example



1. Use "Interface" command to configure a group of ports' 802.1q/Port-based 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 pvid [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan trunk-vlan [1-	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).

4094]		
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode access		Set the selected ports to the access mode (untagged).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk		Set the selected ports to the trunk mode (tagged).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk native		Enable native VLAN for untagged traffic on the selected ports. (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 dot1q-vlan mode dot1q-tunnel		Set the selected ports to dot1q-tunnel (Q-in-Q) mode. (Tagged and untagged)
Switch(config-if-PORT-PORT)# vlan port-based [name]	[name]	Set the selected ports to a specified port-based VLAN. **Note :** **Need to create a port-based VLAN group under the VLAN global configuration mode before joining it.**
No command		
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan pvid		Reset the selected ports' PVID back to the default setting.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan mode		Reset the selected ports' 802.1q VLAN mode setting back to the default (Access Mode).
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the specified trunk VLAN ID from the selected ports.
Switch(config-if-PORT-PORT)# no vlan port-based [name]	[name]	Remove the selected ports from the specified port-based VLAN.

2. Create/Modify an 802.1q VLAN and a management VLAN rule or create a port-based VLAN group.

VLAN dot1q Command	Parameter	Description
Switch(config)# vlan dot1q-vlan [1-4094]	[1-4094]	Enter a VLAN ID number to create a new 802.1q VLAN or modify an existing 802.1q VLAN.
Switch(config-vlan-ID)# name [vlan_name]	[vlan_name]	Specify a descriptive name for the created VLAN ID, maximun 15 characters.
Switch(config)# vlan management-vlan [1-4094]	[1-4094]	Enter the management VLAN ID.

management-port [port_list] mode [access | trunk | trunk-native]	[port_list]	Specify the management port number.
	[access | trunk | trunk-native]	Specify whether the management port is in trunk or access mode. **"trunk" mode:** Set the selected ports to tagged. **"access" mode:** Set the selected ports to untagged. **"trunk-native" mode:** Set the selected ports to tagged or untagged.
Switch(config)# vlan port-based [name]	[name]	Specify a descriptive name for the port-based VLAN you would like to create, maximun 15 characters.
Switch(config)# vlan port-based [name] include-cpu		Include CPU into the specified Port-Based VLAN.
Switch(config)# vlan dot1q-tunnel ethertype [0xWXYZ]	[0xWXYZ]	Configure outer VLAN's ethertype. (Range: 0x0000~FFFF)
No command		
Switch(config-vlan-ID)# no name		Remove the descriptive name for the specified VLAN ID.
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 the specified Port-Based VLAN.
Switch(config)# no vlan dot1q-tunnel ethertype		Reset outer VLAN's ethertype back to the default setting. (9100)
Switch(config)# no vlan dot1q-vlan [1-4094]	[1-4094]	Remove the specified VLAN ID from the Trunk VLAN table.
Show command		
Switch(config)# show vlan		Show IEEE 802.1q VLAN table.
Switch(config-vlan-ID)# show		Show the membership status of the specified 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 specific ports' VLAN assignment and VLAN mode.
Switch(config)# show vlan port-based		Show port-based VLAN table.
Exit command		
Switch(config-vlan-ID)# exit		Return to Global Configuration mode.
Examples of Port-based VLAN		
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 as management ports.

3. Set up VLAN ID translation (or VLAN mapping).

Besides the aforementioned ways of creating VLANs, another way to establish the translated VLANs is to configure VLAN ID translation (or VLAN mapping) on trunk ports connected to a customer network to map the original VLANs to the translated VLANs. Through this VLAN ID translation, it will save much effort in massive Ethernet network deployments.

Packets entering the trunk port are mapped to a translated VLAN based on the port number and the original VLAN ID of the packet. In a typical metro deployment, VLAN mapping takes place on user network interfaces. Because the VLAN ID is mapped to the translated VLAN on ingress, all forwarding operations on the Managed Switch are performed with the usage of the translated VLAN information rather than the original VLAN information.

VLAN Mapping Command	Parameter	Description
Switch(config)# vlan mapping		Enable VLAN Translation function globally.
Switch(config)# vlan mapping name [name] interface [port_number] original-vid [1-4094] mapped-vid [1-4094] priority [0-7]	[name]	Specify a descriptive name for the VLAN mapping rule. Up to 32 alphanumeric characters can be accepted.
	[port_number]	Specify one preferred trunk port used for the VLAN ID translation. **Note: For more details on turnk port settings, see Section 2.6.28.**
	[1-4094]	Specify the original VLAN ID entering the switch from the customer network for the VLAN ID translation.Valid range: 1-4094. **Note: Different original VIDs belonging to the specific port cannot be translated into the same Mapped VID.**
	[1-4094]	Specify the preferred VLAN ID that the assigned original VID will be translated. Valid range: 1-4094. **Note: Different Mapped VIDs cannot be assigned to the trunk port with the same original VID.**
	[0-7]	Specify the preferred priority bit value to replace the original priority level in the tagged packets. Valid range: 0~7.
No command		
Switch(config)# no vlan mapping		Disable VLAN Translation function globally.
Switch(config)# no vlan mapping name [name]	[name]	Remove the specified mapping rule by name from the VLAN mapping rule table.
Show command		
Switch(config)# show vlan mapping		Show the current VLAN Translation configuration.

4. Set up Selective Q-in-Q.

Selective Q-in-Q, an extension of DOT1Q-Tunnel, is implemented based on both interfaces and VLAN IDs. An interface configured with Selective Q-in-Q can forward packets based on a single VLAN tag or double VLAN tags. Additionally, Selective Q-in-Q adds different outer VLAN tags to packets carrying different inner VLAN IDs. It marks the outer 802.1p fields and adds different outer VLAN tags to packets upon the 802.1p fields in inner VLAN tags.

In the VLAN application, not only does Selective Q-in-Q make a distinction between service provider's and customer's networks but provides extensive service functions as well as the more flexible networking.

VLAN Mapping Command	Parameter	Description
Switch(config)# vlan selective-qinq		Enable Selective Q-in-Q function globally.
Switch(config)# vlan selective-qinq tpid [1-3] ethertype [0xWXYZ]	[1-3]	Configure outer VLAN's EtherType for the specified TPID (Tag Protocol Identifier). The system supports 4 TPIDs. The default configuration of these TPIDs is as follows: **Default TPID** = 8100 (A fixed value that cannot be changed.) **TPID 1** = The default setting is 9100. (Use the same EtherType as Dot1q Tunnel) **TPID 2** = The default setting is 88A8. **TPID 3** = The default setting is 9200.
	[0xWXYZ]	Vaild outer VLAN's EtherType range: 0000~FFFF.
Switch(config)# vlan selective-qinq name [name] interface [port_number] inner-vid [1-4094] outer-vid [1-4094] tpid [default | 1-3] priority [0-7]	[name]	Specify a descriptive name for the specific Selective Q-in-Q rule. Up to 32 alphanumeric characters can be accepted.
	[port_number]	Specify the preferred trunk-native port(s) (e.g. 1,2,3-7) used for the specific Selective Q-in-Q rule. **Note 1 : Selective Q-in-Q based on the VLAN ID can only be enabled on trunk-native interfaces in the inbound direction.** **Note 2 : For more details on trunk-native port settings, see Section 2.6.28**.

	[1-4094]	Specify the customer VLAN ID (C-VLAN) that enters the switch from customer's network. You can enter one or a consecutive string of VLAN IDs, for example, 100 or 100-110. Valid range: 1-4094.
	[1-4094]	Specify the outer VLAN ID (SP-VLAN) of the service provider network. Valid range: 1-4094.
	[default | 1-3]	Specify the preferred TPID to the specific Selective Q-in-Q rule.
	[0-7]	Set up 802.1p bit value for the outer VID. Valid range: 0~7.
No command		
Switch(config)# no vlan selective-qinq		Disable Selective Q-in-Q function globally.
Switch(config)# no vlan selective-qinq name [name]	[name]	Remove the specified Selective Q-in-Q rule by name from the Selective Q-in-Q rule table
Show command		
Switch(config)# show vlan selective-qinq all		Show the current all Selective Q-in-Q configuration.
Switch(config)# show vlan selective-qinq all [interface | inner-vid | outer-vid]	[interface | inner-vid | outer-vid]	Show the current all Selective Q-in-Q configuration sorted by specific option.
Switch(config)# show vlan selective-qinq interface [port_list]	[port_list]	Show the current Selective Q-in-Q configuration of the specified port(s).
Switch(config)# show vlan selective-qinq inner-vid [VID_list]	[VID_list]	Show the current Selective Q-in-Q configuration of the specified inner VLAN ID(s).
Switch(config)# show vlan selective-qinq outer-vid [VID_list]	[VID_list]	Show the current Selective Q-in-Q configuration of the specified outer VLAN ID(s).
Switch(config)# show vlan selective-qinq tpid		Show the current all TPIDs' configuration.

For 802.1q VLAN configuration via CLI, we will demostrate the following four examples to have the users realize the commands we mentioned above.

Example 1,

We will configure FOS-5152 Managed Switch via CLI as the Table 2-3 listed.

Name	Ports	Mode	PVID	VID
Sales	1-2	Trunk	Default	10,20
RD	3-4	Trunk-native	50	30,40
SQA	5-6	Access	60	N/A
PME	7-8	Access	70	N/A

Table 2-3

1. Create 802.1q VLAN IDs.

FOS-5152(config)# interface 1-2	Enter port 1 to port 2's interface mode.
FOS-5152(config-if-1,2)# vlan dot1q-vlan trunk-vlan 10, 20	Set port 1 to port 2's Trunk-VLAN ID (VID) to 10 and 20.
FOS-5152(config-if-1,2)# vlan dot1q-vlan mode trunk	Set the selected ports to Trunk Mode (tagged).
FOS-5152(config-if-1,2)# exit	Exit current ports interface mode.
FOS-5152 (config)# interface 3-4	Enter port 3 to 4's interface mode.
FOS-5152(config-if-3,4)# vlan dot1q-vlan pvid 50	Set port 3 to port 4's Access-VLAN ID (PVID) to 50.
FOS-5152(config-if-3,4)# vlan dot1q-vlan trunk-vlan 30,40	Set port 3 to port 4's Trunk-VLAN ID (VID) to 30 and 40.
FOS-5152(config-if-3,4)# vlan dot1q-vlan mode selective-qinq	Set the selected ports to Selective Q-in-Q Mode (tagged and untagged).
FOS-5152(config-if-3,4)# exit	Exit current ports interface mode.
FOS-5152 (config)# interface 5-6	Enter port 5 to port 6's interface mode.
FOS-5152(config-if-5,6)# vlan dot1q-vlan pvid 60	Set port 5 to port 6's Access-VLAN ID (PVID) to 60.
FOS-5152(config-if-5,6)# vlan dot1q-vlan mode access	Set the selected ports to Access Mode (untagged).
FOS-5152(config-if-5,6)# exit	Exit current ports interface mode.
FOS-5152(config)# interface 7-8	Enter port 7 to port 8's interface mode.
FOS-5152(config-if-7,8)# vlan dot1q-vlan pvid	Set port 7 to port 8's Access-VLAN ID

70	(PVID) to 70.
FOS-5152(config-if-7,8)# vlan dot1q-vlan mode access	Set the selected ports to Access Mode (untagged).
FOS-5152(config-if-7,8)# exit	Exit current ports interface mode.

2. Modify 802.1q VLAN IDs' names.

FOS-5152(config)# vlan dot1q-vlan 10	Enter VLAN 10.
FOS-5152 (config-vlan-10)# name Sales	Specify "Sales" as the name for VLAN 10.
FOS-5152 (config-vlan-10)# exit	Exit VLAN 10.
FOS-5152(config)# vlan dot1q-vlan 20	Enter VLAN 20.
FOS-5152(config-vlan-20)# name Sales	Specify "Sales" as the name for VLAN 20.
FOS-5152(config-vlan-20)# exit	Exit VLAN 20.
FOS-5152(config)# vlan dot1q-vlan 30	Enter VLAN 30.
FOS-5152(config-vlan-30)# name RD	Specify "RD" as the name for VLAN 30.
FOS-5152(config-vlan-30)# exit	Exit VLAN 30.
FOS-5152(config)# vlan dot1q-vlan 40	Enter VLAN 40.
FOS-5152(config-vlan-40)# name RD	Specify "RD" as the name for VLAN 40.
FOS-5152(config-vlan-40)# exit	Exit VLAN 40.
FOS-5152(config)# vlan dot1q-vlan 50	Enter VLAN 50.
FOS-5152(config-vlan-50)# name RD	Specify "RD" as the name for VLAN 50.
FOS-5152(config-vlan-50)# exit	Exit VLAN 50.
FOS-5152(config)# vlan dot1q-vlan 60	Enter VLAN 60.
FOS-5152(config-vlan-60)# name SQA	Specify "SQA" as the name for VLAN 60.
FOS-5152(config-vlan-60)# exit	Exit VLAN 60.
FOS-5152 (config)# vlan dot1q-vlan 70	Enter VLAN 70.
FOS-5152 (config-vlan-70)# name PME	Specify "PME" as the name for VLAN 70.
FOS-5152 (config-vlan-70)# exit	Exit VLAN 70.

Example 2,

We will configure two sets of FOS-5152 Managed Switch(including #1 FOS-5152 and #2 FOS-5152) via CLI as the Table 2-4 listed.

Port No.	Mode	Access-VLAN (PVID)	Trunk-VLAN (VID)	EtherType
1	Dot1q-tunnel	10	1	9100
2	Trunk	1	10	9100
3	Dot1q-tunnel	20	1	9100
4	Dot1q-tunnel	20	1	9100

Table 2-4

Below is the complete CLI commands applied to #1 FOS-5152. Also issue the same commands to #2 FOS-5152.

	Command	Purpose
STEP1	**configure** **Example:** FOS-5152# config FOS-5152(config)#	**Enter the global configuration mode.**
STEP2	**vlan dot1q-tunnel ethertype** *0xWXYZ* **Example:** FOS-5152(config)# vlan dot1q-tunnel ethertype 9100 OK !	**In this example, it configures the dot1q-tunnel ethertype value as "9100"**
STEP3	**interface** *port_list* **Example:** FOS-5152(config)# interface 1 FOS-5152 (config-if-1)#	**Specify Port 1 that you would like to configure it as dot1q-tunnel port.**
STEP4	**vlan dot1q-vlan access-vlan** *vlan_id* **Example:** FOS-5152(config-if-1)# vlan dot1q-vlan pvid 10 OK !	**In this example, it configures Access-VLAN ID "10" to Port 1.**
STEP5	**vlan dot1q-vlan mode** *dot1q-tunnel* **Example:** FOS-5152(config-if-1)# vlan dot1q-vlan mode dot1q-tunnel OK !	**Configure Port 1's VLAN mode as "dot1q-tunnel" mode.**
STEP6	**exit** **Example:** FOS-5152(config-if-1)# exit FOS-5152(config)#	**Return to the global configuration mode.**
STEP7	**interface** *port_list* **Example:** FOS-5152(config)# interface 2 FOS-5152(config-if-2)#	**Specify Port 2 that you would like to configure it as Trunk port.**
STEP8	**vlan dot1q-vlan trunk-vlan** *vlan_id* **Example:** FOS-5152(config-if-2)# vlan dot1q-vlan trunk-vlan 10 OK !	**In this example, it configures Trunk-VLAN ID "10" to Port 2.**
STEP9	**v lan dot1q-vlan mode** *trunk* **Example:** FOS-5152(config-if-2)# vlan dot1q-vlan mode trunk OK !	**Configure Port 2's VLAN mode as "Trunk" mode.**
STEP10	**no vlan dot1q-vlan trunk-vlan** *vlan_id*	**Remove the Trunk-VLAN ID "1" from Port 2.**

	Example: FOS-5152(config-if-2)# no vlan dot1q-vlan trunk-vlan 1 OK !	
STEP10	**exit** **Example:** FOS-5152 (config-if-2)# exit FOS-5152 (config)#	**Return to the global configuration mode.**
STEP11	**interface** *port_list* **Example:** FOS-5152(config)# interface 3 FOS-5152 (config-if-3)#	**Specify Port 3 that you would like to configure it as Dot1q-Tunnel port.**
STEP12	**vlan dot1q-vlan access-vlan** *vlan_id* **Example:** FOS-5152(config-if-3)# vlan dot1q-vlan pvid 20 OK !	**In this example, it configures Access-VLAN ID "20" to Port 3.**
STEP13	**vlan dot1q-vlan mode** *dot1q-tunnel* **Example:** **FOS-5152** (config-if-3)# vlan dot1q-vlan mode dot1q-tunnel OK !	**Configure Port 3's VLAN mode as "dot1q-tunnel" mode.**
STEP14	**exit** **Example:** FOS-5152 (config-if-3)# exit FOS-5152 (config)#	**Return to the global configuration mode.**
STEP15	**interface** *port_list* **Example:** FOS-5152(config)# interface 4 FOS-5152(config-if-4)#	**Specify Port 4 that you would like to configure it as dot1q-tunnel port.**
STEP16	**vlan dot1q-vlan access-vlan** *vlan_id* **Example:** FOS-5152(config-if-4)# vlan dot1q-vlan pvid 20 OK !	**In this example, it configures Access-VLAN ID "20" to Port 4.**
STEP17	**vlan dot1q-vlan mode** *dot1q-tunnel* **Example:** **FOS-5152** (config-if-4)# vlan dot1q-vlan mode dot1q-tunnel OK !	**Configure Port 4's VLAN mode as "dot1q-tunnel" mode.**
STEP18	**exit** **Example:** FOS-5152 (config-if-4)# exit FOS-5152 (config)#	**Return to the global configuration mode.**
STEP19	**exit** **Example:**	**Return to the Privileged mode.**

	FOS-5152(config)# exit FOS-5152#	
STEP20	**write** **Example:** FOS-5152# write Save Config Succeeded!	**Save the running configuration into the startup configuration.**

After completing the VLAN settings for your FOS-5152 switches, you can issue the commands listed below for checking your configuration

For Example,

FOS-5152(config)# show vlan interface

```
==================================================================
IEEE 802.1q Tag VLAN Interface
==================================================================
CPU VLAN ID                : 1
Dot1q-Tunnel EtherType :  0x9100

Port   P-Bit   Port VLAN Mode PVID Trunk-vlan
----  --------- ---------------------- ------- ----------------
  1         0    dot1q tunnel        10     1
  2         0    trunk                 1    10
  3         0    dot1q tunnel        20     1
  4         0    dot1q tunnel        20     1
  5         0    access                1     1
  6         0    access                1     1
                        …
 27         0     access               1    1
 28         0     access               1    1

FOS-5128(config)#
```

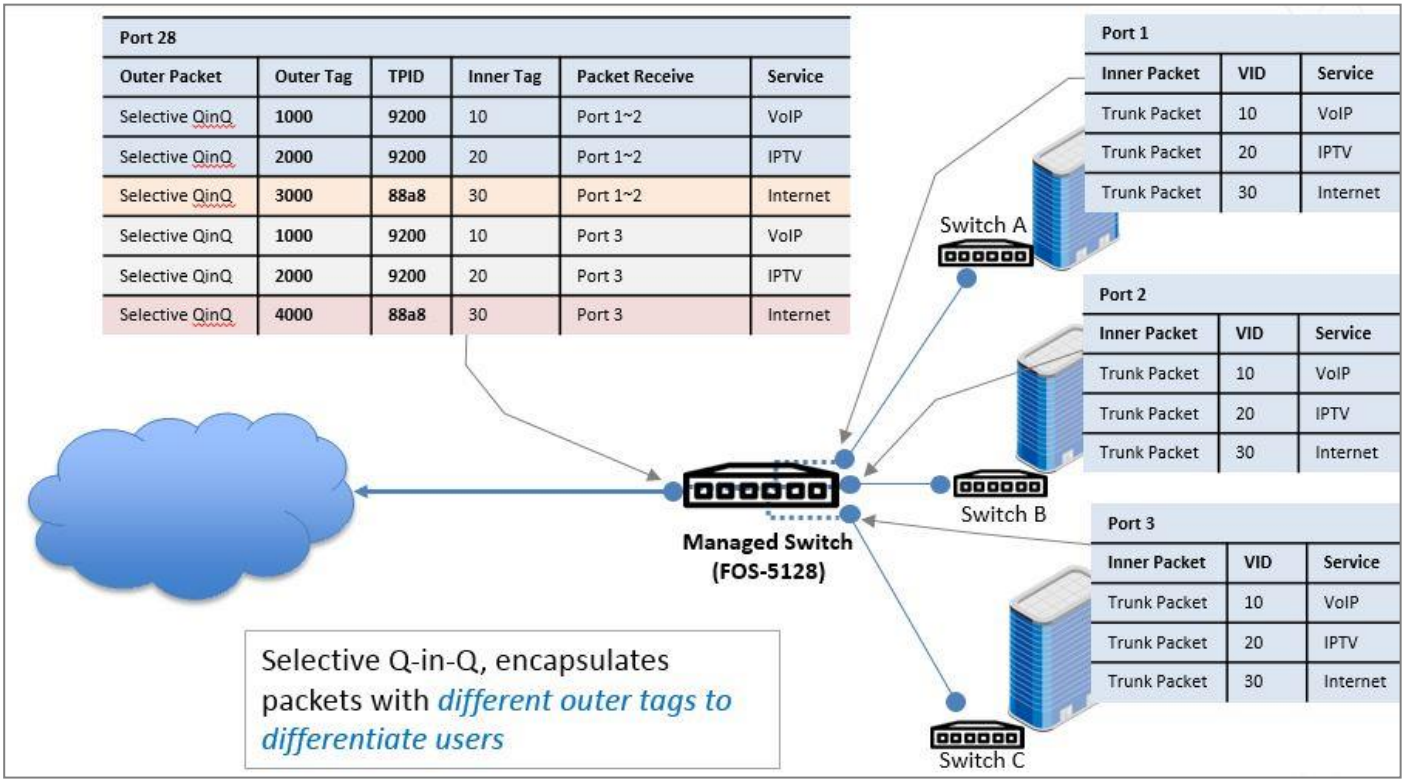
```
==================================================================
IEEE 802.1q VLAN Table
==================================================================
CPU VLAN ID          : 1
Management Priority : 0

U: Untagged, T: Tagged, D: Dot1q-Tunnel, V: Member, -: Not Member
S: Sender, R: Receiver, *: Denotes MVR VLAN ID
------------------------------------------------------------------------------------------------------------
VLAN Name       VLAN  1          8  9           16  17          24  25 28  CPU
-----------------      --------  ------------ ------------------ ------------------ --------- ----
Default_VLAN          1   ----UUUU  UUUUUUUU  UUUUUUUU  UUUU  V
VLAN0010             10  DT--------- -----------------  ------------------  ---------  --
VLAN0020             20  ----DD----  ----------------- ------------------   ---------  --


FOS-5128(config)#
```

Example 3,

We will configure one set of Managed Switch FOS-5152 via CLI as the Table 2-5 listed to demonstrate Selection Q-in-Q application through a single uplink port.



As the above figure shows, three clients are assigned three VLANs that the tag values are 10, 20 & 30 in Internet service. VLAN 10 corresponds to VoIP, VLAN 20 corresponds to IPTV and VLAN 30 corresponds to Internet. After the downlink ports enable Selective Q-in-Q function that connects Managed Switch to switch A, B & C, the packets will be packed with different external tags according to VLAN ID of service.

The packets with tag 10 will be packed an external tag 1000 directly;
The packets with tag 20 will be packed an external tag 2000 directly;
The packets with tag 30 (from switch A & B) will be packed an external tag 3000 directly;
The packets with tag 30 (from switch C) will be packed an external tag 4000 directly.

Service Name	Inner VID	Outer VID
VoIP	10	1000
IPTV	20	2000
Internet	30	3000 (Packets come from switch A & B)
	30	4000 (Packets come from switch C)

Table 2-5

- On Managed Switch, add VLAN 1000 to packets that have inner VLAN IDs 10 and enter Interface 1, and VLAN 2000 to packets that have inner VLAN IDs 20 and enter Interface 1, and VLAN 3000 to packets that have inner VLAN IDs 30 and enter Interface 1.

- On Managed Switch, add VLAN 1000 to packets that have inner VLAN IDs 10 and enter Interface 2, and VLAN 2000 to packets that have inner VLAN IDs 20 and enter Interface 2, and

VLAN 3000 to packets that have inner VLAN IDs 30 and enter Interface 2.

- On Managed Switch, add VLAN 1000 to packets that have inner VLAN IDs 10 and enter Interface 3, and VLAN 2000 to packets that have inner VLAN IDs 20 and enter Interface 3, and VLAN 4000 to packets that have inner VLAN IDs 30 and enter Interface 3.

- Configure Interface 28 on Managed Switch to allow packets from VLAN 1000, 2000, 3000 and 4000.

Note:

1. *Selective Q-in-Q based on the VLAN ID can be only enabled on selective-qinq mode interfaces in the inbound direction.*
2. *The outer VLAN ID must exist and the interface must be added to the outer VLAN in tagged mode.*
3. *VLAN translation and Selective Q-in-Q cannot be configured on the same interface.*

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

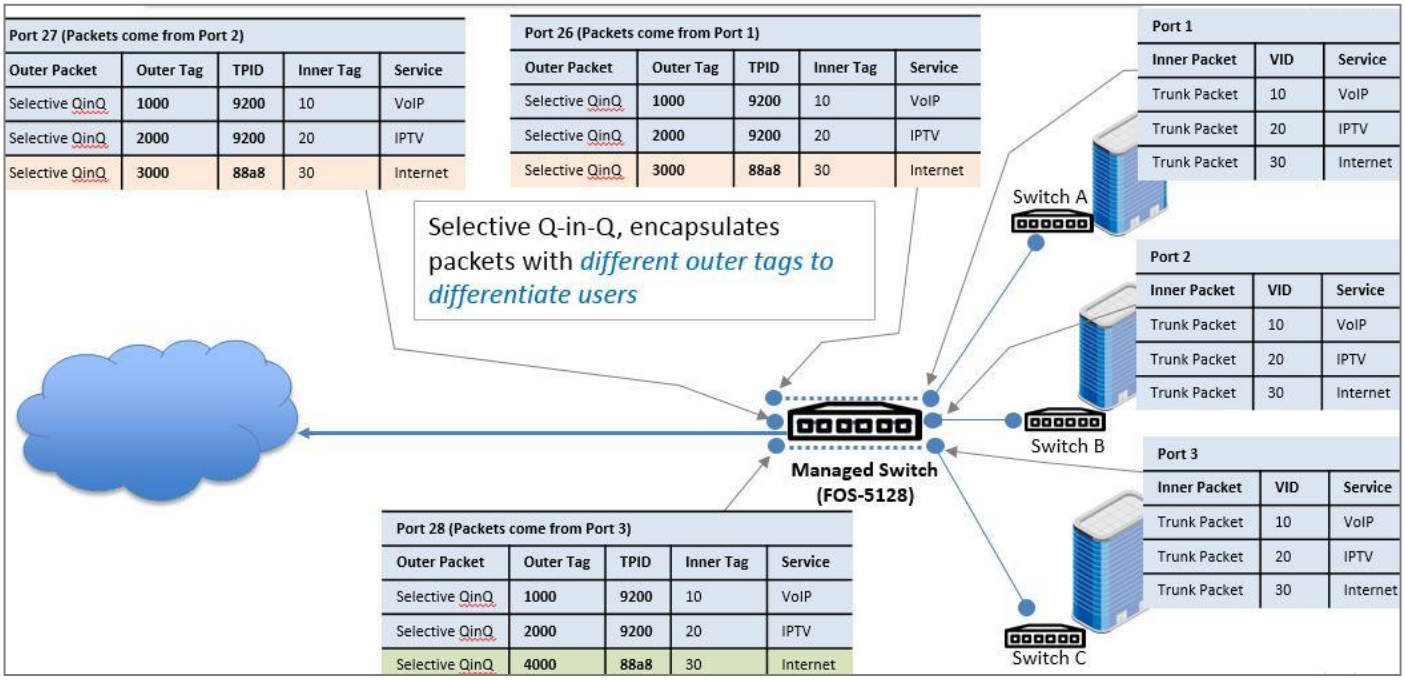
	Command	Purpose
STEP1	FOS-5152# **config** FOS-5152(config)#	**Enter the global configuration mode.**
STEP2	FOS-5152(config)# **vlan dot1q-vlan 10** **name VoIP** **exit**	**Create VLAN 10. And set VLAN 10's name as "VoIP".**
STEP3	FOS-5152(config)# **vlan dot1q-vlan 20** **name IPTV** **exit**	**Create VLAN 20. And set VLAN 20's name as "IPTV".**
STEP4	FOS-5152(config)# **vlan dot1q-vlan 30** **name Internet** **exit**	**Create VLAN 30. And set VLAN 30's name as "Internet".**
STEP5	FOS-5152(config)# **vlan dot1q-vlan 1000** **name VoIP_ISP** **exit**	**Create VLAN 1000. And set VLAN 1000's name as "VoIP_ISP".**
STEP6	FOS-5152(config)# **vlan dot1q-vlan 2000** **name IPTV_ISP** **exit**	**Create VLAN 2000. And set VLAN 2000's name as "IPTV_ISP".**
STEP7	FOS-5152(config)# **vlan dot1q-vlan 3000** **name Internet_ISP_A** **exit**	**Create VLAN 3000. And set VLAN 3000's name as "Internet_ISP_A".**
STEP8	FOS-5152(config)# **vlan dot1q-vlan 4000** **name Internet_ISP_B** **exit**	**Create VLAN 4000. And set VLAN 4000's name as "Internet_ISP_B".**

STEP9	FOS-5152(config)# **interface 1**	**Enter Port 1.**
STEP10	FOS-5152 (config-if-1)# **vlan dot1q-vlan pvid 101** **vlan dot1q-vlan mode selective-qinq** **no vlan dot1q-vlan trunk-vlan 1** **vlan dot1q-vlan trunk-vlan 1000,2000,3000** **exit**	**Assign PVID of Port 1 as 101.** **Set the VLAN mode of Port 1 as selective-qinq mode.** **Deny VID 1 for tagged packets.** **Allow VIDs 1000, 2000 and 3000 for tagged packets.**
STEP11	FOS-5152(config)# **interface 2**	**Enter Port 2.**
STEP12	FOS-5152 (config-if-2)# **vlan dot1q-vlan pvid 102** **vlan dot1q-vlan mode selective-qinq** **no vlan dot1q-vlan trunk-vlan 1** **vlan dot1q-vlan trunk-vlan 1000,2000,3000** **exit**	**Assign PVID of Port 2 as 102.** **Set the VLAN mode of Port 2 as selective-qinq mode.** **Deny VID 1 for tagged packets.** **Allow VIDs 1000, 2000 and 3000 for tagged packets.**
STEP13	FOS-5152(config)# **interface 3**	**Enter Port 3.**
STEP14	FOS-5152 (config-if-3)# **vlan dot1q-vlan pvid 103** **vlan dot1q-vlan mode selective-qinq** **no vlan dot1q-vlan trunk-vlan 1** **vlan dot1q-vlan trunk-vlan 1000,2000,4000** **exit**	**Assign PVID of Port 3 as 103.** **Set the VLAN mode of Port 3 as selective-qinq mode.** **Deny VID 1 for tagged packets.** **Allow VIDs 1000, 2000 and 4000 for tagged packets.**
STEP15	FOS-5152(config)# **interface 28**	**Enter Port 28.**
STEP16	FOS-5152 (config-if-28)# **vlan dot1q-vlan mode trunk** **no vlan dot1q-vlan trunk-vlan 1** **vlan dot1q-vlan trunk-vlan 1000,2000,3000,4000** **exit**	**Set the VLAN mode of Port 28 as trunk mode.** **Deny VID 1 for tagged packets.** **Allow VIDs 1000, 2000, 3000 and 4000 for tagged packets.**
STEP17	FOS-5152(config)# **vlan selective-qinq**	**Enable Selective Q-in-Q function globally.**
STEP18	FOS-5152(config)# **vlan selective-qinq name VoIP_ISP interface 1-2 inner-vid 10 outer-vid 1000 tpid 3 priority 0**	**Create a Selective Q-in-Q rule named "VoIP_ISP", and configure outer tag VID as 1000, EtherType as TPID 3 (9200) and 802.1p priority as 0 when the inner tag VID of Ports 1~2 is 10.**
STEP19	FOS-5152(config)# **vlan selective-qinq name IPTV_ISP interface 1-2 inner-vid 20 outer-vid 2000 tpid 3 priority 0**	**Create a Selective Q-in-Q rule named "IPTV_ISP", and configure outer tag VID as 2000, EtherType as TPID 3 (9200) and 802.1p priority as 0 when the inner tag VID of Ports 1~2 is 20.**

STEP20	FOS-5152(config)# **vlan selective-qinq name Internet_ISP interface 1-2 inner-vid 30 outer-vid 3000 tpid 2 priority 0**	**Create a Selective Q-in-Q rule named “Internet_ISP”, and configure outer tag VID as 3000, EtherType as TPID 2 (88a8) and 802.1p priority as 0 when the inner tag VID of Ports 1~2 is 30.**
STEP21	FOS-5152(config)# **vlan selective-qinq name VoIP_ISP interface 3 inner-vid 10 outer-vid 1000 tpid 3 priority 0**	**Create a Selective Q-in-Q rule named “VoIP_ISP”, and configure outer tag VID as 1000, EtherType as TPID 3 (9200) and 802.1p priority as 0 when the inner tag VID of Port 3 is 10.**
STEP22	FOS-5152(config)# **vlan selective-qinq name IPTV_ISP interface 3 inner-vid 20 outer-vid 2000 tpid 3 priority 0**	**Create a Selective Q-in-Q rule named “IPTV_ISP”, and configure outer tag VID as 2000, EtherType as TPID 3 (9200) and 802.1p priority as 0 when the inner tag VID of Port 3 is 20.**
STEP23	FOS-5152(config)# **vlan selective-qinq name Internet_ISP interface 3 inner-vid 30 outer-vid 4000 tpid 2 priority 0**	**Create a Selective Q-in-Q rule named “Internet_ISP”, and configure outer tag VID as 4000, EtherType as TPID 2 (88a8) and 802.1p priority as 0 when the inner tag VID of Port 3 is 30.**

Example 4,

We will configure one set of Managed Switch FOS-5152 via CLI as the Table 2-6 listed to demonstrate Selection Q-in-Q application through multiple uplink ports.



As the above figure shows, three clients are assigned three VLANs that the tag values are 10, 20 & 30 in internet service. VLAN 10 corresponds to VoIP, VLAN 20 corresponds to IPTV and VLAN 30 corresponds to Internet. After the downlink ports enable selective QinQ function that connects Managed Switch to switch A, B & C, the packets will be packed with different external tags according to VLAN ID of service.

The packets with tag 10 will be packed an external tag 1000 directly;
The packets with tag 20 will be packed an external tag 2000 directly;
The packets with tag 30 (from switch A & B) will be packed an external tag 3000 directly;
The packets with tag 30 (from switch C) will be packed an external tag 4000 directly.

Service Name	Inner VID	Outer VID
VoIP	10	1000
IPTV	20	2000
Internet	30	3000 (Packets come from switch A & B)
	30	4000 (Packets come from switch C)

Table 2-6

- On Managed Switch, add VLAN 1000 to packets that have inner VLAN IDs 10 and enter Interface 1, and VLAN 2000 to packets that have inner VLAN IDs 20 and enter Interface 1, and VLAN 3000 to packets that have inner VLAN IDs 30 and enter Interface 1.

- On Managed Switch, add VLAN 1000 to packets that have inner VLAN IDs 10 and enter Interface 2, and VLAN 2000 to packets that have inner VLAN IDs 20 and enter Interface 2, and VLAN 3000 to packets that have inner VLAN IDs 30 and enter Interface 2.

- On Managed Switch, add VLAN 1000 to packets that have inner VLAN IDs 10 and enter Interface 3, and VLAN 2000 to packets that have inner VLAN IDs 20 and enter Interface 3, and VLAN 4000 to packets that have inner VLAN IDs 30 and enter Interface 3.

- Configure Interfaces 26~27 on Managed Switch to allow packets from VLAN 1000, 2000 and 3000.

- Configure Interface 28 on Managed Switch to allow packets from VLAN 1000, 2000 and 4000.

Note:

1. Selective Q-in-Q based on the VLAN ID can be only enabled on selective-qinq mode interfaces in the inbound direction.
2. The outer VLAN ID must exist and the interface must be added to the outer VLAN in tagged mode.
3. VLAN translation and Selective Q-in-Q cannot be configured on the same interface.

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

	Command	Purpose
STEP1	FOS-5152# **config** FOS-5152(config)#	**Enter the global configuration mode.**
STEP2	FOS-5152(config)# **vlan dot1q-vlan 10** **name VoIP** **exit**	**Create VLAN 10. And set VLAN 10's name as "VoIP".**
STEP3	FOS-5152(config)# **vlan dot1q-vlan 20** **name IPTV** **exit**	**Create VLAN 20. And set VLAN 20's name as "IPTV".**
STEP4	FOS-5152(config)# **vlan dot1q-vlan 30** **name Internet** **exit**	**Create VLAN 30. And set VLAN 30's name as "Internet".**
STEP5	FOS-5152(config)# **vlan dot1q-vlan 1000** **name VoIP_ISP** **exit**	**Create VLAN 1000. And set VLAN 1000's name as "VoIP_ISP".**
STEP6	FOS-5152(config)# **vlan dot1q-vlan 2000** **name IPTV_ISP** **exit**	**Create VLAN 2000. And set VLAN 2000's name as "IPTV_ISP".**
STEP7	FOS-5152(config)# **vlan dot1q-vlan 3000** **name Internet_ISP_A** **exit**	**Create VLAN 3000. And set VLAN 3000's name as "Internet_ISP_A".**
STEP8	FOS-5152(config)# **vlan dot1q-vlan 4000** **name Internet_ISP_B** **exit**	**Create VLAN 4000. And set VLAN 4000's name as "Internet_ISP_B".**

STEP9	FOS-5152(config)# **interface 1**	**Enter Port 1.**
STEP10	FOS-5152 (config-if-1)# **vlan dot1q-vlan pvid 101** **vlan dot1q-vlan mode selective-qinq** **no vlan dot1q-vlan trunk-vlan 1** **vlan dot1q-vlan trunk-vlan 1000,2000,3000** **exit**	**Assign PVID of Port 1 as 101.** **Set the VLAN mode of Port 1 as selective-qinq mode.** **Deny VID 1 for tagged packets.** **Allow VIDs 1000, 2000 and 3000 for tagged packets.**
STEP11	FOS-5152(config)# **interface 2**	**Enter Port 2.**
STEP12	FOS-5152 (config-if-2)# **vlan dot1q-vlan pvid 102** **vlan dot1q-vlan mode selective-qinq** **no vlan dot1q-vlan trunk-vlan 1** **vlan dot1q-vlan trunk-vlan 1000,2000,3000** **exit**	**Assign PVID of Port 2 as 102.** **Set the VLAN mode of Port 2 as selective-qinq mode.** **Deny VID 1 for tagged packets.** **Allow VIDs 1000, 2000 and 3000 for tagged packets.**
STEP13	FOS-5152(config)# **interface 3**	**Enter Port 3.**
STEP14	FOS-5152 (config-if-3)# **vlan dot1q-vlan pvid 103** **vlan dot1q-vlan mode selective-qinq** **no vlan dot1q-vlan trunk-vlan 1** **vlan dot1q-vlan trunk-vlan 1000,2000,4000** **exit**	**Assign PVID of Port 3 as 103.** **Set the VLAN mode of Port 3 as selective-qinq mode.** **Deny VID 1 for tagged packets.** **Allow VIDs 1000, 2000 and 4000 for tagged packets.**
STEP15	FOS-5152(config)# **interface 26**	**Enter Port 26.**
STEP16	FOS-5152 (config-if-26)# **vlan dot1q-vlan mode trunk** **no vlan dot1q-vlan trunk-vlan 1** **vlan dot1q-vlan trunk-vlan 1000,2000,3000** **exit**	**Set the VLAN mode of Port 26 as trunk mode.** **Deny VID 1 for tagged packets.** **Allow VIDs 1000, 2000 and 3000 for tagged packets.**
STEP17	FOS-5152(config)# **interface 27**	**Enter Port 27.**
STEP18	FOS-5152 (config-if-27)# **vlan dot1q-vlan mode trunk** **no vlan dot1q-vlan trunk-vlan 1** **vlan dot1q-vlan trunk-vlan 1000,2000,3000** **exit**	**Set the VLAN mode of Port 27 as trunk mode.** **Deny VID 1 for tagged packets.** **Allow VIDs 1000, 2000 and 3000 for tagged packets.**

STEP19	FOS-5152(config)# **interface 28**	**Enter interface 28.**
STEP20	FOS-5152 (config-if-28)# **vlan dot1q-vlan mode trunk** **no vlan dot1q-vlan trunk-vlan 1** **vlan dot1q-vlan trunk-vlan 1000,2000,4000** **exit**	**Set the VLAN mode of Port 28 as trunk mode.** **Deny VID 1 for tagged packets.** **Allow VIDs 1000, 2000 and 4000 for tagged packets.**
STEP21	FOS-5152(config)# **vlan selective-qinq**	**Enable Selective Q-in-Q function globally.**
STEP22	FOS-5152(config)# **vlan selective-qinq name VoIP_ISP interface 1-2 inner-vid 10 outer-vid 1000 tpid 3 priority 0**	**Create a Selective Q-in-Q rule named "VoIP_ISP", and configure outer tag VID as 1000, EtherType as TPID 3 (9200) and 802.1p priority as 0 when the inner tag VID is 10 of Ports 1~2.**
STEP23	FOS-5152(config)# **vlan selective-qinq name IPTV_ISP interface 1-2 inner-vid 20 outer-vid 2000 tpid 3 priority 0**	**Create a Selective Q-in-Q rule named "IPTV_ISP", and configure outer tag VID as 2000, EtherType as TPID 3 (9200) and 802.1p priority as 0 when the inner tag VID is 20 of Ports 1~2.**
STEP24	FOS-5152(config)# **vlan selective-qinq name Internet_ISP interface 1-2 inner-vid 30 outer-vid 3000 tpid 2 priority 0**	**Create a Selective Q-in-Q rule named "Internet_ISP", and configure outer tag VID as 3000, EtherType as TPID 2 (88a8) and 802.1p priority as 0 when the inner tag VID is 30 of Ports 1~2.**
STEP25	FOS-5152(config)# **vlan selective-qinq name VoIP_ISP interface 3 inner-vid 10 outer-vid 1000 tpid 3 priority 0**	**Create a Selective Q-in-Q rule named "VoIP_ISP", and configure outer tag VID as 1000, EtherType as TPID 3 (9200) and 802.1p priority as 0 when the inner tag VID is 10 of Port 3.**
STEP26	FOS-5152(config)# **vlan selective-qinq name IPTV_ISP interface 3 inner-vid 20 outer-vid 2000 tpid 3 priority 0**	**Create a Selective Q-in-Q rule named "IPTV_ISP", and configure outer tag VID as 2000, EtherType as TPID 3 (9200) and 802.1p priority as 0 when the inner tag VID is 20 of Port 3.**
STEP27	FOS-5152(config)# **vlan selective-qinq name Internet_ISP interface 3 inner-vid 30 outer-vid 4000 tpid 2 priority 0**	**Create a Selective Q-in-Q rule named "Internet_ISP", and configure outer tag VID as 4000, EtherType as TPID 2 (88a8) and 802.1p priority as 0 when the inner tag VID is 30 of Port 3.**

2.6.31 Interface Command

Use “interface” command to set up configurations of several discontinuous ports or a range of ports.

1. Entering interface numbers.

Interface 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 below 2-17 commands.

2. Enable port auto-negotiation.

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

3. Set up link aggregation or port-trunking.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# channel-group lacp		Set the selected interfaces’ to be aggregated via LACP. **Note: At lease 2 ports but not more than 8 ports can be aggregated.**
Switch(config-if-PORT-PORT)# channel-group lacp key [0-255]	[0-255]	Specify a key to the selected interfaces. (0: auto)
Switch(config-if-PORT-PORT)# no channel-group lacp role		Specify the selected interfaces to passive LACP role.
Switch(config-if-PORT-PORT)# channel-group lacp role [active | passive]	[active | passive]	Specify the selected interfaces as active or passive LACP role.
Switch(config-if-PORT-PORT)# channel-group trunking [group_name]	[group_name]	Specify the selected interfaces to the trunking group. **Note1: At lease 2 ports but not more than 8 ports can be aggregated.** **Note2: Ports cannot be in LACP and port-trunking mode at the same time.** **Note3 : A port-trunking group need to created before assigning ports to it.**

		(See Section 2.6.6 “channel-group”)
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 trunking		Remove the selected ports from a link aggregation group.

4. Set up port description.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# description [description]	[description]	Enter the description for the selected port(s). Up to 35 characters can be accepted.
No command		
Switch(config-if-PORT-PORT)# no description		Clear the port description for the selected ports.

5. Set up port duplex mode.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# duplex [full]	[full]	Configure the port duplex as **full**.
No command		
Switch(config-if-PORT-PORT)# no duplex		Configure the port duplex as **half**. **Note1: 1-28 fiber ports cannot be configured as half duplex.**

6. Enable flow control operation.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# flowcontrol		Enable flow control on the selected port(s).
No command		
Switch(config-if-PORT-PORT)# no flowcontrol		Disable flow control on the selected port(s).

7. Setup DHCP snooping/relay sub-commands

Command	Parameter	Description
Switch(config-if-PORT-PORT)# ip dhcp snooping option		Enable the selected interfaces’ DHCP Option 82 / DHCPv6 Option 37 relay agent globally.
Switch(config-if-PORT-PORT)# ip dhcp snooping circuit		Enable the selected interfaces’ DHCPv4 Option 82 / DHCPv6 Option 37 Manual Circuit Id.

Switch(config-if-PORT-PORT)# ip dhcp snooping circuit formatted		Enable the Formatted DHCPv4 Option 82 / DHCPv6 Option 37 Circuit Id for the selected interfaces.
Switch(config-if-PORT-PORT)# ip dhcp snooping circuit id [circuit_id]	[circuit_id]	Configure DHCPv4 Option 82 / DHCPv6 Option 37 Circuit ID. The circuit ID can be a string of up to 63 characters.
Switch(config-if-PORT-PORT)# ip dhcp snooping trust		Enable the selected interfaces as DHCPv4 Option 82 / DHCPv6 Option 37 trust ports.
Switch(config-if-PORT-PORT)# ip dhcp snooping server-trust		Enable the selected interfaces as DHCPv4/DHCPv6 server trust ports. **Note: A port / ports cannot be configured as option 82/option 37 trust and server trust at the same time.**
No command		
Switch(config-if-PORT-PORT)# no ip dhcp snooping option		Disable the selected interfaces' DHCPv4 Option 82 / DHCPv6 Option 37 relay agent.
Switch(config-if-PORT-PORT)# no ip dhcp snooping trust		Reset the selected interfaces back to non-DHCPv4 Option 82 / DHCPv6 Option 37 trust ports.
Switch(config-if-PORT-PORT)# no ip dhcp snooping server-trust		Reset the selected interfaces back to non-DHCPv4/DHCPv6 server trust ports.
Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit		Disable the selected interfaces' DHCPv4 Option 82 / DHCPv6 Option 37 Manual Circuit Id.
Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit id		Clear DHCPv4 Option 82 / DHCPv6 Option 37 Circuit Id.
Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit formatted		Disable the Formatted DHCPv4 Option 82 / DHCPv6 Option 37 Circuit Id for the selected interfaces.

8. Setup IGMP snooping/MLD sub-commands

Command	Parameter	Description
Switch(config-if-PORT-PORT)# ip igmp filter		Enable IGMP filter for the selected ports.
Switch(config-if-PORT-PORT)# ip igmp filter profile [profile_name]	[profile_name]	Assign the selected ports to an IGMP filter profile. **Note: Need to create an IGMP filter profile first under the igmp global configuration mode before assigning it.**
Switch(config-if-PORT-PORT)# ip igmp filter max-groups [1-512]	[1-512]	Specify the maximum groups number of multicast streams to the selected ports.
Switch(config-if-PORT)# ip igmp static-multicast-ip [E.F.G.H | E:F:G:H:I:J:K:L] vlan [1-4094]	[E.F.G.H | E:F:G:H:I:J:K:L]	Create/specify a static multicast IP and the specified VLAN entry to the selected port. **Note: Only one port could be assigned at a time.**

	[1-4094]	Specify a VLAN ID.
No command		
Switch(config-if-PORT-PORT)# no ip igmp filter		Disable IGMP filter for the selected interfaces.
Switch(config-if-PORT-PORT)# no ip igmp filter profile [profile_name]	[profile_name]	Remove the specified profile from the selected ports.
Switch(config-if-PORT-PORT)# no ip igmp max-groups		Reset the maximum number of multicast streams back to the default (512 channels).
Switch(config-if-PORT)# no ip igmp static-multicast-ip [E.F.G.H | E:F:G:H:I:J:K:L] vlan [1-4094]	[E.F.G.H | E:F:G:H:I:J:K:L]	Remove the specific static multicast IP. **Note: Only one port could be assigned at a time.**
	[1-4094]	Remove the specified VLAN ID.

9. Enable loop-detection per port.

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

10. Setup IP source guard

Command	Parameter	Description
Switch(config-if-PORT-PORT)# ip sourceguard [dhcp | fixed-ip]	[dhcp | fixed-ip]	Specify the authorized access type as either DHCP or fixed-IP for the selected ports. **dhcp:** DHCP server assigns IP address. **fixed IP:** Only Static IP (Create Static IP table first).
Switch(config-if-PORT)# ip sourceguard static-ip [A.B.C.D | A:B:C:D:E:F:G:H] vlan [1-4094]	[A.B.C.D | A:B:C:D:E:F:G:H]	Add a static IPv4/IPv6 address to static IP address table. **Note: Only one port could be assigned at a time.**
	[1-4094]	Specify VLAN ID. **Note : Static IP can only be configured when IP sourceguard is set to fixed-ip.**
No command		
Switch(config-if-PORT-PORT)# no ip sourceguard		Reset IP sourceguard type setting of the selected ports back to the default (unlimited)

		unlimited: Non-Limited (Allows both static IP and DHCP-assigned IP). This is the default setting.

11. Configure MAC table learning and static MAC table.

Command	Parameter	Description
Switch(config-if-PORT)# mac address-table static-mac [xx:xx:xx:xx:xx:xx] vlan [1-4094]	[xx:xx:xx:xx:xx:xx]	Specify a MAC address to the VLAN entry. **Note: Only one port could be set at a time.**
	[1-4094]	Specify the VLAN where the packets with the destination MAC address can be forwarded to the selected port.
Switch(config-if-PORT-PORT)# mac learning		Enable MAC address learning function of the selected port(s).
No command		
Switch(config-if-PORT)# no mac address-table static-mac [xx:xx:xx:xx:xx:xx] vlan [1-4094]	[xx:xx:xx:xx:xx:xx]	Remove the specified MAC address from the MAC address table. **Note: Only one port could be set at a time.**
	[1-4094]	Remove the VLAN to which the specified MAC belongs.
Switch(config-if-PORT-PORT)# no mac learning		Disable MAC address learning function of the selected port(s).

12. Configure QoS rate limit.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# qos rate-limit ingress rate [500-1000000 | 1-1000] Kbps/Mbps	[500-1000000 | 1-1000] Kbps/Mbps	Specify the **ingress** rate limit value. (Valid range is from 500-1000000 in unit of Kbps or 1-1000 in unit of Mbps).
Switch(config-if-PORT-PORT)# qos rate-limit egress rate [500-1000000 | 1-1000] Kbps/Mbps	[500-1000000 | 1-1000] Kbps/Mbps	Specify the **egress** rate limit value. (Valid range is from 500-1000000 in unit of Kbps or 1-1000 in unit of Mbps).
No command		
Switch(config-if-PORT-PORT)# no qos rate-limit ingress		Disable QoS ingress rate limit settings.
Switch(config-if-PORT-PORT)# no qos rate-limit egress		Disable QoS egress rate limit settings.

13. Shutdown interface.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# shutdown		Disable the selected interfaces.
No command		
Switch(config-if-PORT-PORT)# no shutdown		Enable the selected interfaces.

14. Configure RSTP parameters per port.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# spanning-tree		Enable spanning-tree protocol on the selected interface(s).
Switch(config-if-PORT-PORT)# spanning-tree cost [0-200000000]	[0-200000000]	Specify the path cost value on the selected interface(s).
Switch(config-if-PORT-PORT)# spanning-tree priority [0-15]	[0-15]	Specify priority value on the selected interface(s). **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 interface(s) as edge ports.
Switch(config-if-PORT-PORT)# spanning-tree p2p [forced_true|forced_false|auto]	[forced_true|forced_false|auto]	Set the selected interfaces to non-point to point ports (forced_false) or allow the Managed Switch to detect point to point status automatically (auto). By default, physical ports are set to point to point ports (forced_true).
No command		
Switch(config-if-PORT-PORT)# no spanning-tree		Disable spanning-tree protocol on the selected interface(s).
Switch(config-if-PORT-PORT)# no spanning-tree cost		Reset the cost value back to the default for the selected interface(s).
Switch(config-if-PORT-PORT)# no spanning-tree priority		Reset the priority value back to the default for the selected interface(s).
Switch(config-if-PORT-PORT)# no spanning-tree edge		Reset the selected interface(s) back to non-edge ports.
Switch(config-if-PORT-PORT)# no spanning-tree p2p		Reset the selected interface(s) back to point

		to point ports (forced_ true).

15. Set up port speed.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# speed [10000 | 1000 | 100 | 10 | auto-speed]	[10000 | 1000 | 100 | 10 | auto-speed]	Configure the port speed as 10000Mbps, 1000Mbps, 100Mbps or 10Mbps. **Note1: Speed can only be configured when auto-negotiation is disabled.** **Note2: Fiber ports cannot be configured as 10Mbps.** **Note3: Only Fiber 25-28 ports can be configured as 10000Mbps.** **Note4: Only Fiber 25-28 ports can be configured as Auto- speed.**
No command		
Switch(config-if-PORT-PORT)# no speed		Reset the port speed setting back to the default.

16. Set up VLAN parameters per port.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# vlan dot1q-vlan pvid [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode access		Set the selected ports to the access mode (untagged).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk		Set the selected ports to the trunk mode (tagged).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk native		Enable native VLAN for untagged traffic on the selected ports. (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 :**

		Need to create a port-based VLAN group under the VLAN global configuration mode before joining it.
No command		
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan pvid		Reset the selected ports' PVID back to the default setting.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the specified trunk VLAN ID from the selected ports.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan mode		Reset the selected ports' 802.1q VLAN mode setting back to the default (Access Mode).
Switch(config-if-PORT-PORT)# no vlan port-based [name]	[name]	Remove the selected ports from the specified port-based VLAN.

17. Set up MAC Limit.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# security mac-limit		Enable MAC Limit function of the selected port(s).
Switch(config-if-PORT-PORT)# security mac-limit maximum [1-50]	[1-50]	Specify the maximum number of source MAC address that can be learned for each of the selected port(s). The valid range of number that can be configured is 1~50.
Switch(config-if-PORT-PORT)# security mac-limit action [drop | shutdown]	[drop | shutdown]	Specify the action that would be taken when the number of source MAC address learned exceeds the limit.
No Command		
Switch(config-if-PORT-PORT)# no security mac-limit		Disable MAC Limit function of the selected port(s).
Switch(config-if-PORT-PORT)# no security mac-limit maximum		Reset the maximum number of source MAC address that can be learned for the selected port(s) back to the default. (1)
Switch(config-if-PORT-PORT)# no security mac-limit action		Reset the action that would be taken when the number of source MAC address learned exceeds the limit back to the default. (Drop)

2.6.32 Show interface statistics Command

The command of "show interface statistics", displaying port traffic statistics, port packet error statistics and port analysis history, can be used either in Privileged mode or Global Configuration mode. This command is useful for network administrators to diagnose and analyze the real-time conditions of each port traffic.

Show interface statistics Command	Parameters	Description
Switch(config)# show interface		Show the overall interface

		configurations.
Switch(config)# show interface [port_list]	[port_list]	Show interface configurations of selected ports.
Switch(config)# show interface statistics analysis		Display packets analysis (events) for each port.
Switch(config)# show interface statistics analysis [port_list]	[port_list]	Display packets analysis for the selected ports.
Switch(config)# show interface statistics analysis rate		Display packets analysis (rates) for each port.
Switch(config)# show interface statistics analysis rate [port_list]	[port_list]	Display packets analysis (rates) for the selected ports.
Switch(config)# show interface statistics clear		Clear all statistics counters.
Switch(config)# show interface statistics clear [port_list]	[port_list]	Clear statistics counters of selected ports.
Switch(config)# show interface statistics error		Display error packets statistics (events) for each port.
Switch(config)# show interface statistics error [port_list]	[port_list]	Display error packets statistics (events) for the selected ports.
Switch(config)# show interface statistics error rate		Display error packets statistics (rates) for each port.
Switch(config)# show interface statistics error rate [port_list]	[port_list]	Display error packets statistics (rates) for the selected ports.
Switch(config)# show interface statistics traffic		Display traffic statistics (events) for each port.
Switch(config)# show interface statistics traffic [port_list]	[port_list]	Display traffic statistics (events) for the selected ports.
Switch(config)# show interface statistics traffic rate		Display traffic statistics (rates) for each port.
Switch(config)# show interface statistics traffic rate [port_list]	[port_list]	Display traffic statistics (rates) for the selected ports.

2.6.33 Show sfp Command

When you slide-in SFP transceiver, detailed information about this module can be viewed by issuing this command.

Show sfp Command	Description
Switch(config)# show sfp information	Display SFP information, including the speed of transmission, the distance of transmission, vendor name, vendor PN, and vendor SN.
Switch(config)# show sfp state	Show the slide-in SFP modules' current temperature, Tx Bias power, TX power, RX power and voltage.

2.6.34 Show running-config & start-up-config & default-config Command

Show running-config & start-up-config & default-config Command	Parameters	Description
Switch(config)# show running-config		Show the difference between the running configuration and the default configuration.
Switch(config)# show running-config include [string]	[string]	Specify the keyword to search for the matched information from the difference between the running configuration and the default configuration.
Switch(config)# show running-config full		Show the full running configuration currently used in the Manged Switch. Please note that you must save the running configuration into your switch flash before rebooting or restarting the device.
Switch(config)# show running-config full include [string]	[string]	Specify the keyword to search for the matched information from the full running configuration.
Switch(config)# show running-config interface [port_list]	[port_list]	Show the running configuration currently used in the Manged Switch for the the specific port(s).
Switch(config)# show running-config interface [port_list] include [string]		Specify the keyword to search for the matched information from the running configuration of the specific port(s).
Switch(config)# show start-up-config		Show the difference between the startup configuration and the default configuration.
Switch(config)# show start-up-config include [string]	[string]	Specify the keyword to search for the matched information from the difference between the startup configuration and the default configuration.
Switch(config)# show start-up-config full		Display the system configuration stored in Flash.
Switch(config)# show start-up-config full include [string]	[string]	Specify the keyword to search for the matched information from the full startup configuration.
Switch(config)# show default-config		Display the system factory default configuration.
Switch(config)# show default-config include [string]	[string]	Specify the keyword to search for the matched information from the system factory default configuration.

2.6.35 Show log Command

Show Log Command	Parameters	Description
Switch(config)# show log		Display the entire event log currently stored in the Managed Switch, by each time showing 10 events from the newest to the oldest.
Switch(config)# show log clear		Remove the entire event log currently stored in the Managed Switch.
Switch#(config) show log link-flap [port_number]	[port_number]	Display the record of a specified port's condition where the link alternates between up and down states.
Switch#(config) show log index [ID range]	[1-2000]	Display a certain part of the event log from a specified index to another according to the specified ID range, by each time showing 10 events from the newest to the oldest. **ID range:** Enter a range of event indexes with a hyphen. For example: 2-4 or 4-500
Switch#(config) show log terminal-length [1-2000]	[1-2000]	Display the entire event log, by each time showing a specified number of events from the newest to the oldest.
Switch#(config) show log reverse		Display the entire event log, by each time showing 10 events from the oldest to the newest.
Switch#(config) show log log-item [exclude | include] [item_list]	[exclude | include]	Display events by filtering out or encompassing events of the specified category.
	[1-43]	Specify the event category from the item list for log filtering. **item_list:** Enter several discontinuous numbers separated by commas or a range of items with a hyphen. For example:1,3 or 2-4 **Note:** Use quick key: a "space" followed by "?" to view the comprehensive item list.
Switch#(config) show log log-item [exclude | include] [item_list] time-range [exclude | include] [ntp-time] start [hh:mm dd MMM yyyy] end [hh:mm dd MMM yyyy]	[exclude | include]	Display events by filtering out or encompassing events of the specified category.
	[1-43]	Specify the event category from the item list for log filtering.
	[exclude | include]	Display events that occurred (didn't occur) during a specified NTP time period.
	[ntp-time]	Filter the events according to NTP time.
	[hh:mm dd	Specify the starting point of an NTP

	MMM yyyy]	time period. **hh:** 0-23 **mm:** 0-59 **dd:** 1-31 **MMM:** jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec **yyyy:** 2021-2037
	[hh:mm dd MMM yyyy]	Specify the ending point of an NTP time period. **hh:** 0-23 **mm:** 0-59 **dd:** 1-31 **MMM:** jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec **yyyy:** 2021-2037
Switch#(config) show log log-item [exclude | include] [item_list] time-range [exclude | include] [up-time] start [hh:mm dddd] end [hh:mm dddd]	[exclude | include]	Display events by filtering out or encompassing events of the specified category.
	[1-43]	Specify the event category from the item list for log filtering.
	[exclude | include]	Display events that occurred (didn't occur) during a specified uptime period.
	[up-time]	Filter the events according to the Managed Switch's uptime.
	[hh:mm dddd]	Specify the starting point of a Managed Switch's uptime period. **hh:** 0-23 **mm:** 0-59 **dddd:** 0-9999
	[hh:mm dddd]	Specify the ending point of a Managed Switch's uptime period. **hh:** 0-23 **mm:** 0-59 **dddd:** 0-9999

3. SNMP NETWORK MANAGEMENT

The Simple Network Management Protocol (SNMP) is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the TCP/IP protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP consists of the following key components.

Managed device is a network node that contains SNMP agent. Managed devices collect and store management information and make this information available to NMS using SNMP. Managed device can be switches/Hub, etc..

MIB (Management Information Base) defines the complete manageable entries of the managed device. These MIB entries can be either read-only or read-write. For example, the System Version is read-only variables. The Port State Enable or Disable is a read-write variable and a network administrator can not only read but also set its value remotely.

SNMP Agent is a management module resides in the managed device that responds to the SNMP Manager request.

SNMP Manager/NMS executes applications that monitor and control managed devices. NMS provide the bulk of the processing and memory resources required for the complete network management. SNMP Manager is often composed by desktop computer/work station and software program such like HP OpenView.
Totally 4 types of operations are used between SNMP Agent & Manager to change the MIB information. These 4 operations all use the UDP/IP protocol to exchange packets.

GET: This command is used by an SNMP Manager to monitor managed devices. The SNMP Manager examines different variables that are maintained by managed devices.

GET Next: This command provides traversal operation and is used by the SNMP Manager to sequentially gather information in variable tables, such as a routing table.

SET: This command is used by an SNMP Manager to control managed devices. The NMS changes the values of variables stored within managed devices.

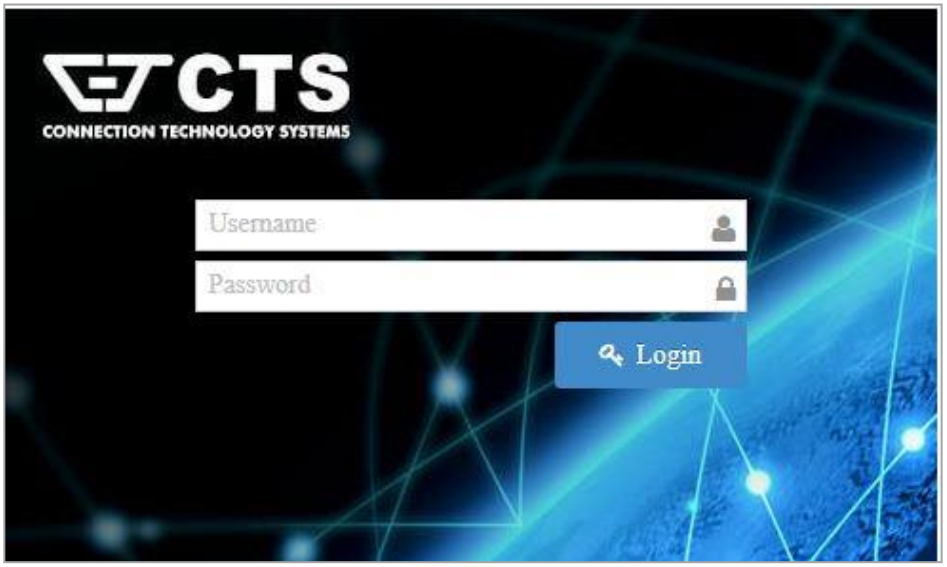
Trap: Trap is used by the managed device to report asynchronously a specified event to the SNMP Manager. When certain types of events occur, a managed device will send a trap to alert the SNMP Manager.
The system built-in management module also supports SNMP management. Users must install the MIB file before using the SNMP based network management system. The MIB file is on a disc or diskette that accompanies the system. The file name extension is .mib, which SNMP based compiler can read.

Please refer to the appropriate documentation for the instructions of installing the system private MIB.

4. WEB MANAGEMENT

You can manage the Managed Switch via a web browser. However, you must first assign a unique IP address to the Managed Switch before doing so. Through the connection of any SFP ports using the fiber cable or any TP ports using a RJ45 cable, you will be allowed to have an access of the Managed Switch and set up the IP address for the first time. (Note: The Managed Switch can be reached with the default IP address of **"192.168.0.1"**. You can change the IP address of the switch to the desired one later in its **Network Management** menu.)

Initiate a web browser and input **http:// 192.168.0.1** to enter the Managed Switch system. Once you gain the access, the following login window will appear. Also input the default administrator username ***admin*** and keep the administrator password field blank (By default, no password is required.) to login into the main screen page.



After you login successfully, the screen with the Main Menu will show up. The functions of Main Menu in the Web Management are similar to those described at the Console Management.

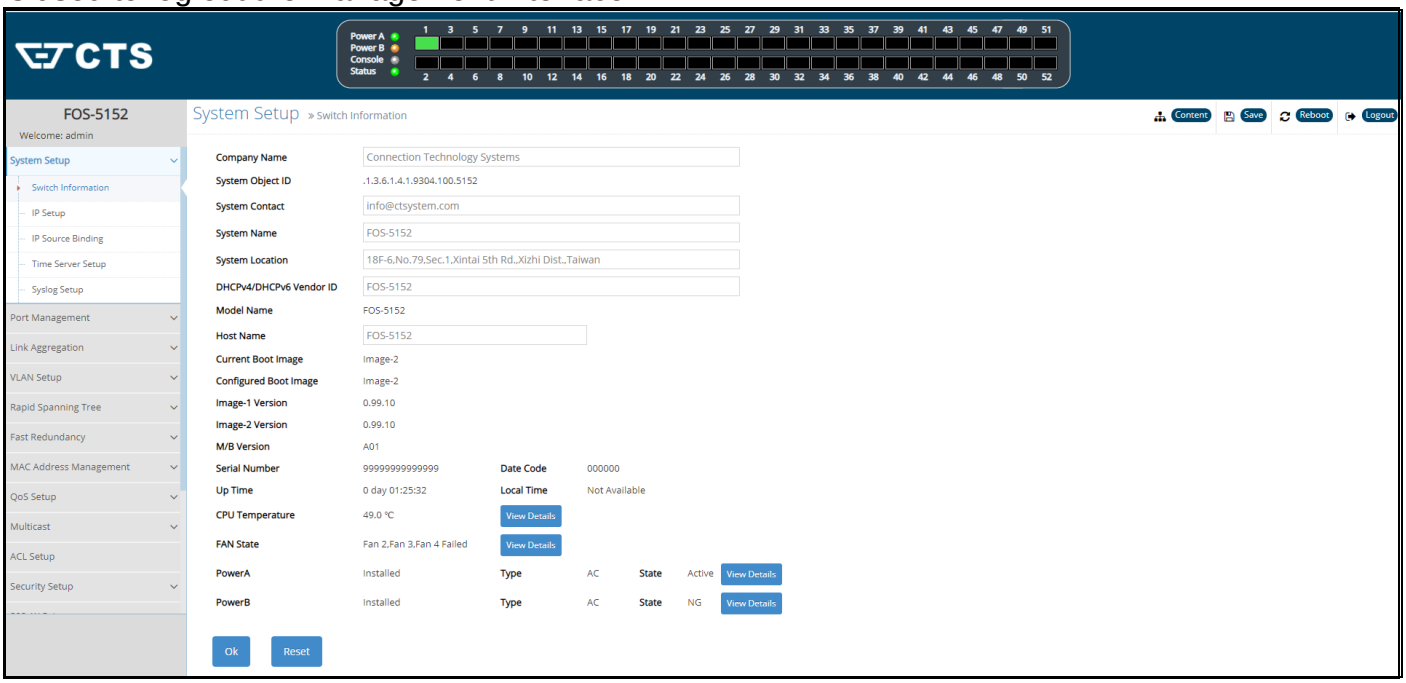
On the top side, it shows the front panel of Managed Switch. On this front panel image, the corresponding link-up ports will be displayed in green color; as to the link-down ports, they will be dark. Red color will be displayed on the corresponding ports while these ports' port state is disabled.

Additionally, there are clicking functions on this front panel image. When clicking on any port of this panel image, you will directly jump to the **Port Setup &Status** webpage.

In this **Port Setup &Status** webpage, it shows the basic information and configuration of each port. For more details about this, please refer to Section 4.2.1 "Port Setup &Status".

Besides the Main Menu, a general overview of the Managed Switch's all functions will also be displayed when clicking on the Content icon among the quick buttons located on the top-right corner of each webpage. You can also reach each fucnions from the listed hyperlink.

As for other quick buttons, the Save icon is provided for the user to save any new settings permanently into Flash, the Reboot icon is used to restart the switch, and the Logout icon is used to log out the management interface.



In the Main Menu, there are 16 main functions, including System Setup, Port Management, Link Aggregation, VLAN Setup, Rapid Spanning Tree, MAC Address Management, QoS Setup, Multicast, ACL Setup, Security Setup, 802.1X Setup, LLDP, Power over Ethernet, Layer 2 Protocol Tunneling, Maintenance, Management and Logout contained. We will respectively describe their sub-functions in the following sections of this chapter.

- **System Setup:** Set up or view the Managed Switch's system information, IP address and related information required for network management applications, etc.
- **Port Management:** Set up each port's configuration and monitor the port's status.
- **Link Aggregation:** Set up port trunking group as well as LACP port configuration, and view the LACP port status and statistics.
- **VLAN Setup:** Set up VLAN mode, VLAN configuration, VLAN translation as well as Selective Q-in-Q, and view the IEEE802.1q VLAN Table of the Managed Switch.
- **Rapid Spanning Tree:** Set up RSTP switch settings, aggregated port settings, physical port settings, etc. And view RSTP VLAN Bridge, port status, and statistics.
- **MAC Address Management:** Set up MAC address, enable or disable MAC security, etc.
- **QoS Setup:** Set up the priority queuing, remarking, rate limit, and so on.

- **Multicast:** Configure IGMP/MLD Snooping, static multicast and MVR parameters, and view the IGMP/MLD status and Groups table.

- **ACL Setup:** Set up access control entries and lists.

- **Security Setup:** Set up DHCP Snooping, DHCP Option 82 / DHCPv6 Option 37 relay agent, port isolation, storm control, MAC limiter, static IPv4/IPv6 table configuration, and so on.

- **802.1X Setup:** Set up the 802.1X system, port Admin state, port reauthenticate, and so on. And view 802.1X port status and statistics.

- **LLDP:** Enable or disable LLDP on ports, set up LLDP-related attributes, and view the TLV information sent by the connected device with LLDP-enabled.

- **Layer 2 Protocol Tunneling:** Enable or disable L2PT function, set up acceptable BPDUs for GBPT (Generic Bridge PDU Tunneling), and view the state of Layer 2 protocol data units (PDUs) as well as their encapsulation & decapsulation & drop counters of each port.

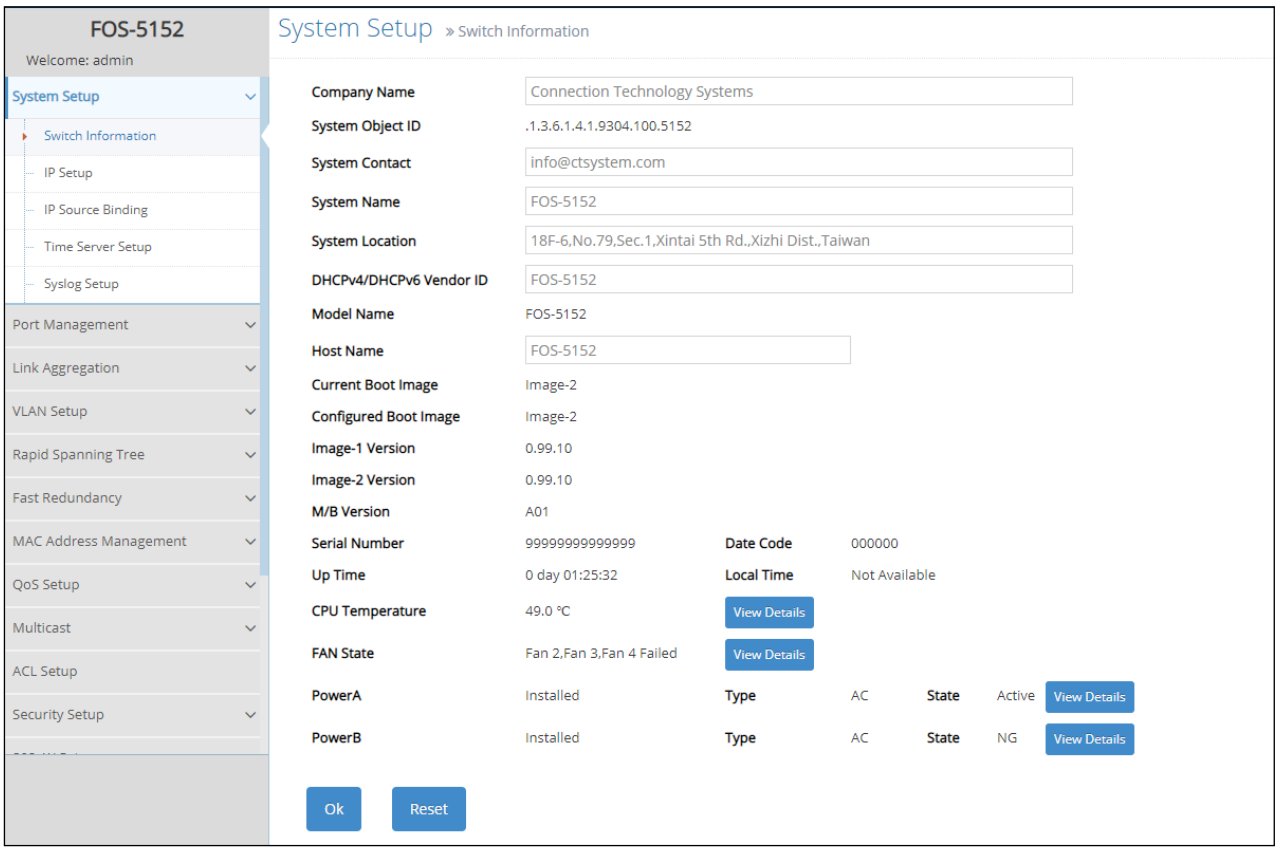
- **Maintenance:** View the operation status and event logs of the system, ping, lookback test, etc..

- **Management:** Enable or disable the specified network services, view the RS-232 serial port setting, user account management, do the firmware upgrade, load the factory default settings, etc..

- **Logout:** Log out the management interface.

4.1 System Setup

In order to enable network management of the Managed Switch, proper network configuration is required. To do this, click the folder **System Setup** from the **Main Menu** and then 5 options within this folder will be displayed as follows.



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

2. **IP Setup:** Set up the required IP configuration of the Managed Switch.

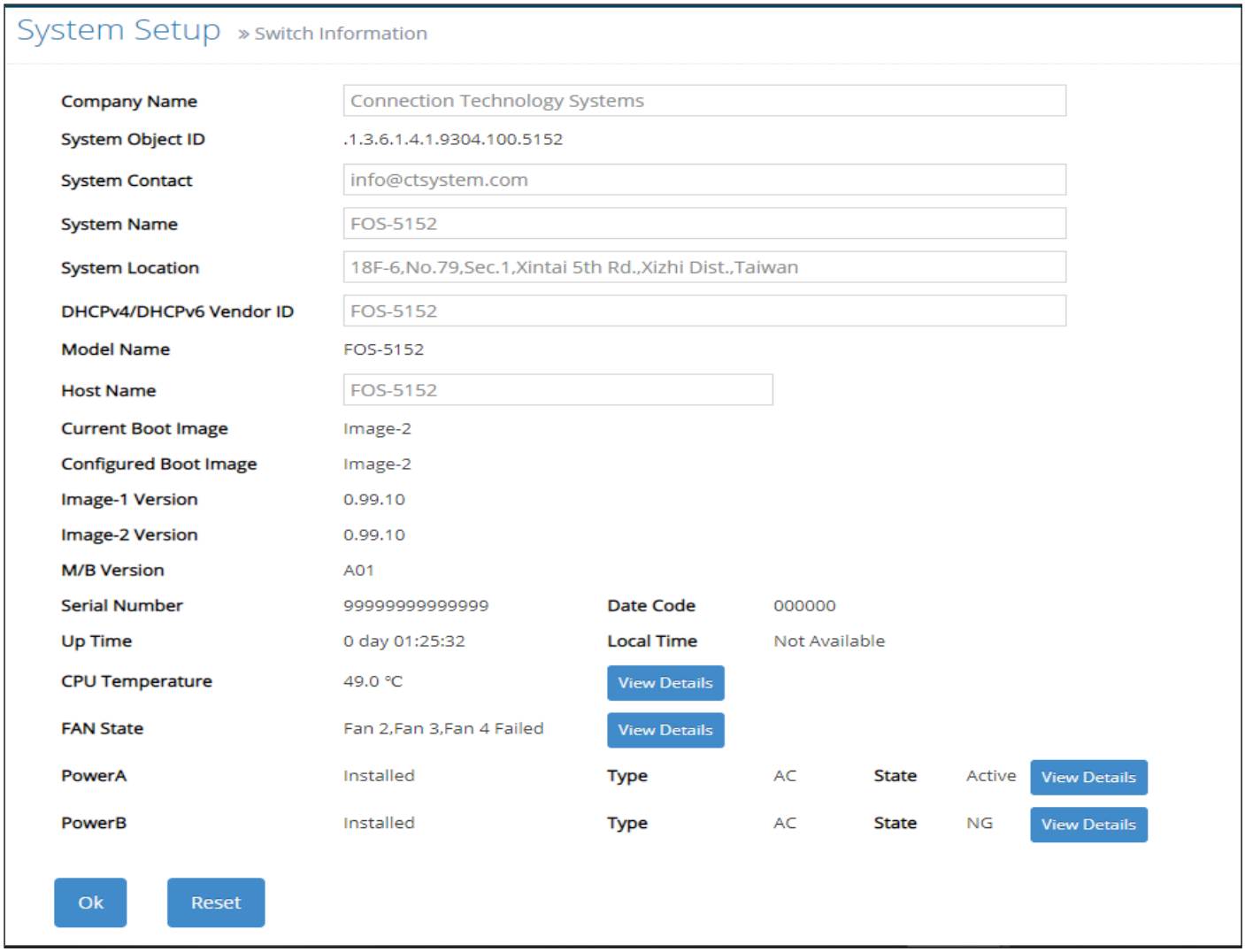
3. **IP Source Binding:** Set up the IP address for source binding.

4. **Time Server Setup:** Set up the time server's configuration.

5. **Syslog Setup:** Set up the Mal-attempt Log server's configuration.

4.1.1 Switch Information

Select the option **System Information** from the **System Setup** menu and then the following screen shows up.



Company Name: Enter a company name for this Managed Switch.

System Object ID: Display the predefined System OID.

System Contact: Enter the contact information for this Managed Switch.

System Name: Enter a descriptive system name for this Managed Switch.

System Location: Enter a brief location description for this Managed Switch.

DHCPv4/DHCPv6 Vendor ID: Vendor Class Identifier that is used for DHCP/DHCPv6 relay agent function. Enter the user-defined DHCP vendor ID, and up to 55 alphanumeric characters can be accepted. Please make sure you have an exact DHCP Vendor ID with the value specified in “vendor-classes” in your dhcpd.conf file. For detailed information, see Appendix B.

Model Name: Display the product’s model name.

Host Name: Enter the product’s host name.

Current Boot Image: The image that is currently being used.

Configured Boot Image: The image you would like to use after rebooting.

Image-1 Version: Display the firmware version 1 (image-1) used in this device.

Image-2 Version: Display the firmware version 2 (image-2) used in this device.

M/B Version: Display the main board version.

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

Date Code: Display the date code of the Managed Switch firmware.

Up Time: Display the up time since last restarting.

Local Time: Display the local time of the system.

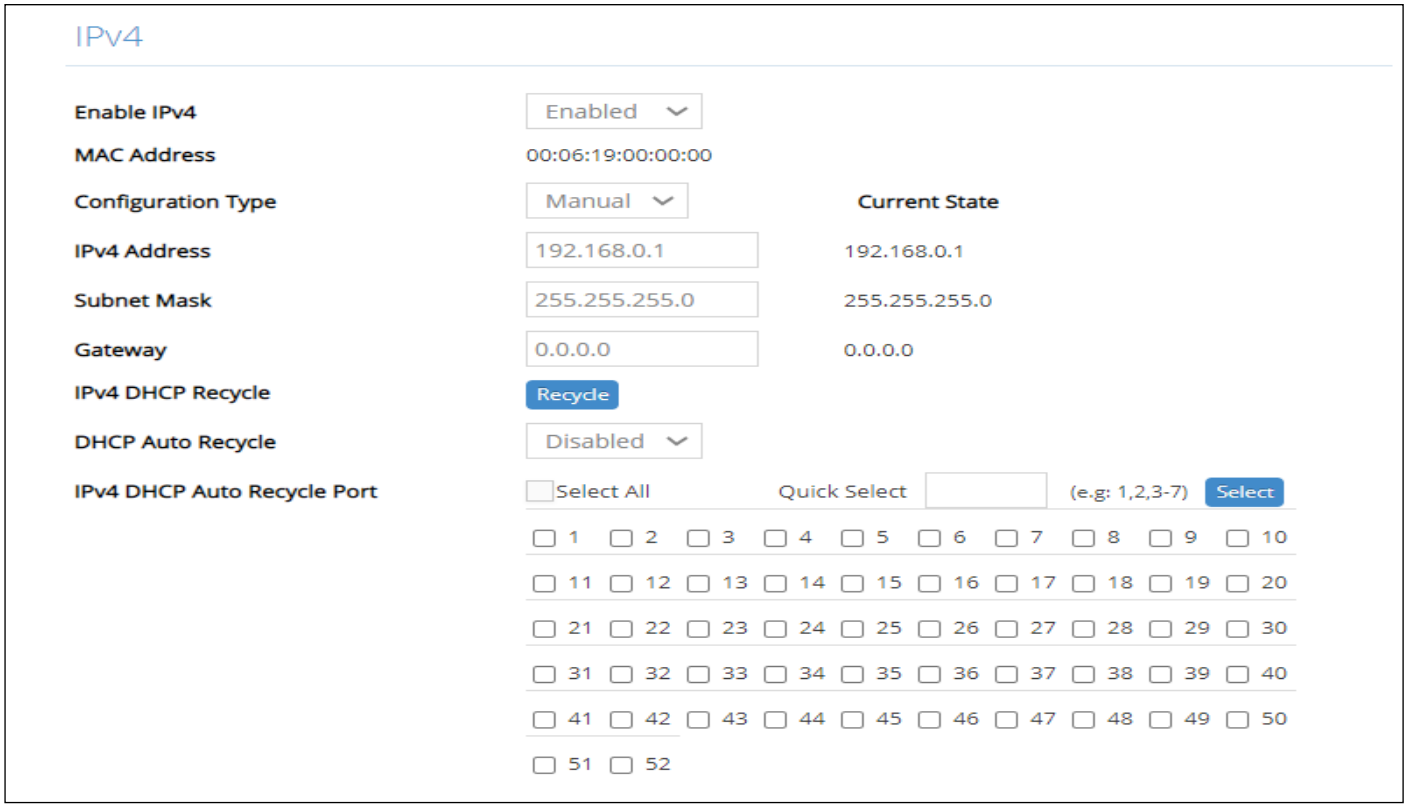
CPU Temperature: Display the current CPU temperature of this device. In case CPU temperature is shown in red color, it stands that CPU temperature currently detected is higher than the **High Temperature Threshold** value you configure. For more details on this or do the further alarm notification settings for CPU temperature of the system, click **View Details** to directly jump to the **CPU Temperature Status** webpage under **Maintenance** folder from the **Main Menu**.

FAN State: Display the status of FAN1, FAN2 and FAN3. For more details on these FANs' speed (RPM), click **View Details** to directly jump to the **FAN State** webpage under **Maintenance** folder from the **Main Menu**.

Power A/B: Display the installation status, the type of power source, and the state of Power A and Power B. For more details on their voltages and state, click **View Details** to directly jump to the **System Voltage** webpage under **Maintenance** folder from the **Main Menu**.

4.1.2 IP Setup

Click the option **IP Setup** from the **System Setup** menu and then the following screen page appears.



Enable IPv4: Click the checkbox in front of **enable IPv4** to enable IPv4 function on the Managed Switch.

MAC Address: This view-only field shows the unique and permanent MAC address assigned to the Managed switch. You cannot change the Managed 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 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.

IPv4 Address: Enter the unique IP address of this Managed Switch. You can use the default IP address or specify a new one when the situation of 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 Switch. This address is required when the Managed 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 Switch are on the same network.

Current State: This view-only field shows currently assigned IP address (by DHCP or manual), Subnet Mask and Gateway of the Managed Switch.

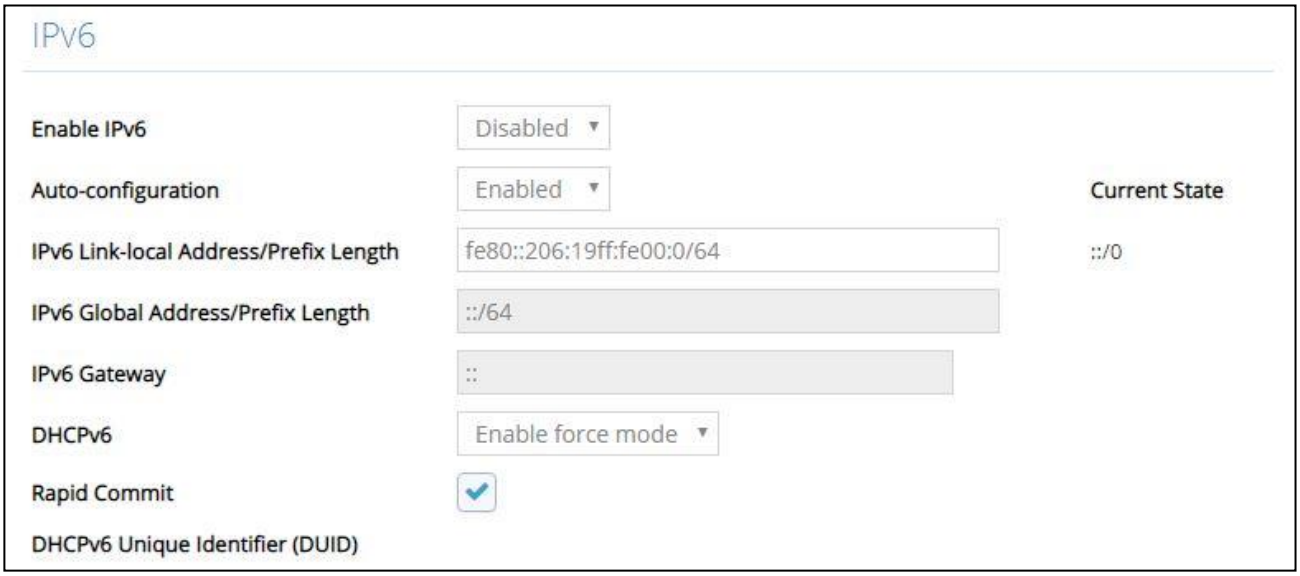
IPv4 DHCP Recycle: Click on **Recycle** manually, DHCP Release packets and Discover packets will be sent to DHCP server. And it will ask for IP address from DHCP server again. Please note that this parameter is just one-time setting and will not be saved into the configuration file of the Managed Switch.

NOTE: *Need to choose "DHCP" as the configuration type before running this function.*

DHCP Auto Recycle: Enable or disable IPv4 DHCP Auto Recycle function globally.

IPv4 DHCP Auto Recycle Port: Enable IPv4 DHCP Auto Recycle function on the specified ports. Only when one of these specific link-up ports is switched from link-down into link-up status, DHCP Release packets and Discover packets will be sent to DHCP server. And it will ask for IP address from DHCP server again.

Just click on the checkbox of the corresponding port number to select the port(s) as IPv4 DHCP auto recycle port. Or directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field and then press the **Select** button, the specified port(s) will be checked immediately. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.



Enable IPv6: Click the checkbox in front of **enable IPv6** to enable IPv6 function on the Managed Switch.

Auto-configuration: Enable Auto-configuration for the Managed Switch to get IPv6 address automatically or disable it for manual configuration.

IPv6 Link-local Address/Prefix Length: The Managed Switch will form a link-local address from its MAC address and the link-local prefix FE80::/10. This is done by putting the prefix into the leftmost bits and the MAC address (in EUI-64 format) into the rightmost bits, and if there are any bits left in between, those are set to zero.

IPv6 Global Address/Prefix Length: This is done in the same fashion as the link-local address, but instead of the link-local prefix FE80:: it will use the prefix supplied by the router and put it together with its identifier (which by default is the MAC address in EUI-64 format).

IPv6 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 Switch. This address is required when the Managed Switch and the network management station are on different networks or subnets.

DHCPv6: Enable or disable DHCPv6 function

Disabled: Disable DHCPv6.

Enable auto mode: Configure DHCPv6 function in auto mode.

Enable force mode: Configure DHCPv6 function in force mode.

Rapid Commit: Check to enable Rapid Commit which allows the server and client to use a two-message exchange to configure clients, rather than the default four-message exchange,

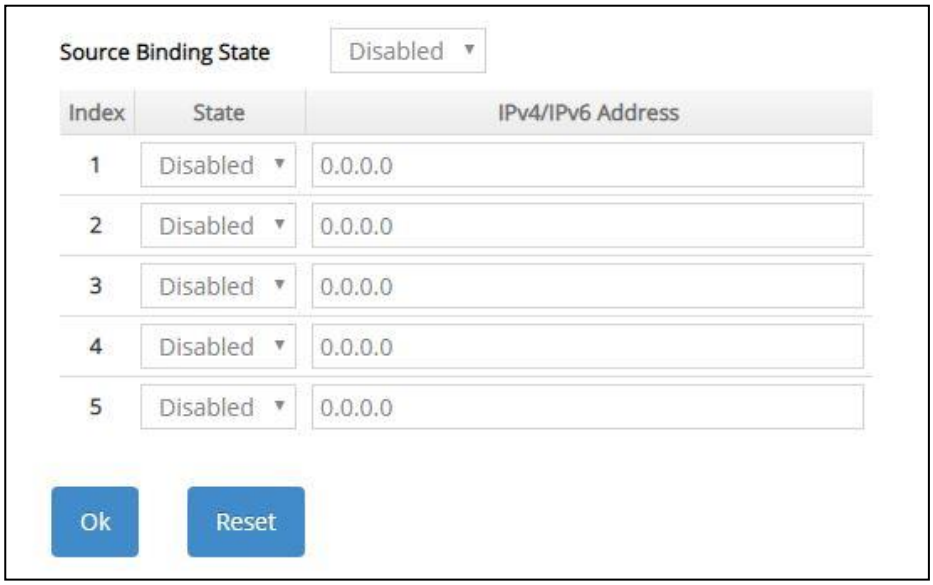
DHCPv6 Unique Identifier (DUID): View-only field that shows the DHCP Unique Identifier (DUID).

Current State: View-only field that shows currently assigned IPv6 address (by auto-configuration or manual) and Gateway of the Managed Switch.

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

4.1.3 IP Source Binding

Click the option **IP Source Binding** from the **System Setup** menu and then the following screen page appears.



Source Binding State: Globally enable or disable IP source binding.

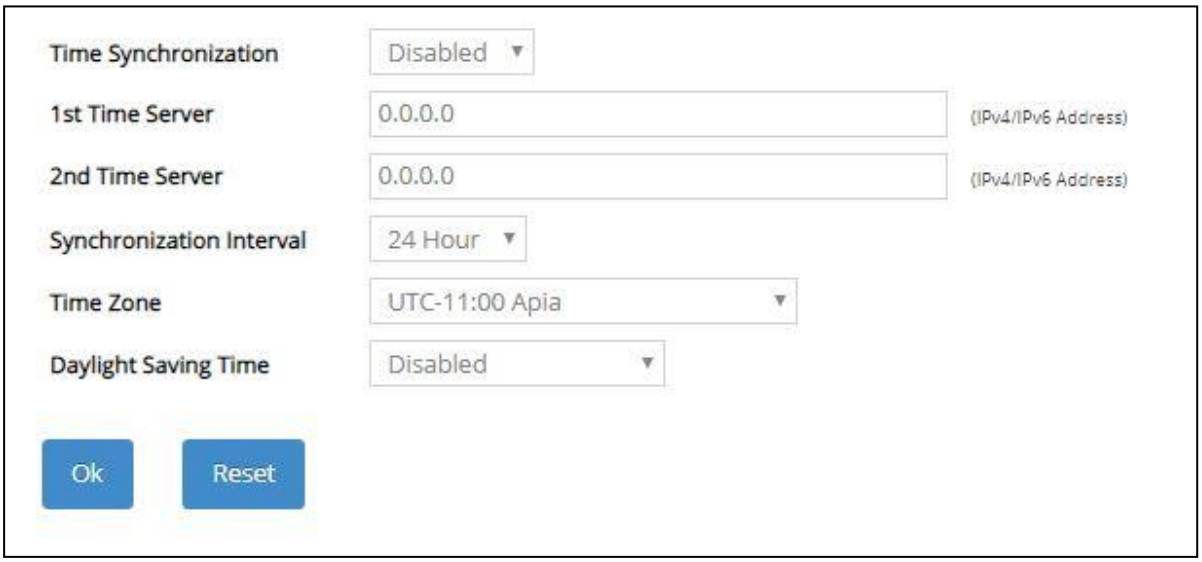
State: Disable or enable the assigned IP address to reach the management.

IPv4/IPv6 Address: Specify the IP address for source binding.

Click **OK**, the new settings will be taken effect immediately or click **Reset** to ignore these settings.

4.1.4 Time Server Setup

Click the option **Time Server Setup** from the **System Setup** menu and then the following screen page appears.



Time Synchronization: To enable or disable the time synchronization function.

1st Time Server: Set up the IPv4/IPv6 address of the first NTP time server.

2nd Time Server: Set up the IPv4/IPv6 address of the secondary NTP time server. When the first NTP time server is down, the Managed Switch will automatically connect to the secondary NTP time server.

Synchronization Interval: Set up the time interval to synchronize with the NTP time server.

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

Daylight Saving Time: Include **"Disabled"**, **"recurring / Weekday"** and **"date / Julian Day"** three options to enable or disable the daylight saving time function. It is a way of getting more daytime hour(s) by setting the time to be hour(s) ahead in the morning.

Daylight Saving Time Date Start: If the "date / Julian Day" option is selected in Daylight Saving Time, click the pull-down menu to select the start date of daylight saving time.

Daylight Saving Time Date End: If the "date **/** Julian Day" option is selected in Daylight Saving Time, click the pull-down menu to select the end date of daylight saving time.

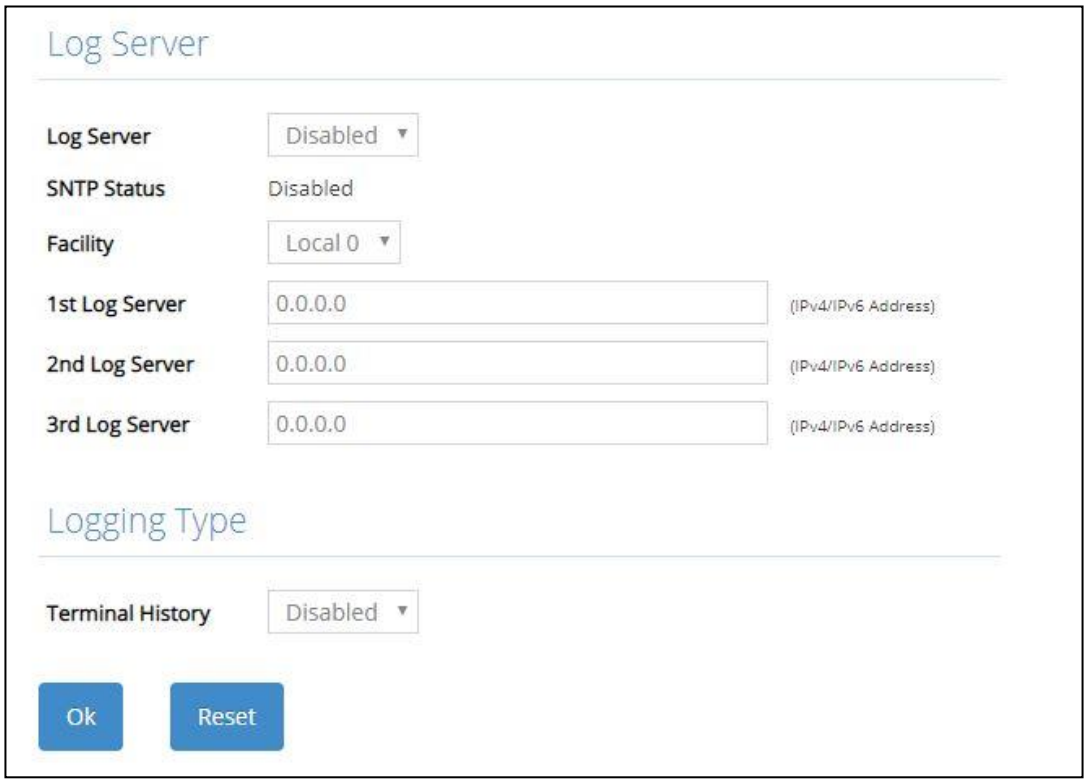
Daylight Saving Time Recurring Star: If the "recurring / Weekday" option is selected in Daylight Saving Time, click the pull-down menu to select the recurring start date of daylight saving time.

Daylight Saving Time Recurring End: If the "recurring / Weekday" option is selected in Daylight Saving Time, click the pull-down menu to select the recurring end date of daylight saving time.

NOTE: *SNTP is used to get the time from those NTP servers. It is recommended that the time server is in the same LAN with the Managed Switch or at least not too far away. In this way, the time will be more accurate.*

4.1.5 Syslog Configuration

Click the option **Syslog Setup** from the **System Setup** menu and then the following screen page appears.



When DHCP snooping filters unauthorized DHCP packets on the network, the mal-attempt log will allow the Managed Switch to send event notification message to log server.

Log Server: Enable or disable mal-attempt log function.

SNTP Status: View-only field that shows the SNTP server status.

Facility: Specify a facility code (Local 0~Local 7) to a specific device for classifying the syslog message provided by different devices.

1st Log Server: Specify the first log server's IPv4/IPv6 address.

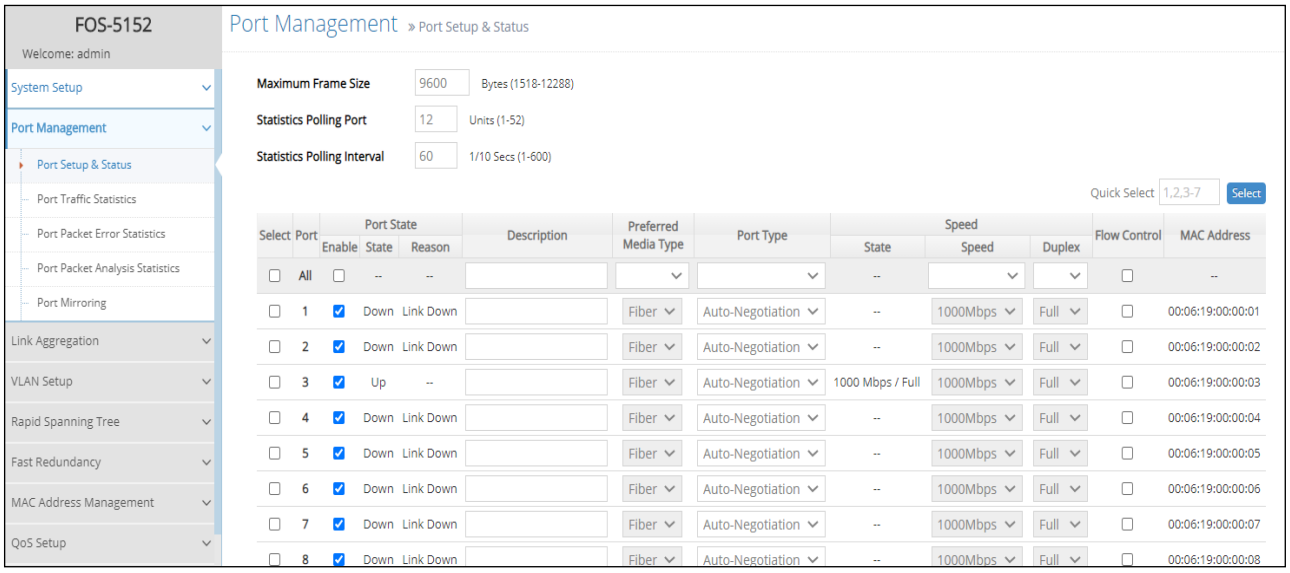
2nd Log Server: Specify the secondary log server's IPv4/IPv6 address. When the first log server is down, the Managed Switch will automatically contact the second or third Log server.

3rd Log Server: Specify the third log server's IPv4/IPv6 address. When the first log server is down, the Managed Switch will automatically contact the secondary or third log server.

Terminal History of Logging Type: Enable or disable whether the log of CLI commands will be forwarded to the Log Server 1~3.

4.2 Port Management

In order to configure each port of the Managed Switch and monitor the real-time ports' link-up status or traffic counters for maintenance or diagnostic purposes. Select the folder **Port Management** from the **Main Menu** and then 5 options within this folder will be displayed for your selection.



1. **Port Setup & Status:** Set up frame size, enable/disable port state & flow control, and view current port media type, port state, etc.

2. **Port Traffic Statistics:** View each port's frames and bytes received or sent, utilization, etc..

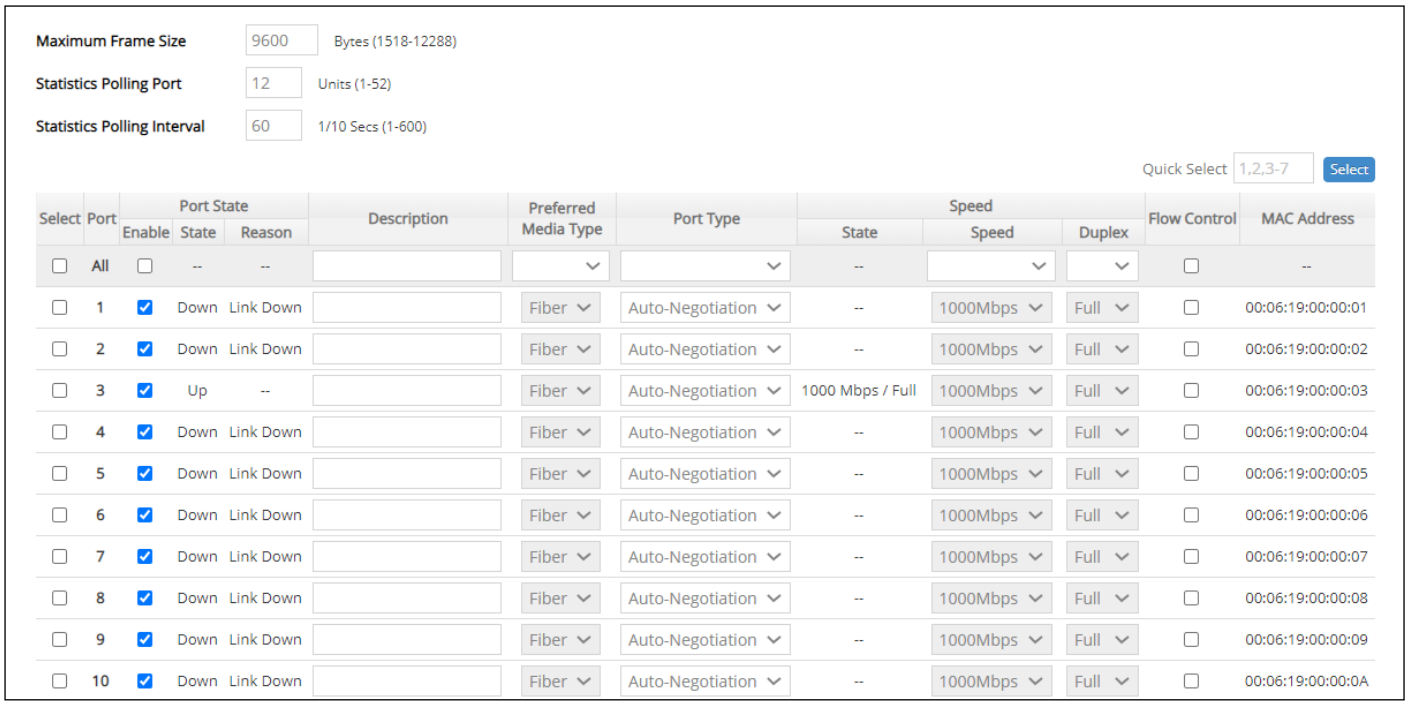
3. **Port Packet Error Statistics:** View each port's traffic condition of error packets, e.g. CRC, fragment, Jabber, etc.

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

5. **Port Mirroring:** Set up TX/RX source port(s) to mirror to the destination port for the traffic monitoring.

4.2.1 Port Setup & Status

Click the option **Port Setup &Status** from the **Port Management** menu and then the following screen page appears.



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

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

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

Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the Port Setup & Status table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Port: The number of the port.

Enable in Port State field**:** Enable or disable the current port state.

State in Port State field**:** View-only field that shows the current link status of the port, either up or down.

Reason in Port State field**:** View-only field that shows the cause of port's link-down state.

Description: Enter a unique description for the port. Up to 35 alphanumeric characters can be accepted.

Preferred Media Type: Select copper or fiber as the preferred media type.

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

State of Port in Speed field**:** View-only field that shows the current operation speed of ports, which can be 100Mbps or 1000Mbps in 1-48 SFP port(s) and 1000Mbps or 10Gbps in 49-52 SFP+ port(s), and the current operation duplex mode of the port, either Full or Half.

Speed of Port in Speed field**:** When you select “Manual” as port type, you can further specify the transmission speed (100Mbps/1000Mbps) of 1-48 SFP port(s) and (1000Mbps/10Gbps/Auto Speed) of 49-52 SFP+ port(s). When you select “Auto-Negotiation” as port type for fiber port(s), the transmission speed is 1000Mbps.

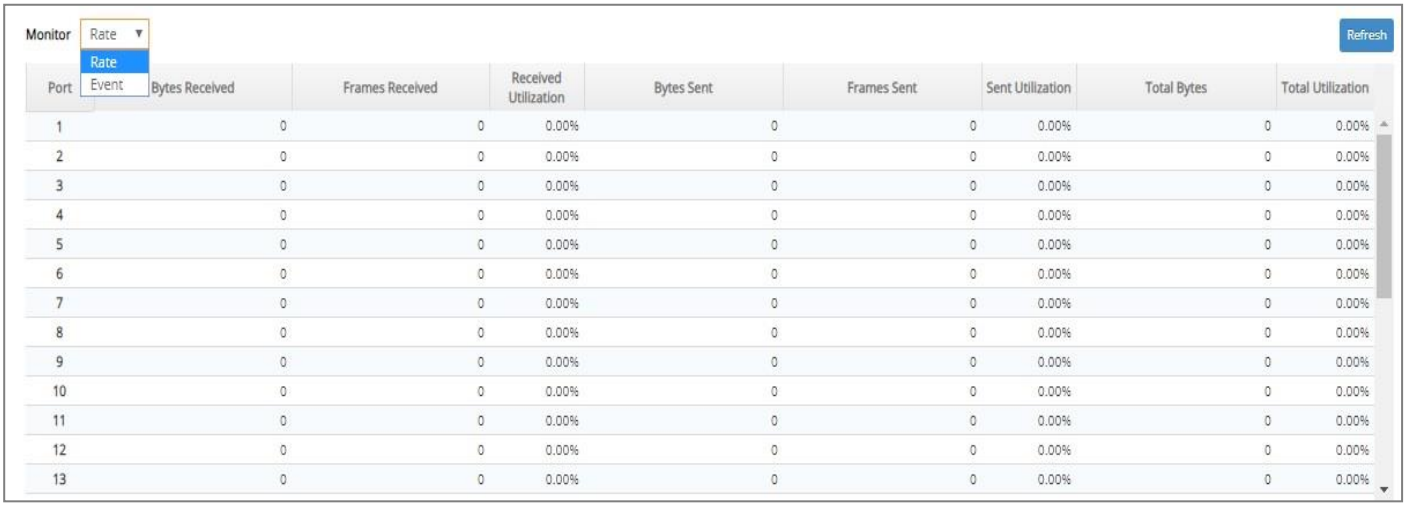
In 49-52 SFP+ port(s), when the port speed is configured as “Auto-speed”, the port(s) will behave as “Manual” and the transmission speed is 10Gbps if the detected speed displayed on **Maintenance->SFP Information-> SFP Port Info** webpage is 10Gbps; and if the detected speed displayed on this webpage is 1Gbps, the port(s) will behave as “Auto-Negotiation” and the transmission speed is 1Gbps. However, the port(s) will automatically enter “Auto-sensing” mode if the port speed is failed to detect.

Duplex of Port in Speed field**:** In Fiber ports, only the full-duplex operation mode is allowed.

Flow Control: Enable or disable the flow control.

4.2.2 Port Traffic Statistics

In order to view the real-time port traffic statistics of the Managed Switch, select the option **Port Traffic Statistics** from the **Port Management** menu and then the following screen page appears.



Monitor: Choose the way of representing Port Traffic Statistics from the pull-down menu. Either “Rate” or “Event” option can be chosen.

Bytes Received: Total bytes received from each port.

Frames Received: Total frames received from each port.

Received Utilization: The ratio of each port receiving traffic and current port’s total bandwidth.

Bytes Sent: The total bytes sent from current port.

Frames Sent: The total frames sent from current port.

Sent Utilization: The ratio of real sent traffic to the total bandwidth of current ports.

Total Bytes: Total bytes of receiving and sending from current port.

Total Utilization: The ratio of real received and sent traffic to the total bandwidth of current ports.

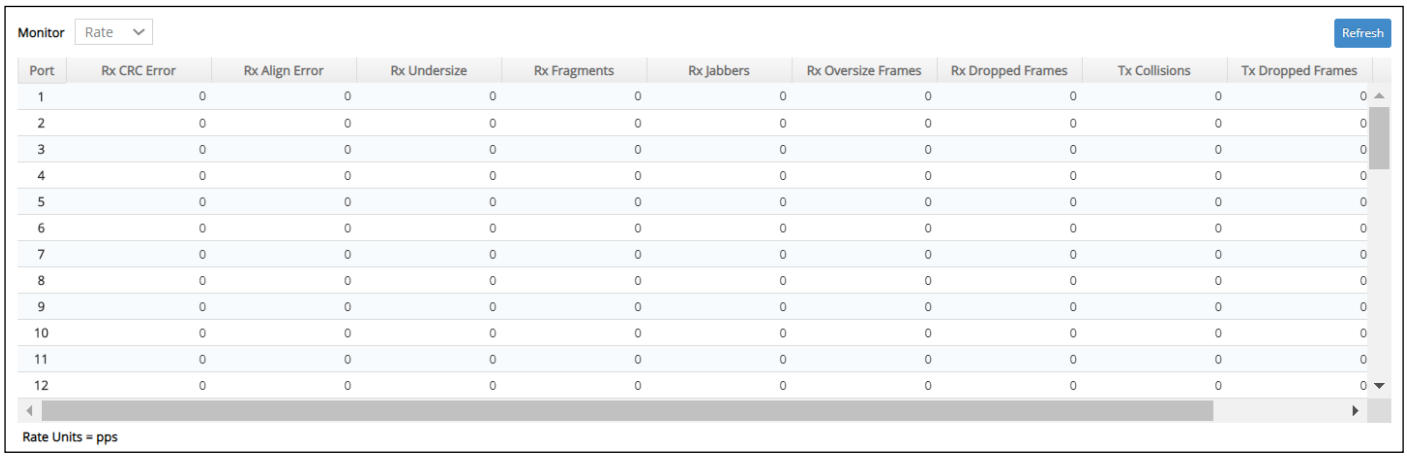
Refresh: Click **Refresh** to update the latest port traffic statistics.

Clear button in Clear Counters field**:** Clear the statistics of the corresponding port if “Event” option is chosen from **Monitor** pull-down menu.

Clear All: This will clear all ports’ counter values and be set back to zero if “Event” option is chosen from **Monitor** pull-down menu.

4.2.3 Port Packet Error Statistics

Port Packet Error Statistics mode counters allow users to view the port error of the Managed Switch. The event mode counters are calculated since the last time that counter was reset or cleared. Select the option **Port Packet Error Statistics** from the **Port Management** menu and then the following screen page appears.



Monitor: Choose the way of representing the Port Packet Error Statistics from the pull-down menu. Either “Rate” or “Event” option can be chosen.

RX CRC/Align Error: CRC/Align Error frames received.

RX Undersize: Undersize frames received.

RX Fragments: Fragments frames received.

RX Jabbers: Jabber frames received.

RX Oversize Frames: Oversize frames received.

RX Dropped Frames: Drop frames received.

TX Collisions: Each port’s Collision frames.

TX Dropped Frames: Drop frames sent.

Total Errors: Total error frames received.

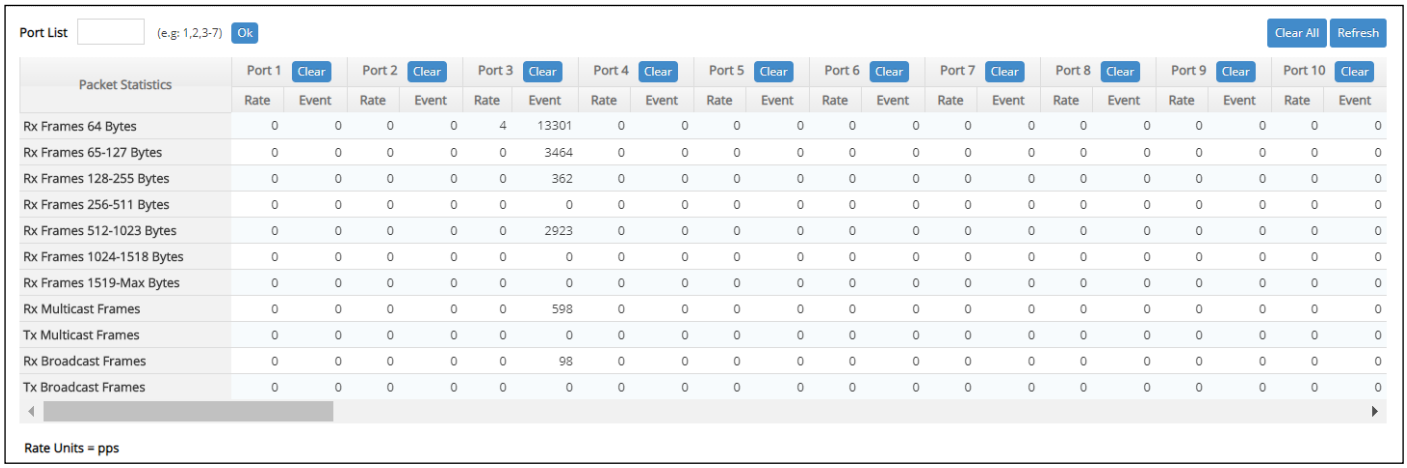
Refresh: Click **Refresh** to update the latest port packet error statistics.

Clear button in Clear Counters field**:** Clear the statistics of the corresponding port if “Event” option is chosen from **Monitor** pull-down menu.

Clear All: This will clear all ports’ counter values and be set back to zero if “Event” option is chosen from **Monitor** pull-down menu.

4.2.4 Port Packet Analysis Statistics

Port Packet Analysis Statistics mode counters allow users to view the port analysis history of the Managed Switch in both “Rate” and “Event” representing ways. The event mode counters are calculated since the last time that counter was reset or cleared. Select the option **Port Packet Analysis Statistics** from the **Port Management** menu and then the following screen page appears.



Port List: Enter the preferred port number (e.g.1, 2, 3-7) and then press the **OK** button, the port packet analysis statistics of the specified port(s) will be displayed immediately.

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 1024-1518 Bytes: 1024-1518 bytes frames received.

RX Frames 1519-Max Bytes: Over 1519 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.

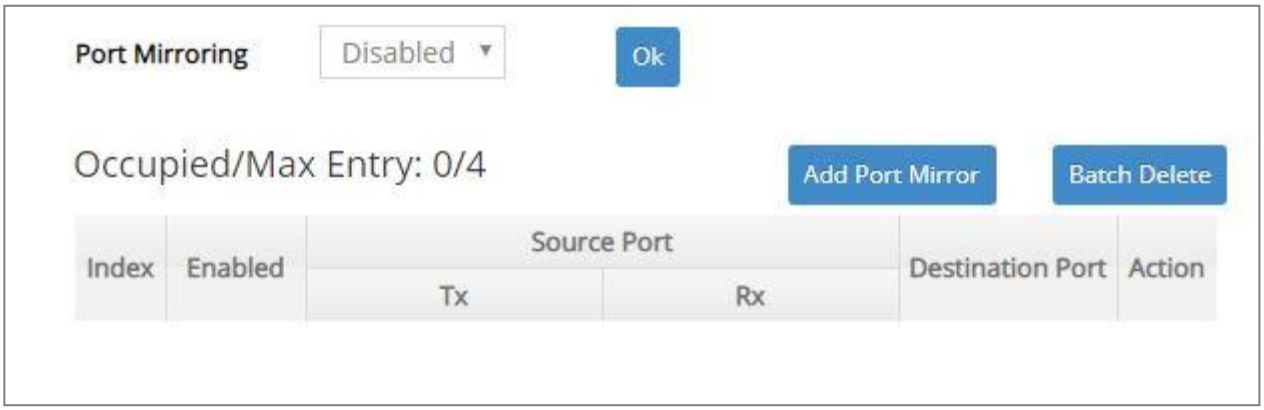
Refresh: Click **Refresh** to update the latest port packet analysis statistics.

Clear button of Per Port**:** Clear the statistics of the corresponding port.

Clear All: This will clear all ports' counter values and be set back to zero.

4.2.5 Port Mirroring

In order to allow the destination port to mirror the source port(s) and enable traffic monitoring, select the option **Port Mirroring** from the **Port Management** menu and then the following screen page appears. Please note that functions of Port Isolation and Port Mirroring cannot be enabled concurrently. When you enable Port Isolation function, Port Mirroring function will be disabled automatically, and vice versa.



This table will display the overview of each configured port mirroring. Up to 4 sets of port mirroring can be set up.

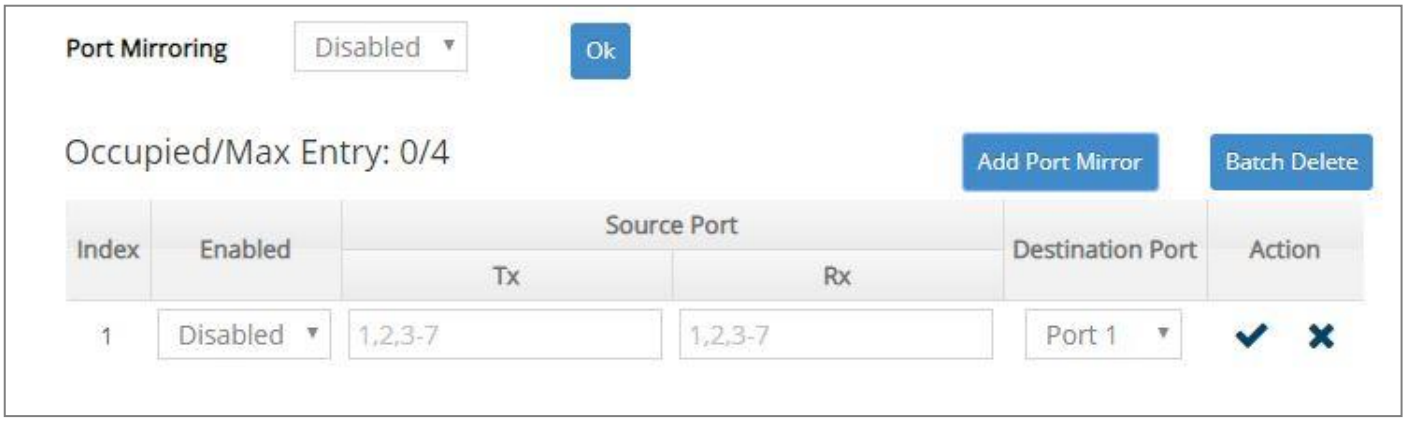
Port Mirroring: Globally enable or disable the Port Mirroring function. Click **OK**, the new setting will be taken effect immediately.

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total port mirroring(s) that have already been created.

Max: This shows the maximum number available for the port mirroring. The maximum number is 4.

Click **Add Port Mirror** to add a new port mirroring entry and then the following screen page appears for the further port mirroring settings.



Enabled: Enable or disable the specific port mirroring.

TX Source Port: Input the port number (e.g.1, 2, 3-7) to specify the transmitting packets of preferred source port(s) for mirroring. Please note that the port selected as the destination port cannot be the source port.

RX Source Port: Input the port number (e.g.1, 2, 3-7) to specify the receiving packets of preferred source port(s) for mirroring. Please note that the port selected as the destination port cannot be the source port.

Destination Port: Choose from port 1 to port 28 from the pull-down menu to designate the destination port. Please note that the destination port of Index 1~4 port mirroring cannot be the same.

Click when the settings are completed, this new port mirroring will be listed on the port mirroring table, or click to cancel the settings.

Click the icon to modify the settings of a specified port mirroring.

Click the icon to remove a specified port mirroring entry and its settings from the port mirroring table. Or click **Batch Delete** to remove a number of /all port mirrorings at a time by clicking on the checkbox belonging to the corresponding port mirroring in the **Action** field and then click **Delete Select Item**, the selected port mirroring(s) will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

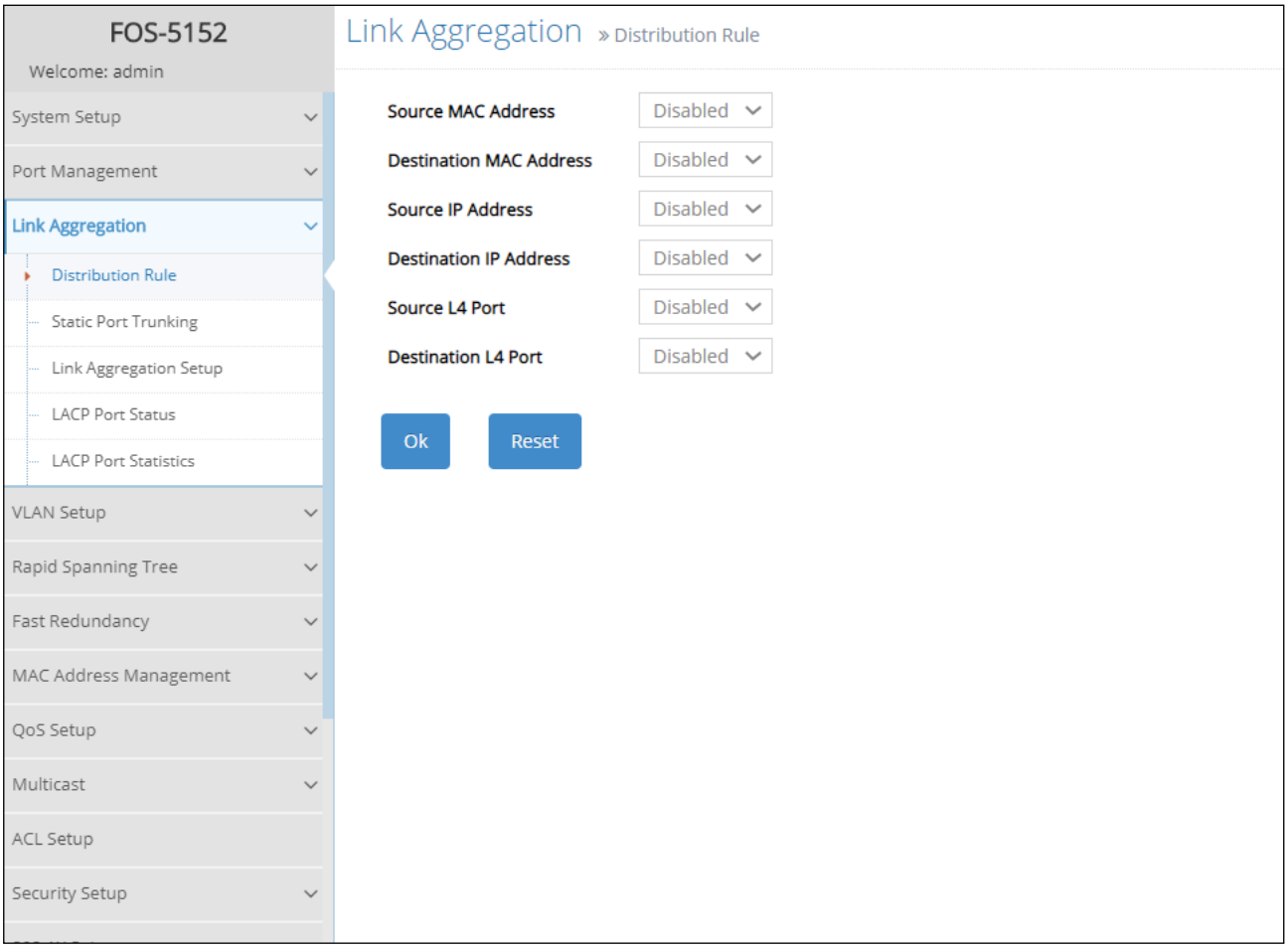
4.3 Link Aggregation

Link aggregation is an inexpensive way to set up a high-speed backbone network that transfers much more data than any one single port or device can deliver 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 and 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.

This Managed switch supports 2 link aggregation modes: static **Port Trunk** and dynamic **Link Aggregation Control Protocol (LACP)** using the IEEE 802.3ad standard. These allow several devices to communicate simultaneously at their full single-port speed while not allowing any one single device to occupy all available backbone capacities.

Click the folder **Link Aggregation** from the **Main Menu** and then 5 options within this folder will be displayed as follows.



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

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

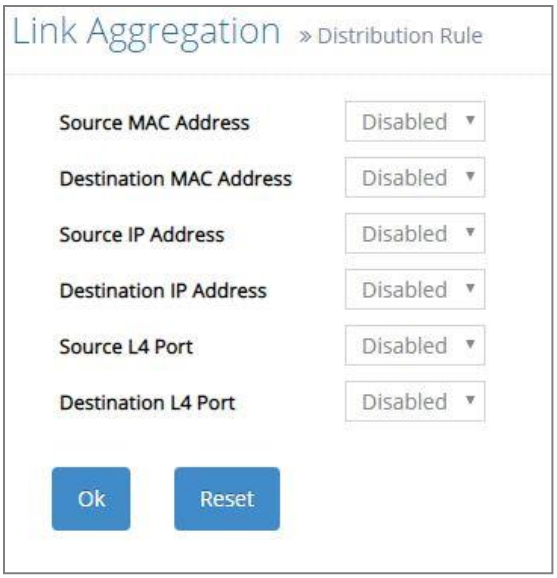
3. **Link Aggregation Setup:** Set up the configuration of LACP on all or some ports.

4. **LACP Port Status:** View the LACP port status.

5. **LACP Port Statistics:** View the LACP port statistics.

4.3.1 Distribution Rule

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



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

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

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

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

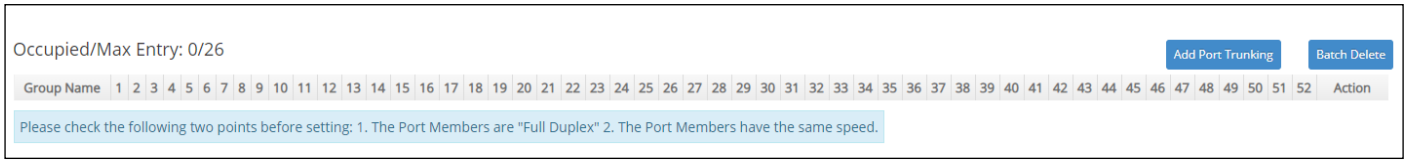
Destination IP Address: Enable or disable packets according to Destination IP address.

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

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

4.3.2 Static Port Trunking

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



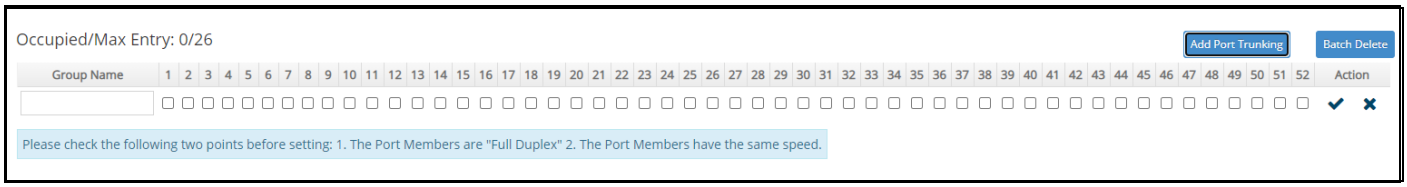
The Managed Switch allows users to create 26 trunking groups. Each group consists of 2 to 8 links (ports).

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total registered trunking groups.

Max: This shows the maximum number available for registration. The maximum number is 26.

Click **Add Port Trunking** to create a new trunking group and then the following screen page appears for the further port trunking settings.



Group Name: Specify the trunking group name. Up to 15 alphanumeric characters can be accepted.

Port Members: Click on the checkbox of the corresponding port number to 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 8 ports in each trunking group.

- Each port can only be grouped in one group.

- If the port is already enabled in LACP Port Configuration, it cannot be grouped anymore.

Click ✔ when the settings are completed, this new trunking group will be listed on the port trunking group table, or click ✖ to cancel the settings.

Click the ✎ icon to modify the settings of a registered trunking group.

Click the 🗑 icon to remove a specified registered trunking group and its settings from the port trunking group table. Or click **Batch Delete** to remove a number of / all trunking groups at a time by clicking on the checkbox belonging to the corresponding trunking group in the **Action** field and then click **Delete Select Item**, these selected trunking groups will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

***NOTE*:** *All trunking ports in the group must be members of the same VLAN, and their Spanning Tree Protocol (STP) status and QoS default priority configurations must be identical. Port locking, port mirroring and 802.1X cannot be enabled on the trunking group. Furthermore, the LACP aggregated links must all be of the same speed and should be configured as full duplex.*

4.3.3 Link Aggregation Setup

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.

Click the option **Link Aggregation Setup** from the **Link Aggregation** menu and then the screen page is shown below. It is necessary to set up both “Key Value” and “Role” two parameters for the designated ports when creating a LACP(dynamic Link Aggregation) group. For more details on these settings, please refer to the following description in this section.

Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the Link Aggregation Setup table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Key Value: 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.

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

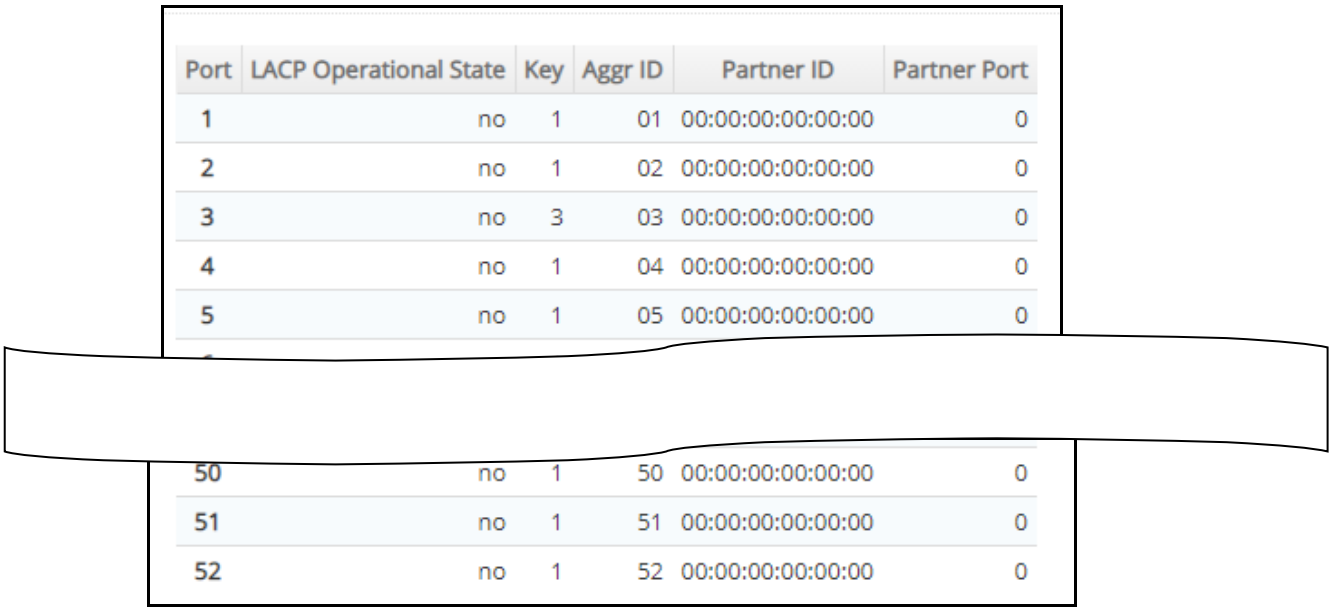
Disable: Disable LACP on specified port(s).

Active: 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: 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.

4.3.4 LACP Port Status

LACP Port Status allows users to view a list of all LACP ports’ information. Select the option **LACP Port Status** from the **Link Aggregation** menu and then the following screen page appears.



Port	LACP Operational State	Key	Aggr ID	Partner ID	Partner Port
1	no	1	01	00:00:00:00:00:00	0
2	no	1	02	00:00:00:00:00:00	0
3	no	3	03	00:00:00:00:00:00	0
4	no	1	04	00:00:00:00:00:00	0
5	no	1	05	00:00:00:00:00:00	0
50	no	1	50	00:00:00:00:00:00	0
51	no	1	51	00:00:00:00:00:00	0
52	no	1	52	00:00:00:00:00:00	0

In this page, you can find the following information about LACP port status:

Port: The number of the port.

LACP Operational State: The current operational state of LACP

Key: The current operational key for the LACP group.

Aggr ID: The ID of the LACP group.

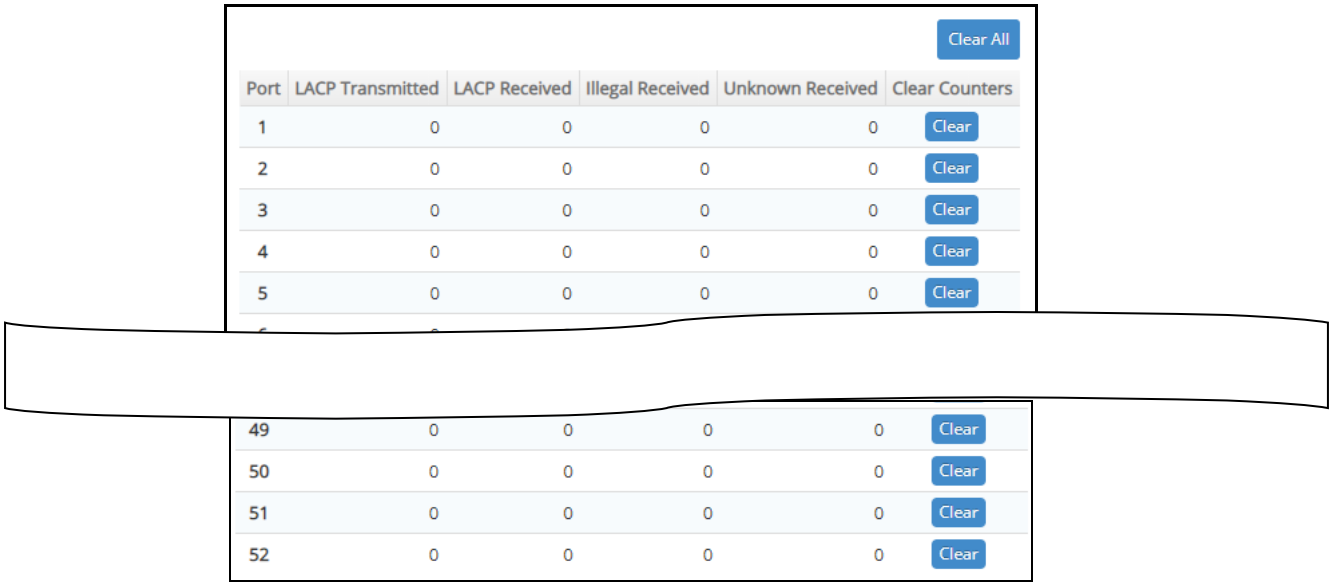
In LACP mode, link aggregation control protocol data unit (LACPDU) is used for exchanging information among LACP-enabled devices. After LACP is enabled on a port, the port sends LACPDUs to notify the remote system of its system LACP priority, system MAC address, port LACP priority, port number and operational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

4.3.5 LACP Port Statistics

In order to view the real-time LACP statistics status of the Managed Switch, select the option **LACP Port Statistics** from the **Link Aggregation** menu and then the following screen page appears.



Port: The port that LACP packets (LACPDU) are transmitted or received.

LACP Transmitted: The current LACP packets transmitted from the port.

LACP Received: The current LACP packets received from the port.

Illegal Received: The current Illegal packets received from the port.

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

Clear button in **Clear Counters** field**:** Clear the statistics of the corresponding port.

Clear All: Clear the statistics of all ports.

4.4 VLAN Setup

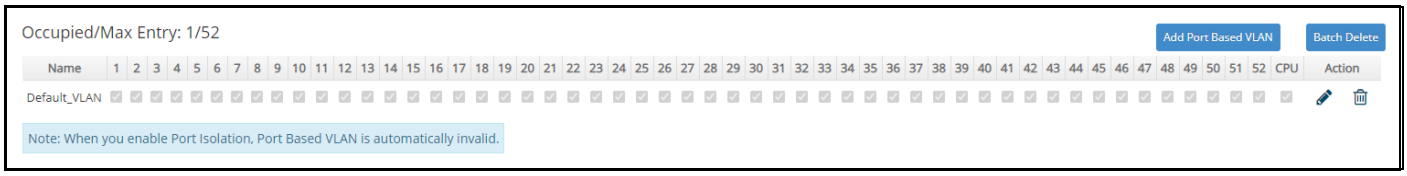
A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast 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. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

4.4.1 Port Based VLAN

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

The following screen page appears when you choose the option **Port Based VLAN** mode from the **VLAN Setup** menu.

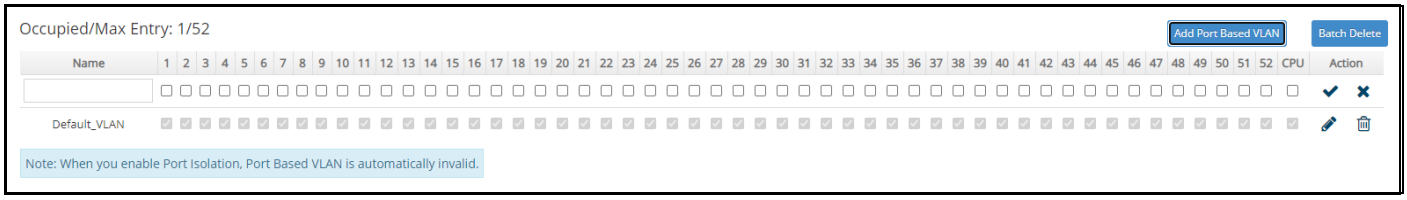


Since source addresses of the packets are listed in MAC address table of specific VLAN (except broadcast/multicast packets), in every VLAN the traffic between two ports will be two-way without restrictions.

Click **Add Port Based VLAN** to add a new VLAN and then the following screen page appears for the further Port-Based VLAN settings.

Click the icon to modify the settings of a specified VLAN.

Click the icon to remove a specified Port-Based VLAN and its settings from the Port-Based VLAN table. Or click **Batch Delete** to remove a number of / all Port-Based VLANs at a time by clicking on the checkbox belonging to the corresponding Port-Based VLAN in the **Action** field and then click **Delete Select Item**, these selected VLANs will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.



Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total Port-Based VLANs that have already been created.

Max: This shows the maximum number of Port-Based VLANs that can be created. The maximum number is 28.

Name: Use the default name or specify a name for your Port-Based VLAN.

Port Number: By clicking on the checkbox of the corresponding ports, it denotes that the selected ports belong to the specified Port-Based VLAN.

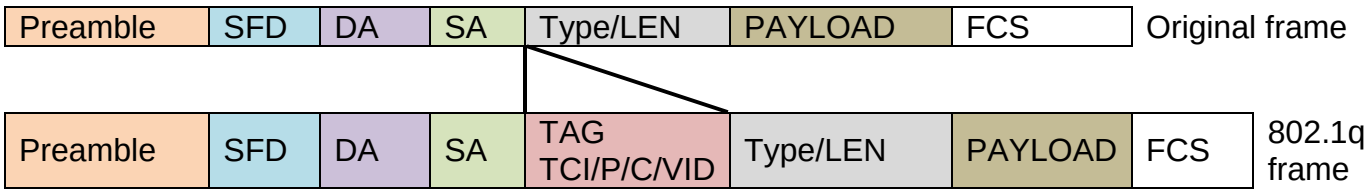
Click ✔ when the settings are completed, this new Port-Based VLAN will be listed on the Port-Based VLAN table, or click ✖ to cancel the settings.

4.4.2 802.1Q VLAN

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 to 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 8100 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 Canonical format - Ethernet 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 to understand.

- **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**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. 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**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

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

- **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, **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. These types of ports are 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 simultaneously with the 802.1Q tagged packets. 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. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.

- **DOT1Q-Tunnel Mode :**
  Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification.
  Using the IEEE 802.1Q tunneling feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using IEEE 802.1Q tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets. A port configured to support IEEE 802.1Q tunneling is called a *tunnel port*. When you configure tunneling, you assign a tunnel

port to a VLAN ID that is dedicated to tunneling. Each customer requires a separate service-provider VLAN ID, but that VLAN ID supports all of the customer's VLANs.
Customer traffic tagged in the normal way with appropriate VLAN IDs comes from an IEEE 802.1Q trunk port on the customer device and into a tunnel port on the service-provider edge switch. The link between the customer device and the edge switch is asymmetric because one end is configured as an IEEE 802.1Q trunk port, and the other end is configured as a tunnel port. You assign the tunnel port interface to an access VLAN ID that is unique to each customer.

- **Selecitve Q-in-Q mode:**
  Selective Q-in-Q mode is specially designed for the port that enabled Selective Q-in-Q function to separate users & service by encapsulating VLAN ID.

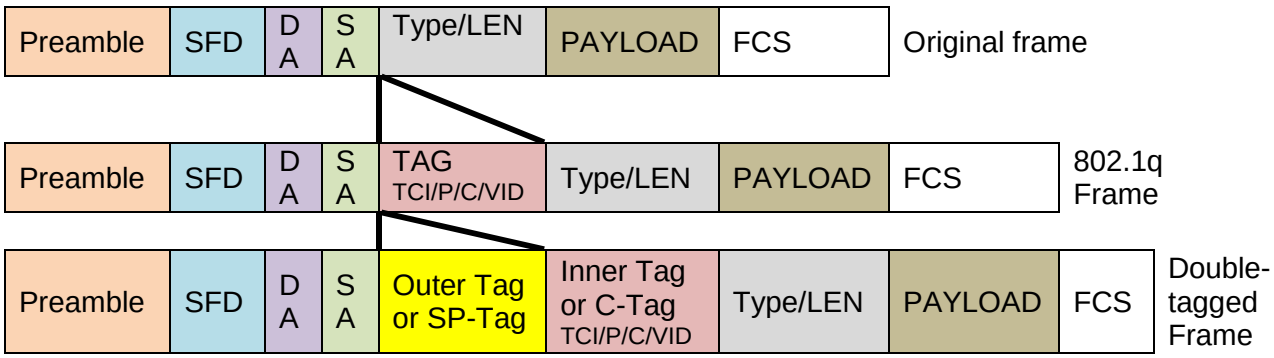
Example : PortX configuration

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 VID 10,11 and 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 VID 10,11 and 12 PortX receives **Untagged** packets and add PVID 20
Trunk-VLAN = 10,11,12 Access-VLAN = 20 **Mode = Dot1q-tunnel**	PortX is a **Dot1q-tunnel Port** PortX's **VID** is ignored. PortX's **PVID** is 20 PortX sends **Untagged** or **Tagged** packets VID 20 PortX receives **Untagged** and **Tagged** packets and add PVID 20(outer tag)
Trunk-VLAN = 10,11,12 Access-VLAN = 20 **Mode = Selective Q-in-Q**	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 VID 10,11 and 12 PortX receives **Untagged** packets and add PVID 20

4.4.3 Introduction to Q-in-Q (DOT1Q-Tunnel)

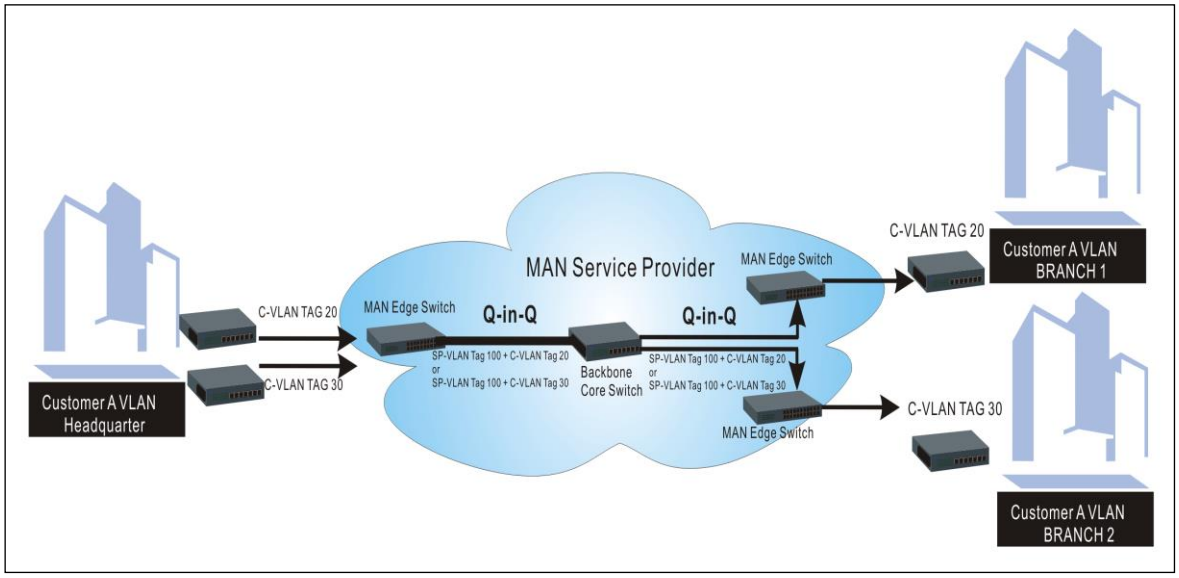
The IEEE 802.1Q double tagging VLAN is also referred to as Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1q VLAN space by tagging the inner tagged packets. In this way, a "double-tagged" frame is created so as to separate customer traffic within a service provider network. As shown below in "Double-Tagged Frame" illustration, an outer tag is added between source destination and inner tag at the provider network's edge. This can support C-VLAN (Customer VLAN) over Metro Area Networks and ensure complete separation between traffic from different user groups. Moreover, the addition of double-tagged space increases the

number of available VLAN tags which allow service providers to use a single SP-VLAN (Service Provider VLAN) tag per customer over the Metro Ethernet network.



Double-Tagged Frame Format

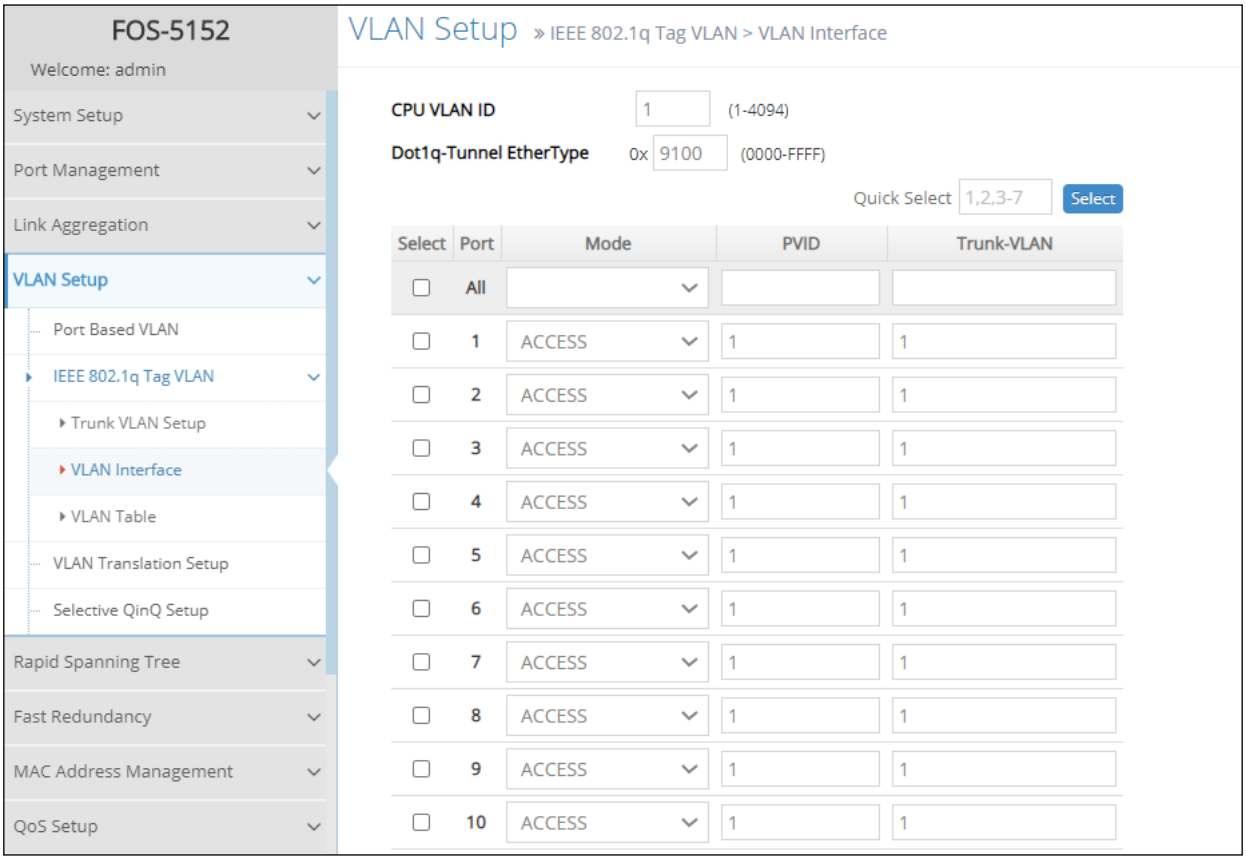
As shown below in "Q-in-Q Example" illustration, Headquarter A wants to communicate with Branch 1 that is 1000 miles away. One common thing about these two locations is that they have the same VLAN ID of 20, called C-VLAN (Customer VLAN). Since customer traffic will be routed to service provider's backbone, there is a possibility that traffic might be forwarded insecurely, for example due to the same VLAN ID used. Therefore, in order to get the information from Headquarter to Branch 1, the easiest way for the carrier to ensure security to customers is to encapsulate the original VLAN with a second VLAN ID of 100. This second VLAN ID is known as SP-VLAN (Service Provider VLAN) that is added as data enters the service provider's network and then removed as data exits. Eventually, with the help of SP-Tag, the information sent from Headquarter to Branch 1 can be delivered with customers' VLANs intactly and securely.



Q-in-Q Example

4.4.4 IEEE 802.1q Tag VLAN

The following screen page appears when you choose the option **IEEE 802.1q Tag VLAN** mode from the **VLAN Setup** menu and then select **VLAN Interface** function.



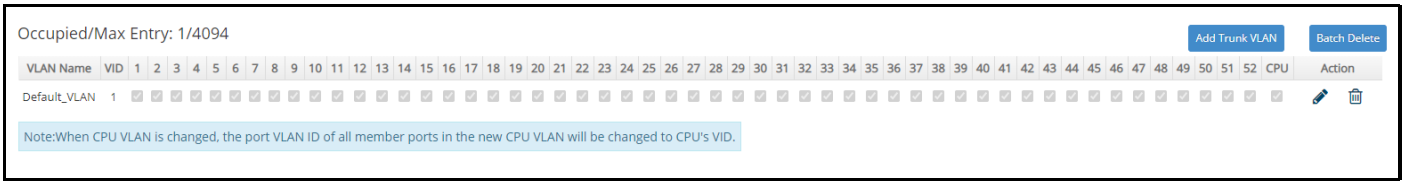
1. **Trunk VLAN Setup:** To create, modify or remove IEEE 802.1q Tag VLAN settings.

2. **VLAN Interface:** To set up VLAN mode, create 802.1q VLAN on the selected port(s), and set up CPU VLAN ID.

3. **VLAN Table:** View the IEEE802.1q VLAN table of the Managed Switch.

4.4.4.1 Trunk VLAN Setup

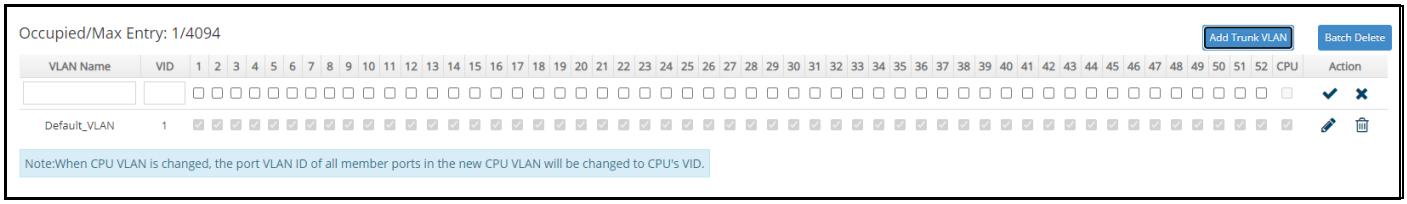
The following screen page appears if you choose **Trunk VLAN Setup** function.



Click **Add Trunk VLAN** to add a new VLAN and then the following screen page appears for the further IEEE 802.1q Tag VLAN settings.

Click the icon to modify the settings of a specified 802.1q VLAN.

Click the icon to remove a specified 802.1q VLAN and its settings from the IEEE 802.1q Tag VLAN Setup table. Or click **Batch Delete** to remove a number of / all 802.1q VLANs at a time by clicking on the checkbox belonging to the corresponding 802.1q VLAN in the **Action** field and then click **Delete Select Item**, these selected VLANs will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.



Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total 802.1q VLANs that have already been created.

Max: This shows the maximum number of 802.1q VLANs that can be created. The maximum number is 4094.

VLAN Name: Use the default name or specify a VLAN name.

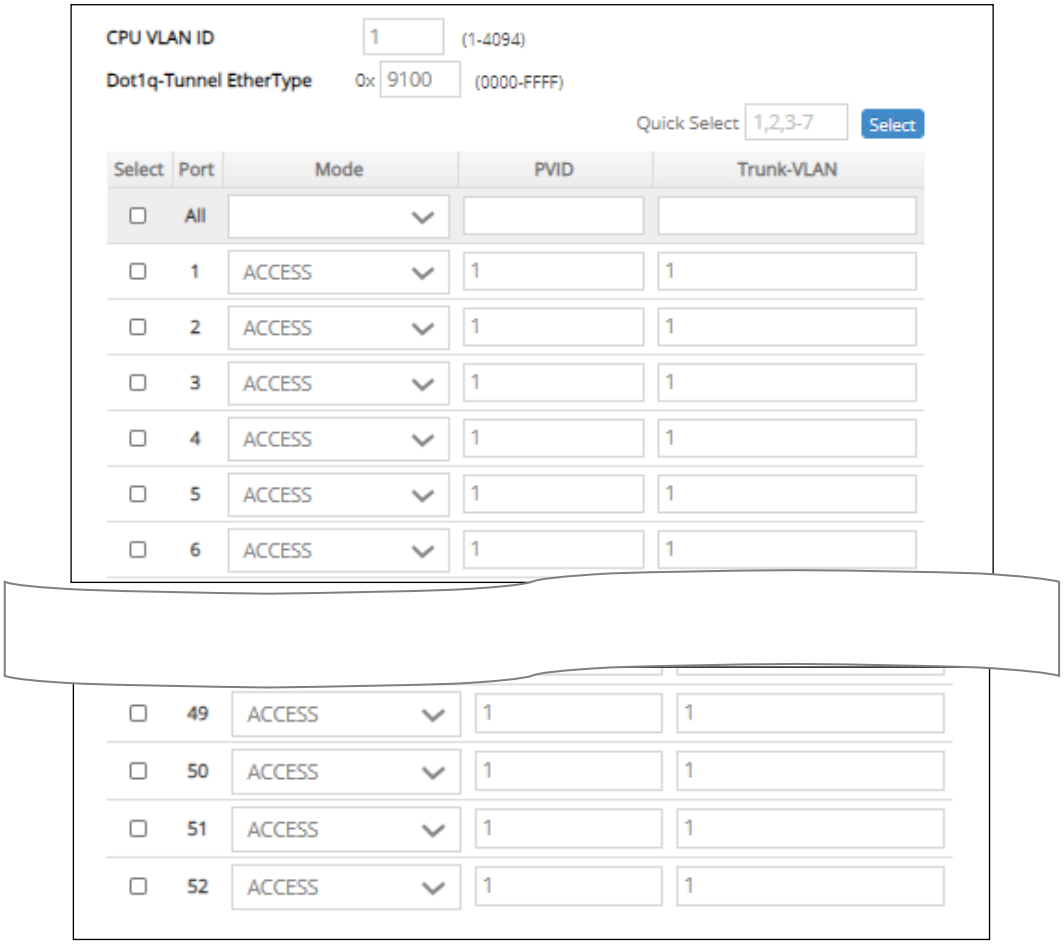
VID: Specify the VLAN ID of the VLAN. Valid range: 1-4094.

VLAN Members: If you check the ports, it denotes that the ports selected belong to the specified VLAN group.

Click ✔ when the settings are completed, this new 802.1q VLAN will be listed on the IEEE 802.1q Tag VLAN Setup table, or click ✖ to cancel the settings.

4.4.4.2 VLAN Interface

The following screen page appears if you choose **VLAN Interface** function.



CPU VLAN ID: Specify an existing VLAN ID.

Dot1q-Tunnel EtherType: Configure outer-VLAN's ethertype. (Range: 0000~FFFF, Default: 9100).

Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the VLAN Interface table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Mode: Pull down the list in the **Mode** field and select the appropriate mode for each port. The port behavior of each mode is listed as the following table.

Access: Set the selected port to the access mode (untagged).

Trunk: Set the selected port to the trunk mode (tagged).

Trunk-Native: Enable native VLAN for untagged traffic on the selected port.

DOT1Q-Tunnel: Set the selected port to the dot1q-tunnel mode (tagged and untagged).

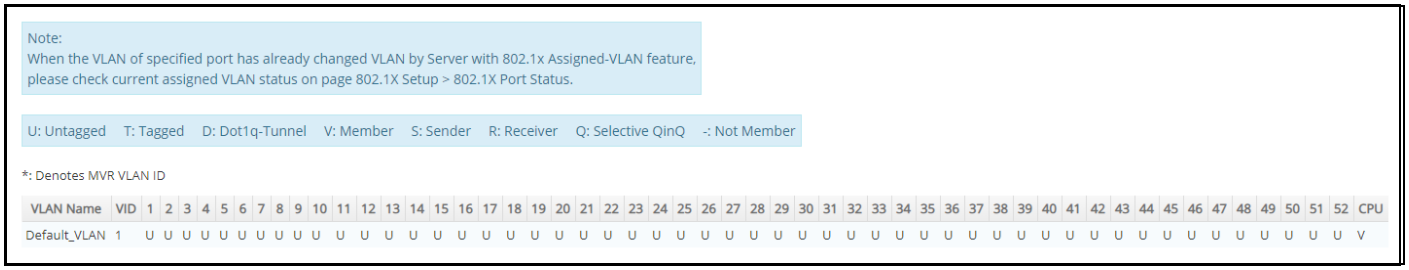
<table>
<tr><th>Mode</th><th colspan="2">Port Behavior</th></tr>
<tr><td rowspan="2">Access</td><td colspan="2">Receive untagged packets only. Drop tagged packets.</td></tr>
<tr><td colspan="2">Send untagged packets only.</td></tr>
<tr><td rowspan="2">Trunk</td><td colspan="2">Receive tagged packets only. Drop untagged packets.</td></tr>
<tr><td colspan="2">Send tagged packets only.</td></tr>
<tr><td rowspan="3">Trunk Native</td><td rowspan="2">Receive both untagged and tagged packets</td><td>Untagged packets: PVID is added</td></tr>
<tr><td>Tagged packets: Stay intact</td></tr>
<tr><td colspan="2">When sending packets, PVID and VID will be compared.
If PVID and VID are the same, PVID will be removed.
If PVID and VID are different, the packets with the original tag (VID) will be sent.</td></tr>
<tr><td>DOT1Q-Tunnel</td><td colspan="2">Receive all tag and untag packets.
Send the packets with the outer tag marked as PVID.</td></tr>
</table>

PVID: Specify the selected ports' Access-VLAN ID (PVID).

Trunk-VLAN: Specify the selected ports' Trunk-VLAN ID (VID).

4.4.4.3 IEEE 802.1q VLAN Table

The following screen page appears if you choose **VLAN Table** function. Please note that when the VLAN of specified port has already been changed by 802.1x Server through the **802.1x Assigned-VLAN** function, please check the current assigned VLAN status on the **802.1X Setup > 802.1X Port Status** webpage that we will describe in Section 4.11.



VLAN Name: View-only field that shows the VLAN name. If the VLAN name belongs to an "Enabled" multicast VLAN ID, it will be automatically changed into the one same as MVR name configured in **MVR > MVR System Setup** function.

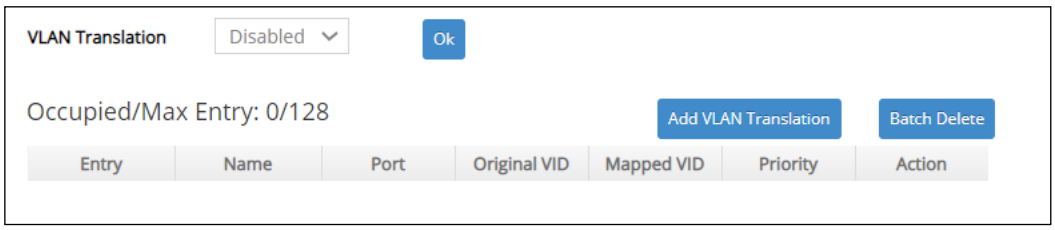
VID: View-only field that shows the ID of the VLAN. And VID marked * stand that it is a MVR VLAN ID.

4.4.5 VLAN Translation Configuration

Besides the aforementioned ways of creating VLANs, another way to establish the translated VLANs is to configure VLAN ID translation (or VLAN mapping) on trunk ports connected to a customer network to map the original VLANs to the translated VLANs. Through this VLAN ID translation, it will save much effort in massive Ethernet network deployments.

Packets entering the trunk port are mapped to a translated VLAN based on the port number and the original VLAN ID of the packet. In a typical metro deployment, VLAN mapping takes place on user network interfaces. Because the VLAN ID is mapped to the translated VLAN on ingress, all forwarding operations on the Managed Switch are performed with the usage of the translated VLAN information rather than the original VLAN information.

Click the option **VLAN Translation Setup** from the **VLAN Setup** menu and then the following screen page appears.



This table will display the overview of each configured VLAN mapping rule. Up to 128 VLAN mapping rules can be set up.

VLAN Translation: Enable or disable VLAN translation function globally. Click **OK** provided for VLAN Translation function, the new settings will be taken effect immediately.

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total VLAN mapping rules that have already been created.

Max: This shows the maximum number available for VLAN mapping rules. The maximum number is 128.

Click **Add VLAN Translation** to add a new VLAN mapping rule and then the following screen page appears for the further VLAN translation settings.

Entry: View-only field. This shows the number of VLAN mapping rule that is currently created.

Name: Specify a name for the VLAN mapping rule. Up to 32 alphanumeric characters can be accepted.

Port: Specify one preferred trunk port used for the VLAN ID translation. (For more details on turnk port settings, please refer to Section 4.4.4.2 “VLAN Interface”.)

Original VID: Specify the original VLAN ID entering the switch from the customer network for the VLAN ID translation.Valid range: 1-4094.

Mapped VID: Specify the preferred VLAN ID that the assigned original VID will be translated. Valid range: 1-4094.

NOTE:
1. Different Mapped VIDs cannot be assigned to the trunk port with the same original VID.
2. Different original VIDs belonging to the specific port cannot be translated into the same Mapped VID.

Priority: Specify the preferred priority bit value to replace the original priority level in the tagged packets. Valid range: 0~7.

Click ✔ when the settings are completed, this new rule will be listed on the VLAN mapping rule table, or click ✖ to cancel the settings.

Click the ✎ icon to modify the settings of a specified VLAN mapping rule.

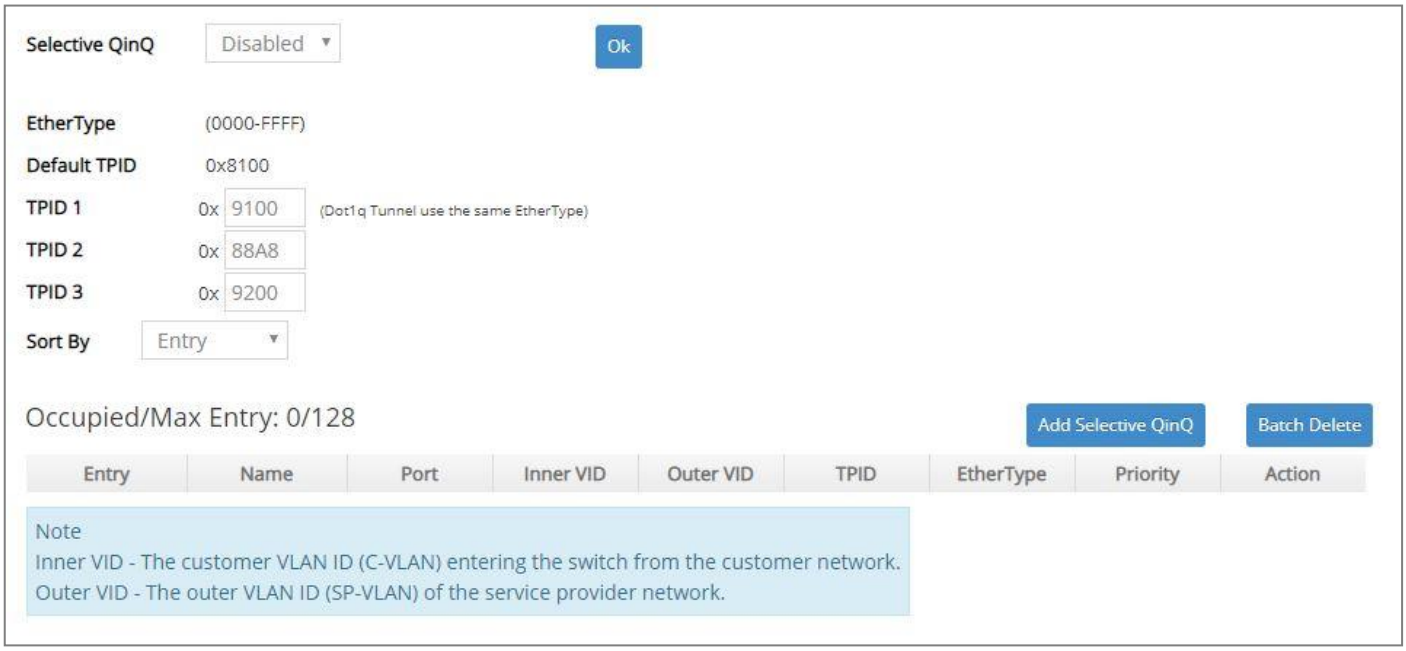
Click the 🗑 icon to remove a specified VLAN mapping rule and its settings from the VLAN mapping rule table. Or click **Batch Delete** to remove a number of / all VLAN mapping rules at a time by clicking on the checkbox belonging to the corresponding rule in the **Action** field and then click **Delete Select Item**, these selected rules will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

4.4.6 Selective Q-in-Q Configuration

Selective Q-in-Q, an extension of DOT1Q-Tunnel, is implemented based on both interfaces and VLAN IDs. An interface configured with Selective Q-in-Q can forward packets based on a single VLAN tag or double VLAN tags. Additionally, Selective Q-in-Q adds different outer VLAN tags to packets carrying different inner VLAN IDs. It marks the outer 802.1p fields and adds different outer VLAN tags to packets upon the 802.1p fields in inner VLAN tags.

In the VLAN application, not only does Selective Q-in-Q make a distinction between service provider's and customer's networks but provides extensive service functions as well as the more flexible networking.

Click the option **Selective QinQ Setup** from the **VLAN Setup** menu and then the following screen page appears.



This table will display the overview of each configured Selective Q-in-Q rule. Up to 128 Selective Q-in-Q rules can be set up.

Selective QinQ: Enable or disable Selective Q-in-Q function globally.

EtherType: View-only field that shows the vaild range (0000~FFFF) of outer VLAN's ethertype for the following 4 TPIDs (Tag Protocol Identifier) that the system supports. The default configuration of these TPIDs is as follows:

Default TPID = 8100 (A fixed value that cannot be changed.)

TPID 1 = The default setting is 9100. (Use the same EtherType as Dot1q Tunnel)

TPID 2 = The default setting is 88A8.

TPID 3 = The default setting is 9200.

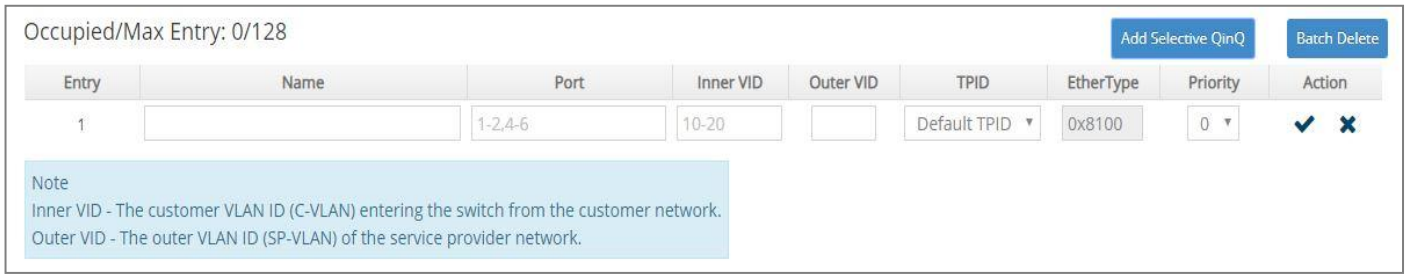
Click **OK**, the new settings will be taken effect immediately.

Sort By: Sort all of the registered Selective Q-in-Q rules by selecting **Entry/Port/Inner VID/Outer VID** option from the **Sort By** pull-down menu.

Occupied/Max Entry: View-only field.

> **Occupied:** This shows the amount of total Selective Q-in-Q rules that have already been created.
>
> **Max:** This shows the maximum number available for Selective Q-in-Q rules. The maximum number is 128.

Click **Add Selective Q-in-Q** to add a new Selective Q-in-Q rule and then the following screen page appears for the further Selective Q-in-Q settings.



Entry: View-only field. This shows the number of Selective Q-in-Q rule that is currently created.

Name: Specify a name for the Selective Q-in-Q rule. Up to 32 alphanumeric characters can be accepted.

Port: Specify the preferred selective-qinq port(s) (e.g. 1,2,3-7) used for the Selective Q-in-Q rule. (For more details on turnk-native port settings, please refer to Section 4.4.4.2 “VLAN Interface”.)

Inner VID: Specify the customer VLAN ID (C-VLAN) that enters the switch from customer’s network. You can enter one or a consecutive string of VLAN IDs, for example, 100 or 100-110. Valid range: 1-4094.

Outer VID: Specify the outer VLAN ID (SP-VLAN) of the service provider network. Valid range: 1-4094.

NOTE:
1. In a Selective Q-in-Q rule, *Inner VID can be the same as Outer VID.*
2. On the same port, Inner VID cannot be duplicated in different Selective Q-in-Q rules*.*

TPID: Specify the preferred TPID to the Selective Q-in-Q rule from the pull-down list.

EtherType: View-only field that shows the current VLAN's ethertype of TPID you select.

Priority: Set up 802.1p bit value for the outer VID. Valid range: 0~7.

Click ✔ when the settings are completed, this new rule will be listed on the Selective Q-in-Q rule table, or click ✖ to cancel the settings.

Click the  icon to modify the settings of a specified Selective Q-in-Q rule.

Click the  icon to remove a specified Selective Q-in-Q rule and its settings from the Selective Q-in-Q rule table. Or click **Batch Delete** to remove a number of / all Selective Q-in-Q rules at a time by clicking on the checkbox belonging to the corresponding rule in the **Action** field and then click **Delete Select Item**, these selected rules will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

4.5 Rapid Spanning Tree

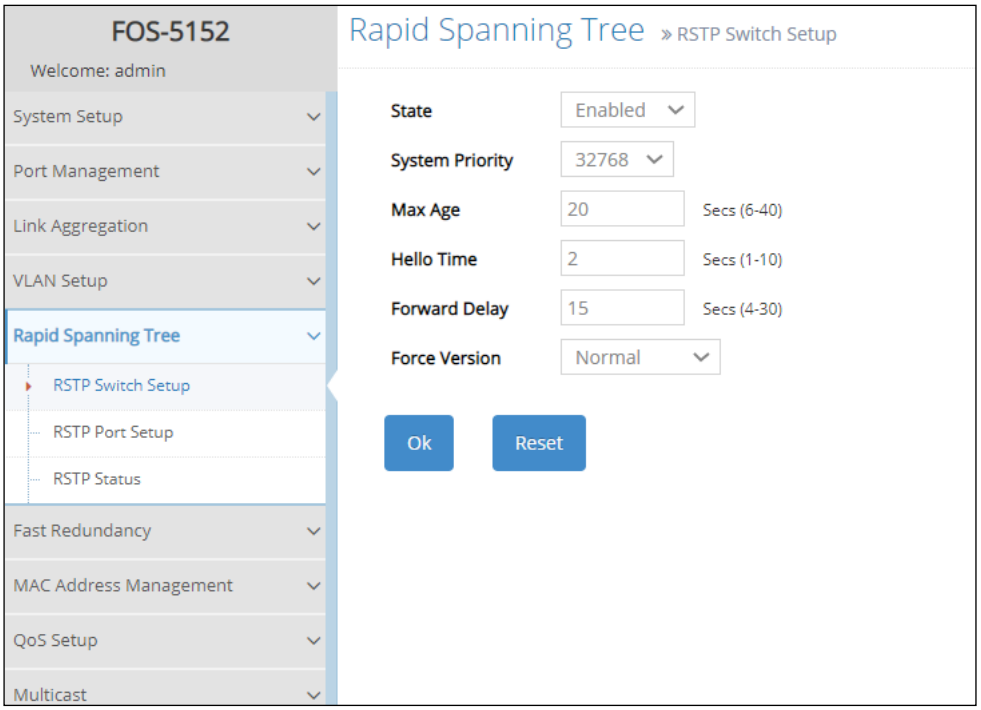
The Spanning Tree Protocol (STP), defined in the IEEE Standard 802.1D, creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches) and disables the links which are not part of that tree, leaving a single active path between any two network nodes.

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 **Main Menu** and then 3 options within this folder will be displayed as follows.



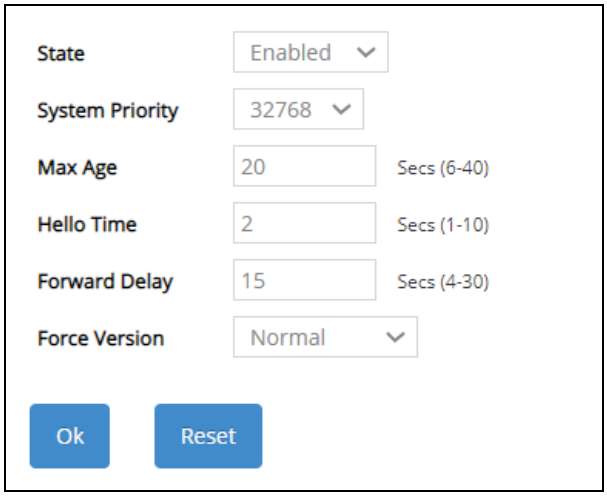
1. **RSTP Switch Setup:** Set up the system priority, max Age, hello time, forward delay time and force version.

2. **RSTP Port Setup:** Set up the RSTP state, path cost, priority, edge status, and point to point setting of each physical port.

3. **RSTP Status:** View RSTP VLAN Bridge, RSTP port status, and RSTP statistics.

4.5.1 RSTP Switch Setup

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



State: Enable or disable Rapid Spanning Tree function globally.

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

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

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

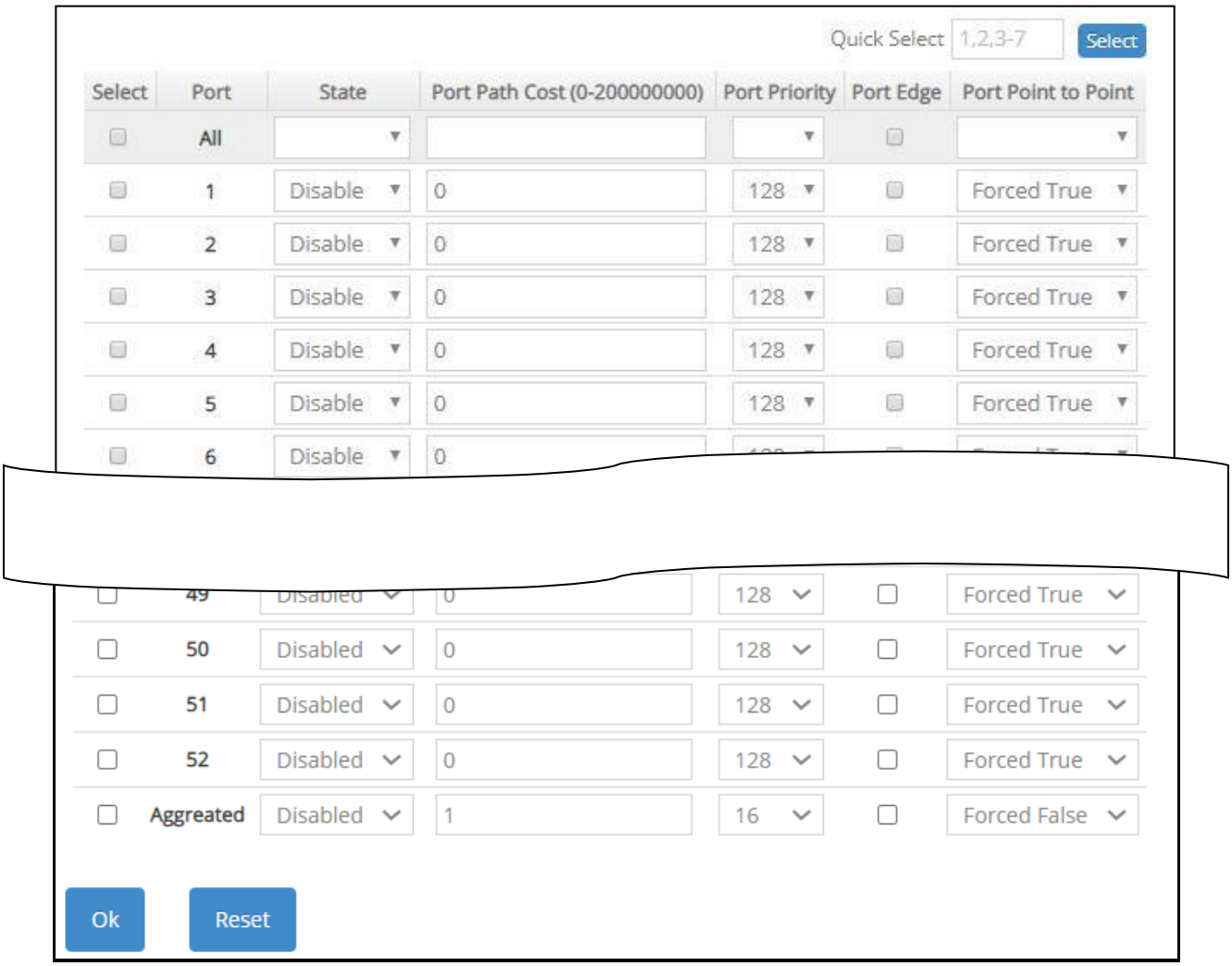
Hello Time: Periodically, a hello packet is sent out by the Root Bridge and the Designated Bridges that are used to communicate information about the topology throughout the entire Bridged Local Area Network.

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

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

4.5.2 RSTP Port Setup

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



Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the RSTP Port Setup table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Port: The number of the port.

State: Pull down the menu of the corresponding port number to enable or disable RSTP for each port. Default is disable.

Port Path Cost: This sets up the path cost of each port. The default value is “0”. “0” means auto-generated port path cost.

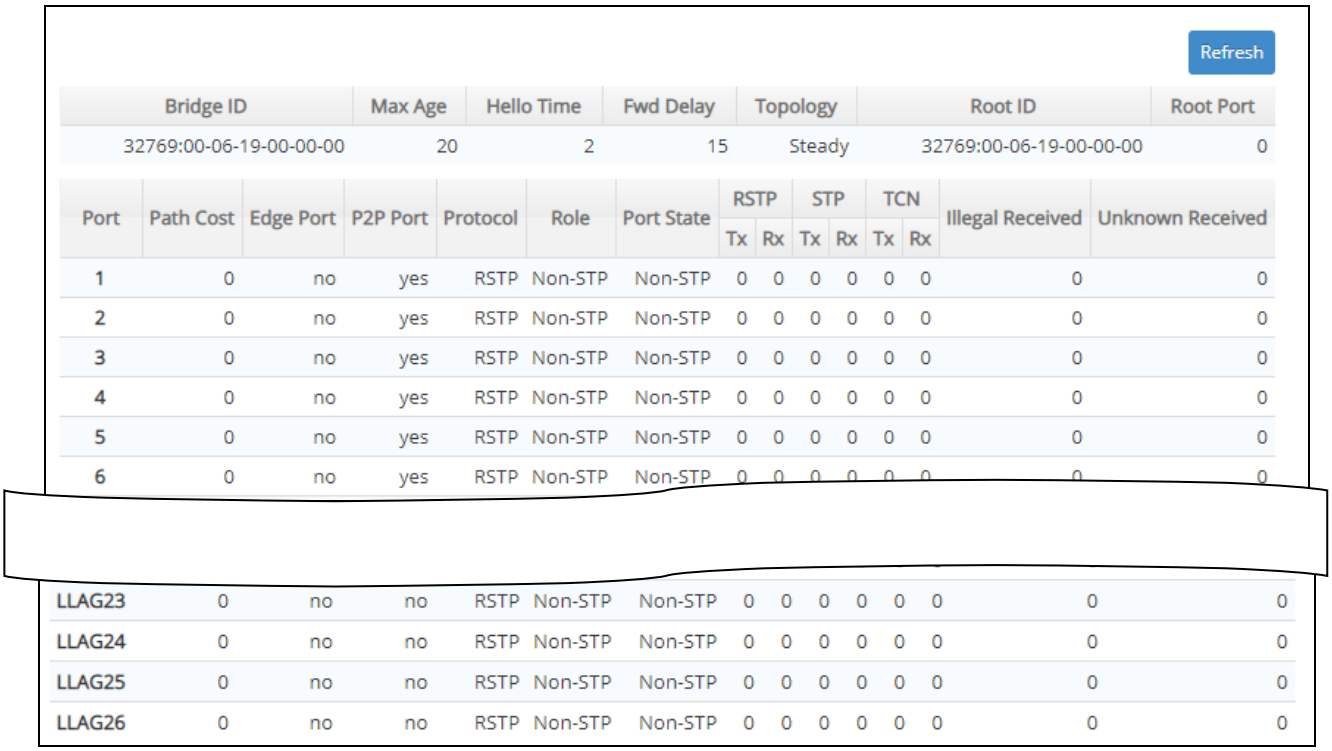
Port Priority: From the pull-down menu of the corresponding port number, you can choose Port Priority value between 0 and 240 for each port. The default value is “128”.

Port Edge: Click on the checkbox of the corresponding port number to enable or disable Port Edge for each port. Default is disable.

Port Point to Point: Pull down the menu of the corresponding port number to set up the Point to Point setting of each port. The default setting is “Forced True”.

4.5.3 RSTP Status

RSTP Status allows users to view a list of RSTP brief information such as Bridge ID, topology status and Root ID, a list of all RSTP ports’ information, and the real-time RSTP statistics of the Managed Switch. Please select the option **RSTP Status** from the **Rapid Spanning Tree** menu and then the following screen page appears.



Refresh: Click **Refresh** to update the latest RSTP status.

Bridge ID: Display RSTP Bridge ID of the Managed Switch

Max Age: Display Max Age setting of the Managed Switch.

Hello Time: Display Hello Time setting of the Managed Switch.

Fwd Delay: Display Forward Delay Time setting of the Managed Switch.

Topology: Display Managed Switch’s state of the topology.

Root ID: Display the Root ID of the Managed Switch.

Root port: Display the Root Port Number of the Managed Switch.

Port: The number of the port.

Path Cost: The Path Cost of each 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).

RSTP Tx: The total transmitted RSTP packets from each port.

RSTP Rx: The total received RSTP packets from each port.

STP Tx: The total transmitted STP packets from each port.

STP Rx: The total received STP packets from each port.

TCN Tx: The total transmitted TCN (Topology Change Notification) packets from each port.

TCN Rx: The total received TCN (Topology Change Notification) packets from each port.

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

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

4.6 Fast Redundancy

Besides RSTP and Ring Detection as we previously mentioned, the employment of CTS's proprietary 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.

CTS's 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

Click the folder **Fast Redundancy** from the **Main Menu** and then 2 options within this folder will be displayed as follows.

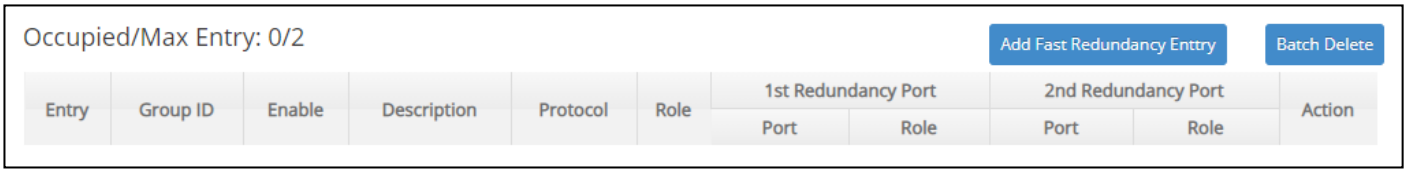
1. **Fast Redundancy Setup:** Configure Fast Ring v2 or Chain protocol to achieve network redundancy and maximum availability.

2. **Fast Redundancy Status:** Investigate a comprehensive table displaying the up-to-date Fast Redundancy status for the monitoring and analysis of your configured network redundancy.

4.6.1 Fast Redundancy Setup

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

Click **Add Fast Redundancy Entry** to add a new fast redundancy. Up to 2 sets of fast redundancy can be created.

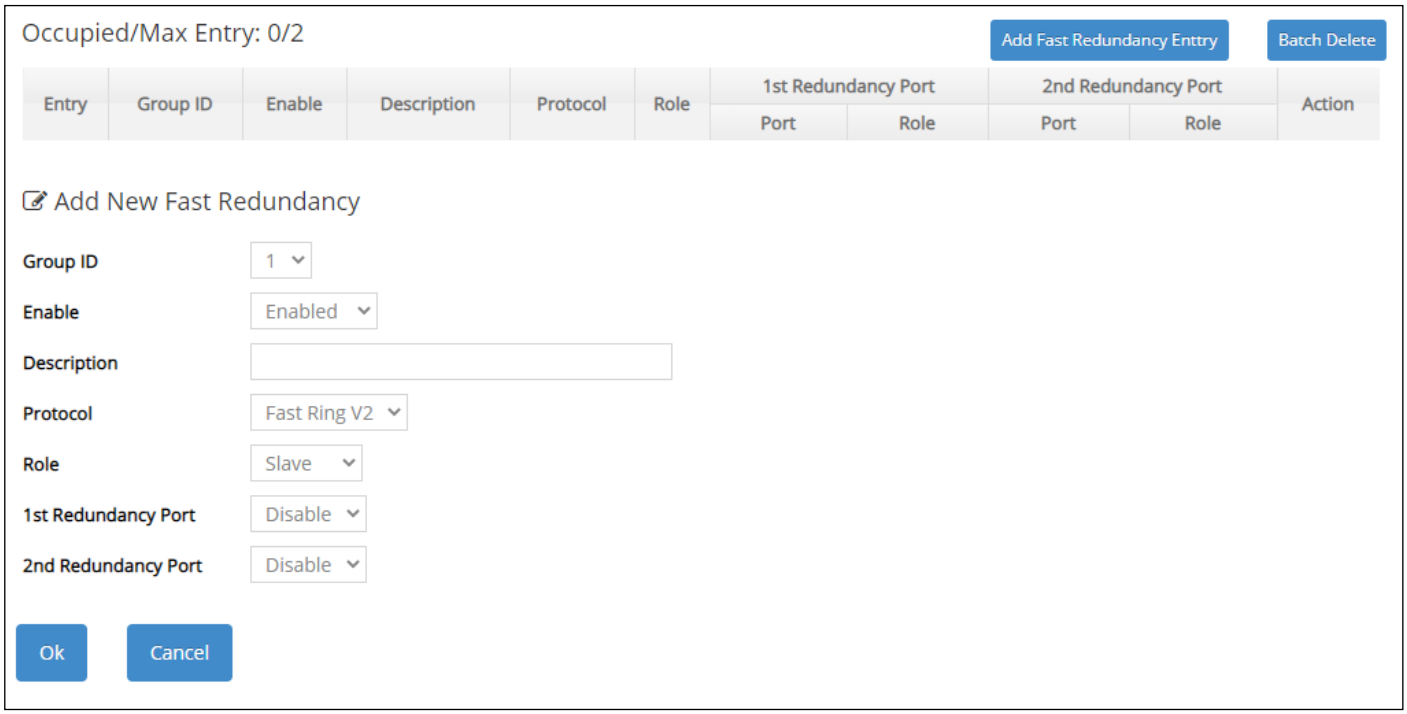


4.6.1.1 Fast Ring v2 Protocol

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.



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.

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

Enable: Enable or disable the ring you configure.

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.

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.

Click the icon to modify the settings of a specified fast redundancy.

Click the icon to remove a specified fast redundancy and its settings from the Fast Redundancy Setup table. Or click **Batch Delete** to remove a number of / all fast redundancy at a time by clicking on the checkbox belonging to the corresponding fast redundancy in the **Action** field and then click **Delete Select Item**, the fast redundancy will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

4.6.1.1.1 Configure a Ring Example using the Fast Ring v2 Protocol

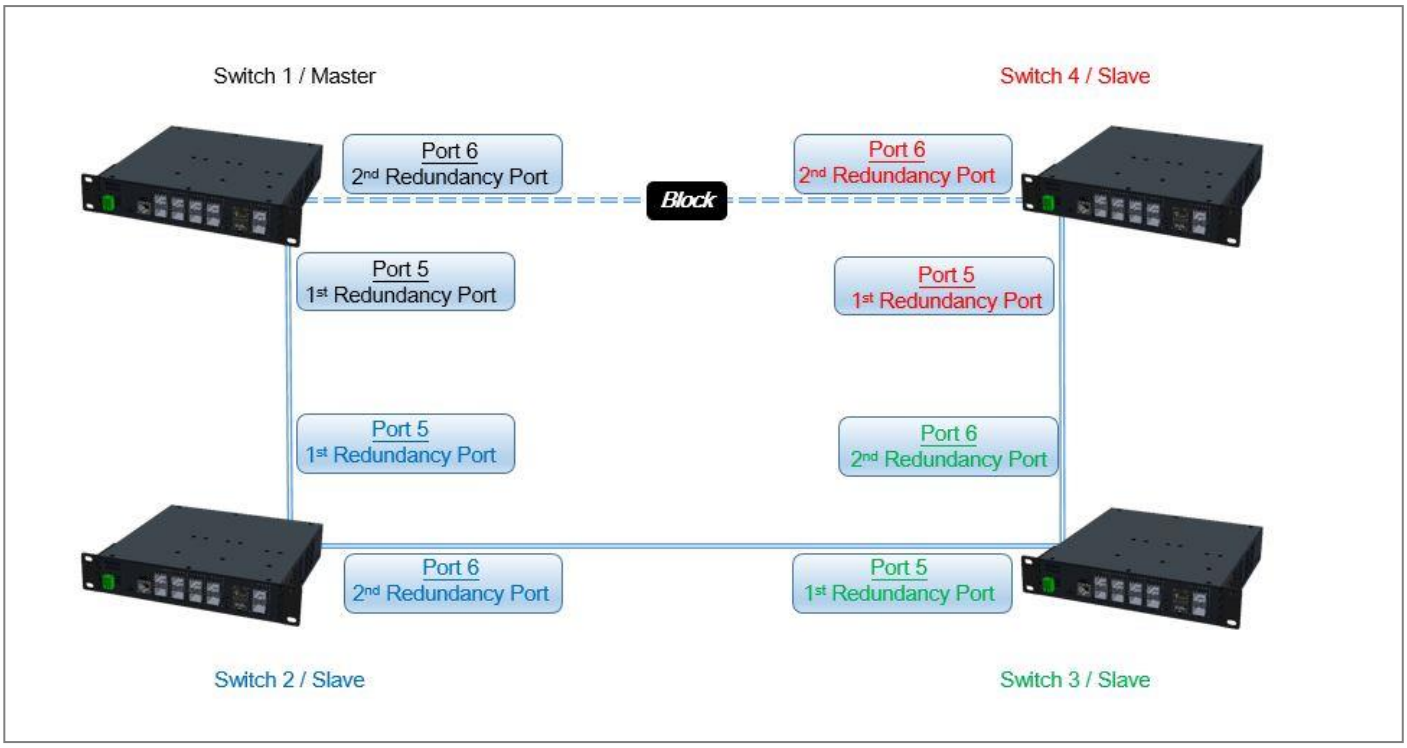


Fig. 4-1 Fast Ring v2 Example Diagram

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

Table 4-1 Fast Ring v2 Configuration

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.

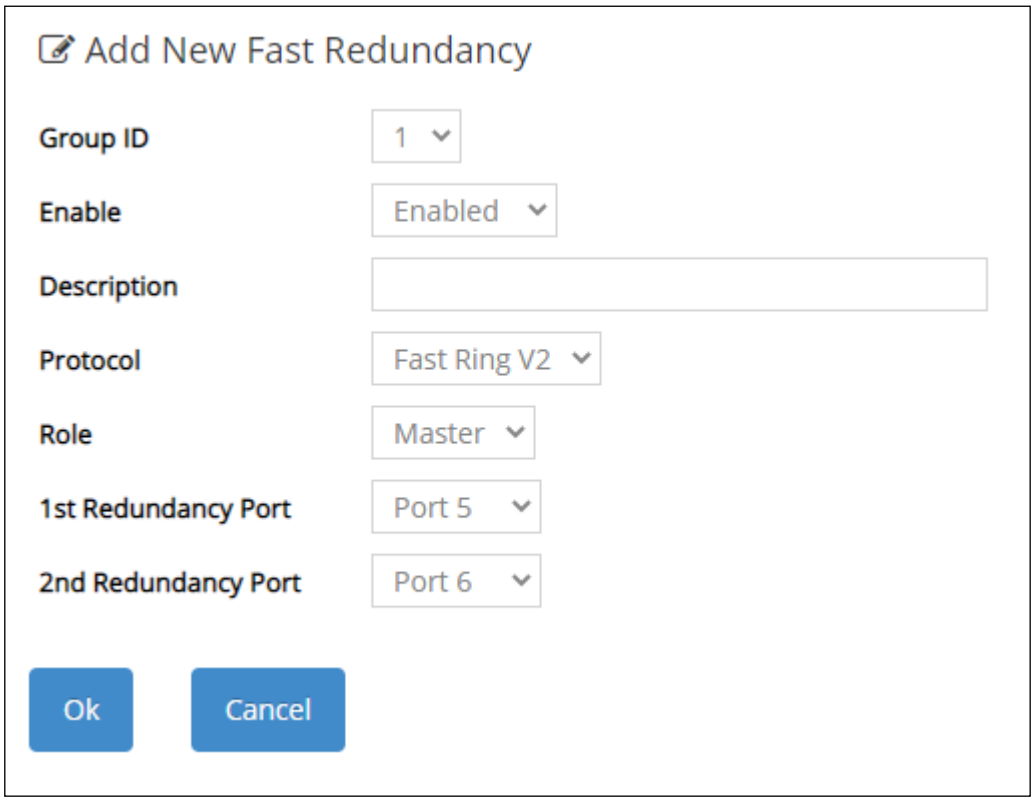
Just follow the procedures listed below for step-by-step instructions to configure a ring as Fig. 4-1 using the Fast Ring v2 protocol.

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 **Fast Redundancy Setup** from the **Fast Redundancy** menu for the Fast Ring v2 configuration. Click the **Add Fast Redundancy Entry** button to create a Fast Ring v2.

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



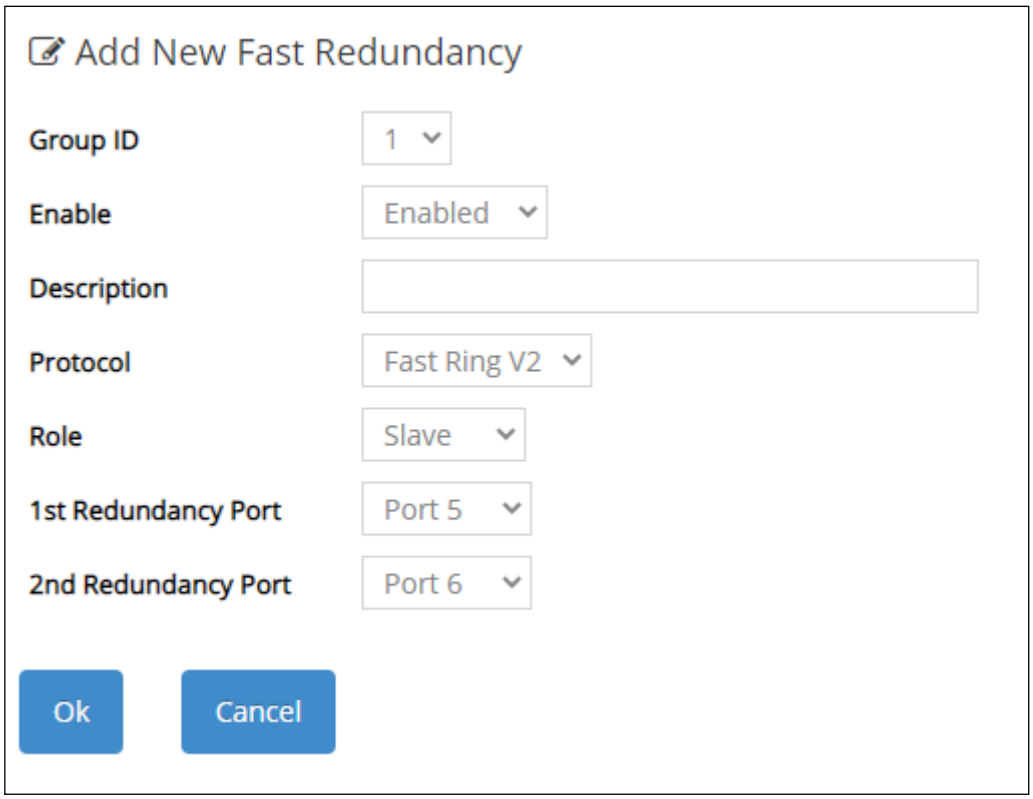
Step 2: Set up the Fast Ring v2 configuration on Switch 2, 3 & 4.

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 **Fast Redundancy > Fast Redundancy Setup** for the Fast Ring v2 configuration. Click the **Add Fast Redundancy Entry** button to create a Fast Ring v2.

2-3. Please refer to each column parameter below, set “Group ID” = 1, “Enable” = Enabled,

"Protocol" = Fast Ring v2, "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.



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.

4.6.1.2 Chain Protocol

CTS's Chain 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:

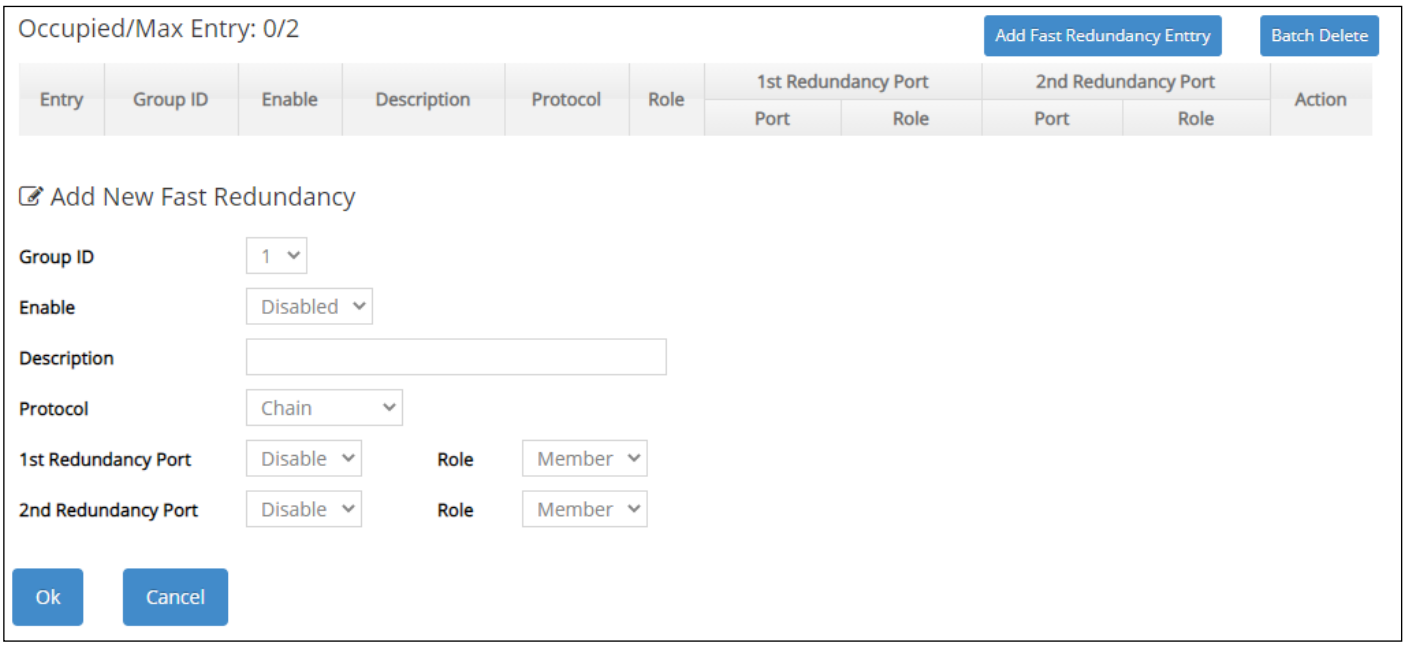
- A Head switch,
- A Tail switch,
- Member switches.

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, CTS's Chain 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.



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.

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

Enable: Enable or disable the chain you configure.

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.

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.

> **Head:** A role acts as the external port for the entire chain.
>
> **Tail:** A role acts as the blocked port for the entire chain.
>
> **Member:** A role acts as an intermediate-connection port between the head port and the tail port.

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.

Click the  icon to modify the settings of a specified fast redundancy.

Click the  icon to remove a specified fast redundancy and its settings from the Fast Redundancy Setup table. Or click **Batch Delete** to remove a number of / all fast redundancy at a time by clicking on the checkbox belonging to the corresponding fast redundancy in the **Action** field and then click **Delete Select Item**, the fast redundancy will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

4.6.1.2.1 Configure a Chain Example using the Chain Protocol

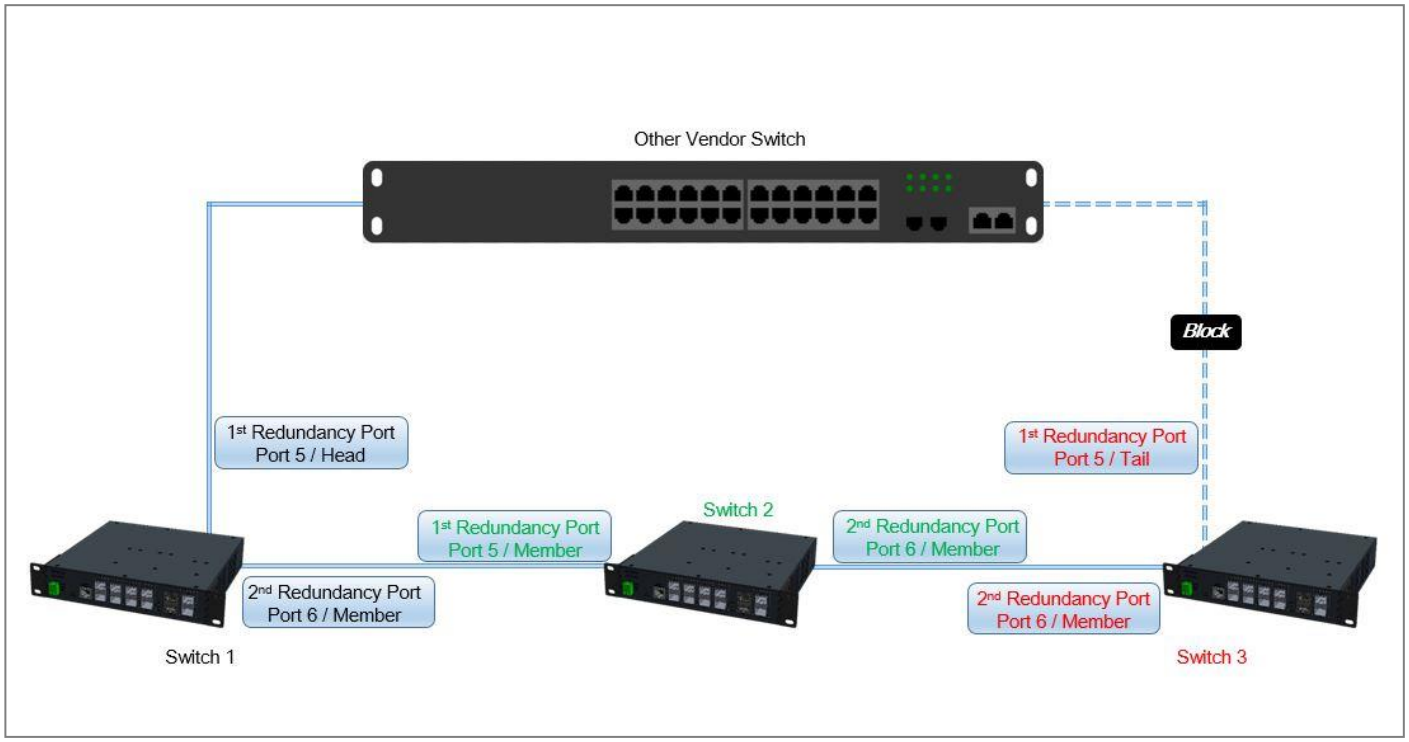


Fig. 4-2 Chain Example Diagram

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

Table 4-2 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.

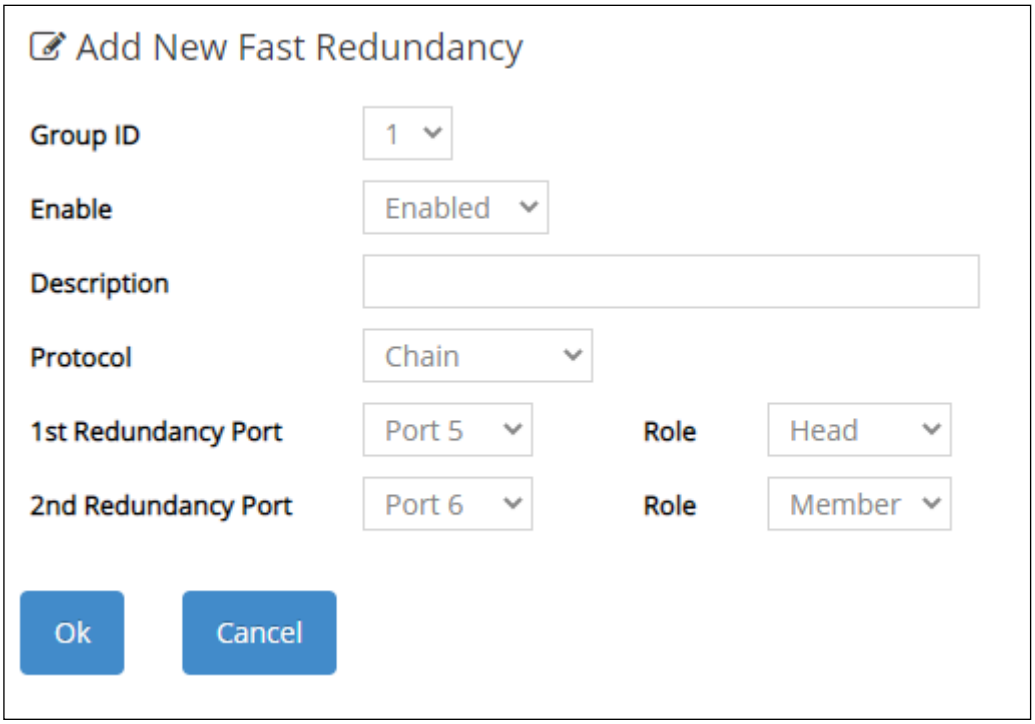
Just follow the procedures listed below for step-by-step instructions to configure a chain as Fig. 4-2 using the Chain protocol.

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 **Fast Redundancy > Fast Redundancy Setup** for the chain configuration. Click the **Add Fast Redundancy Entry** button to create a chain.

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

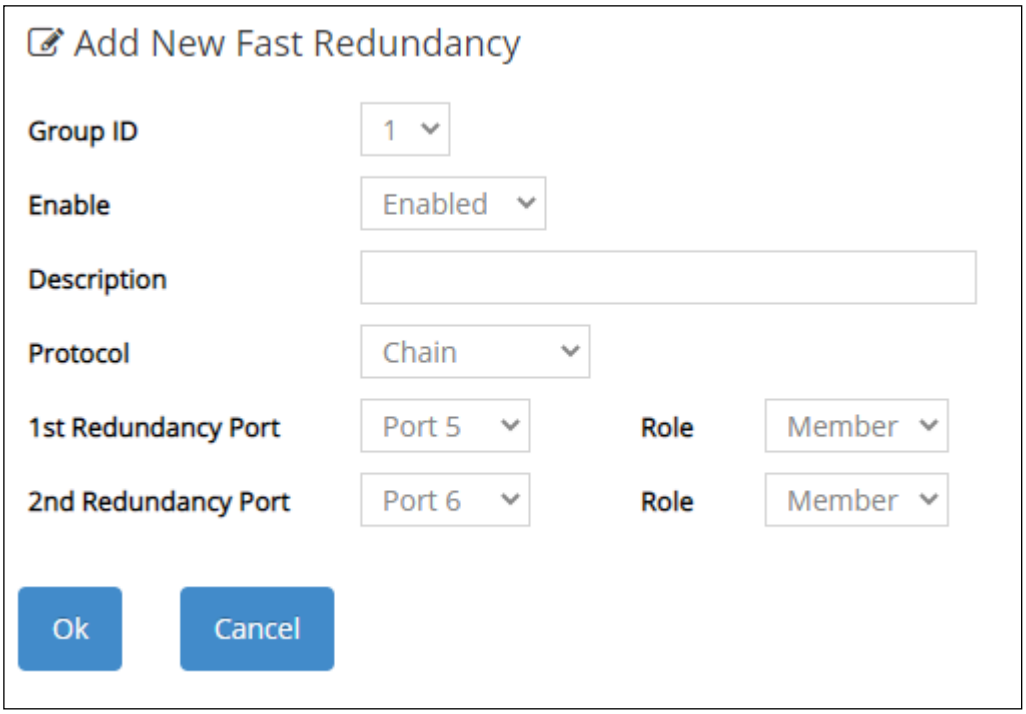


Step 2: Set up the Chain configuration on Switch 2.

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 **Fast Redundancy > Fast Redundancy Setup** for the chain configuration. Click the **Add Fast Redundancy Entry** button to create a chain.

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

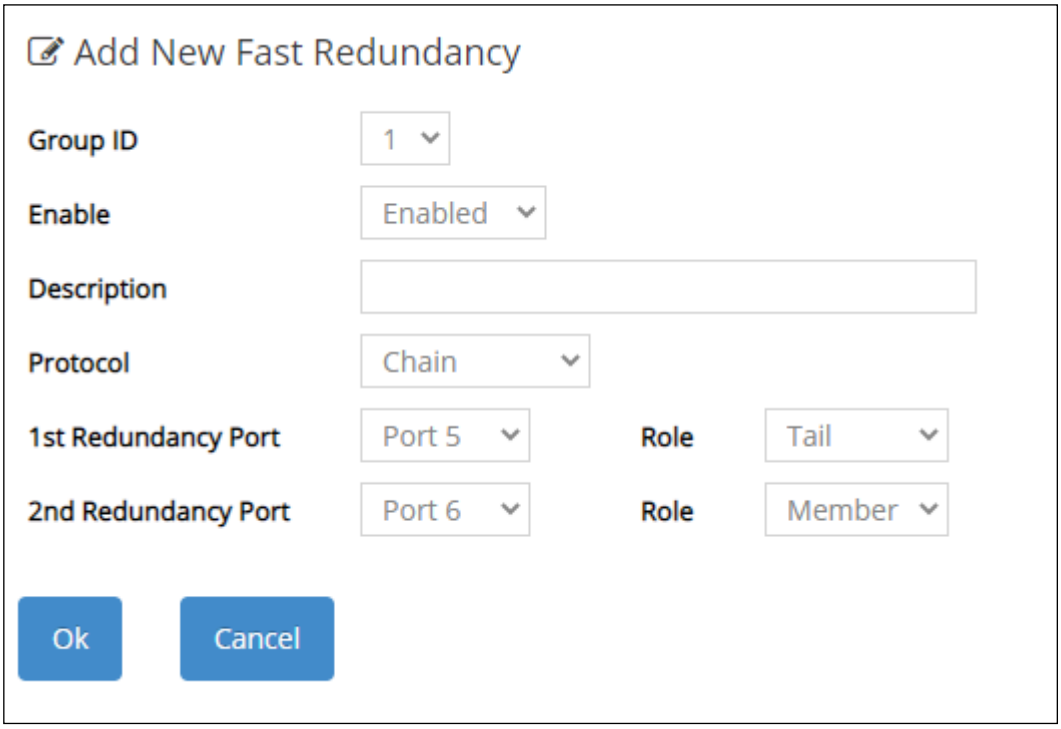


Step 3: Set up the Chain configuration on Switch 3.

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 **Fast Redundancy > Fast Redundancy Setup** for the chain configuration. Click the **Add Fast Redundancy Entry** button to create a chain.

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

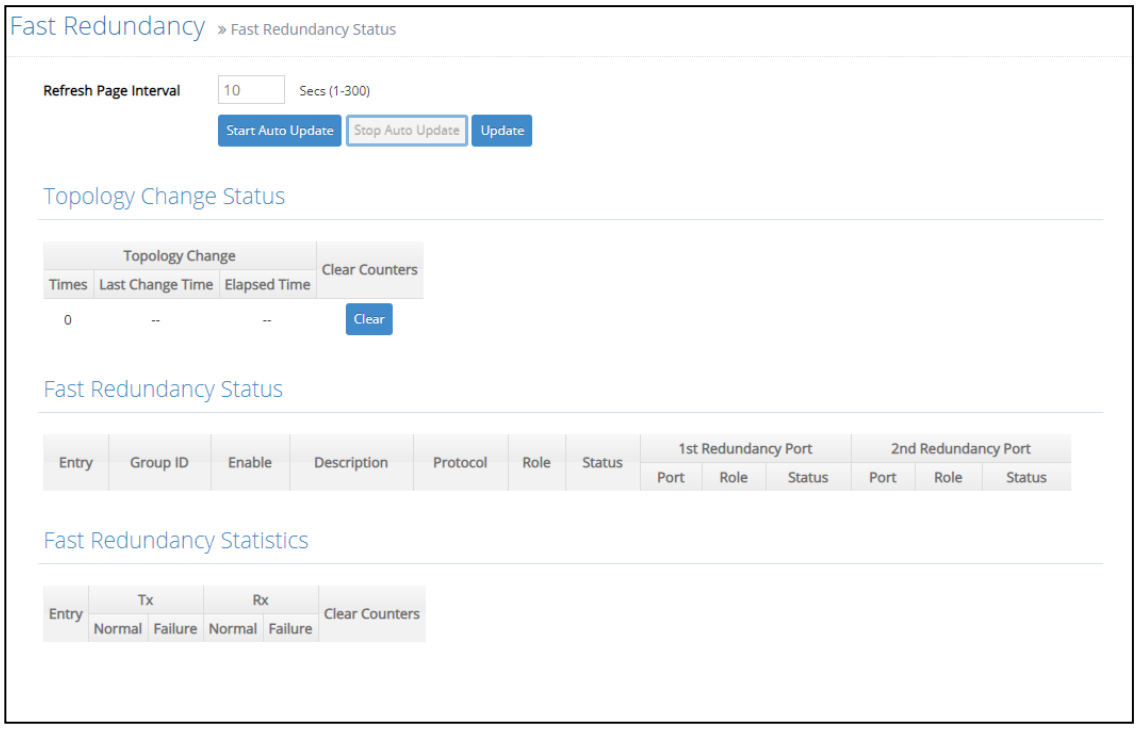


NOTE: *To avoid the occurrence of loop, please do not connect Switch 1, 2, & 3 together in the chain topology before the end of Chain configuration.*

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

4.6.2 Fast Redundancy Status

Fast Redundancy Status allows users to view a list of Fast Redundancy detailed information. This status page is mainly divided into three subdivisions: **Topology Change Status**, allowing users to keep abreast of the dynamic change of the topology wherein the switches operate; **Fast Redundancy Status**, delivering a comprehensive information in exact accordance with the saved-configuration; and **Fast Redundancy Statistics**, offering a real-time Fast Redundancy statistics for efficient troubleshooting and easy monitoring. Please select the option **Fast Redundancy Status** from the **Fast Redundancy** menu and then the following screen page appears.



Refresh Page Interval: Automatically updates statistics of the Fast Redundancy Status page encompassing three main subdivisions 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 to the next system boot-up. Click **Start/Stop Auto Update** to activate auto-update; click **Update** to manually refresh the event log table once.

Topology Change Status: Includes the following information.

1. **Times:** The total number of times the topology has changed.
2. **Last Change time:** The explicit time when the nearest topology change occurs.
3. **Elapsed Time:** Displays how much time has elapsed since the last change of the topology.
4. **Clear**: This allows users to reset the recorded information.

Fast Redundancy Status: Includes the following information.

1. **Entry:** A designated number as either 1 or 2, which is given according to the sequence of added Fast Redundancy. The maximum number is 2.
2. **Group ID:** The group ID of the fast redundancy.

3. **Description:** The description of the group.

4. **Enable:** The availability of the fast redundancy.

5. **Protocol:** The fast redundancy specified as either “Fast Ring v2” or “Chain.”

6. **Role:** The role assigned to the Managed Switch as either Slave or Master when Fast Ring v2 protocol is chosen. It will show “--" when the Chain protocol is chosen.

   Master: A role possesses the ability of blocking or forwarding packets.

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

7. **Status:** Signifies the connection status of the fast redundancy you configured, and includes **Healthy**, **Break** and **Signal Fail** 3 types of state. Each state is described as below.

   Healthy: Indicates that the connection of the fast redundancy is in normal status.

   Break: Indicates that the failure of fast redundancy connection occurs on other switch and its backup link is activated to transmit the data.

   Signal Fail: Indicates that the failure of fast redundancy connection occurs on the switch itself and its backup link is activated to transmit the data.

8. **1st/2nd Redundancy Port:** The port of the Managed Switch acts as the first/second interface of the Fast Redundantcy.

9. **Role of 1st/2nd Redundancy Port:** 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.

   Head: A role acts as the external port for the entire chain.

   Member: A role acts as an intermediate-connection port between the head port and the tail port.

   Tail: A role acts as the blocked port for the entire chain.

10. **Status of 1st/2nd Redundancy Port:** Shows the connection status of the port that acts as the first/secondary redundant port. Includes **Forwarding**, **Blocked** and **Link down** 3 types of port state. Each state is described as below.

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

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

    Link down: Indicates that no port connection eixsts.

Fast Redundancy Statistics: Includes the following information.

1. **Entry:** A designated number as either 1 or 2, which given according to the sequence of the created Fast Redundancy. The maximum number is 2.

2. **TX/RX Source Normal:** The amount of packets successfully transmitted/received.
3. **TX/RX Source Failure:** The amount of packet loss in transmitting/receiving.
4. **Clear**: This allows users to reset the recorded information.

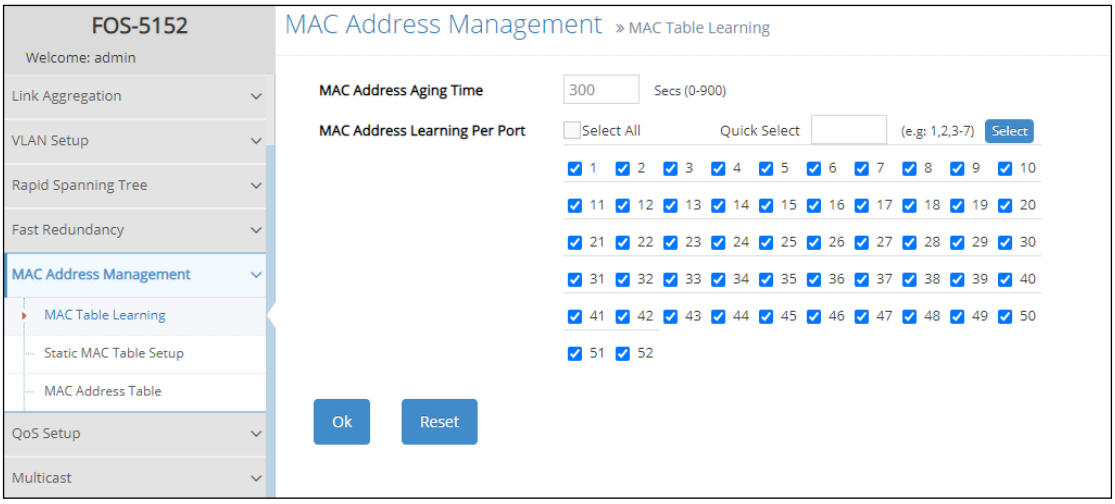
4.7 MAC Address Management

Select the folder **MAC Address Management** from the **Main Menu** and then 3 options will be displayed for your selection.

1. **MAC Table Learning:** Set up MAC address table aging time, and enable/disable MAC address learning function.

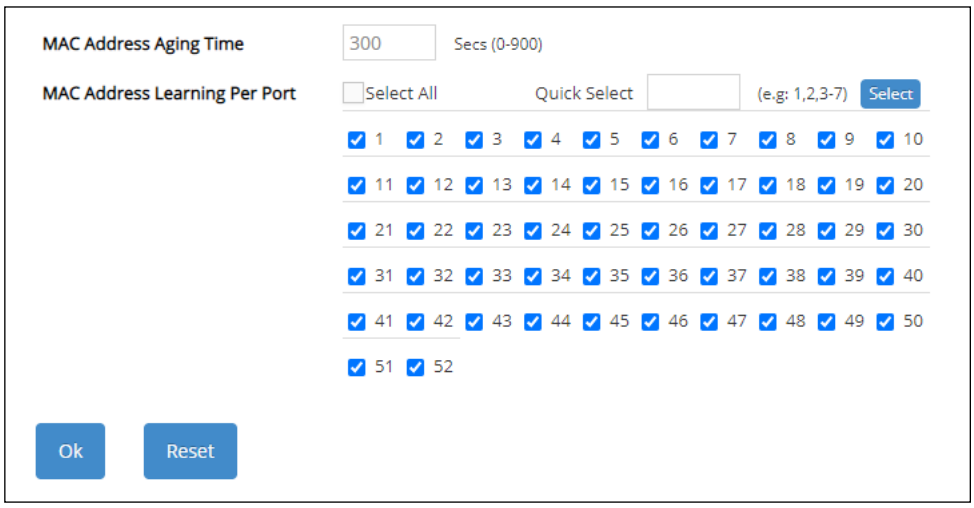
2. **Static MAC Table Setup:** To create, edit or delete the Static MAC Table setting.

3. **MAC Address Table:** List the current MAC addresses automatically learned by the Managed Switch and the created static MAC addresses.



4.7.1 MAC Table Learning

Click the option **MAC Table Learning** from the **MAC Address Management** menu and then the following screen page appears.



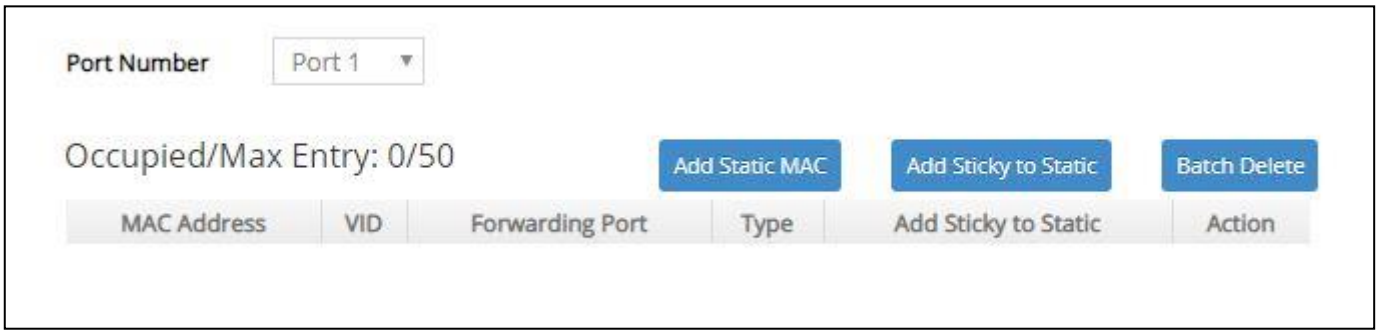
MAC Address Aging Time: Specify MAC address table aging time between 0 and 900 seconds. “0” means that MAC addresses will never age out.

MAC Address Learning Per Port: Enable port MAC address learning function on the specified ports by clicking on the checkbox of the corresponding port number. Or directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field and then press the **Select** button, the specified

port(s) will be checked immediately. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

4.7.2 Static MAC Table Setup

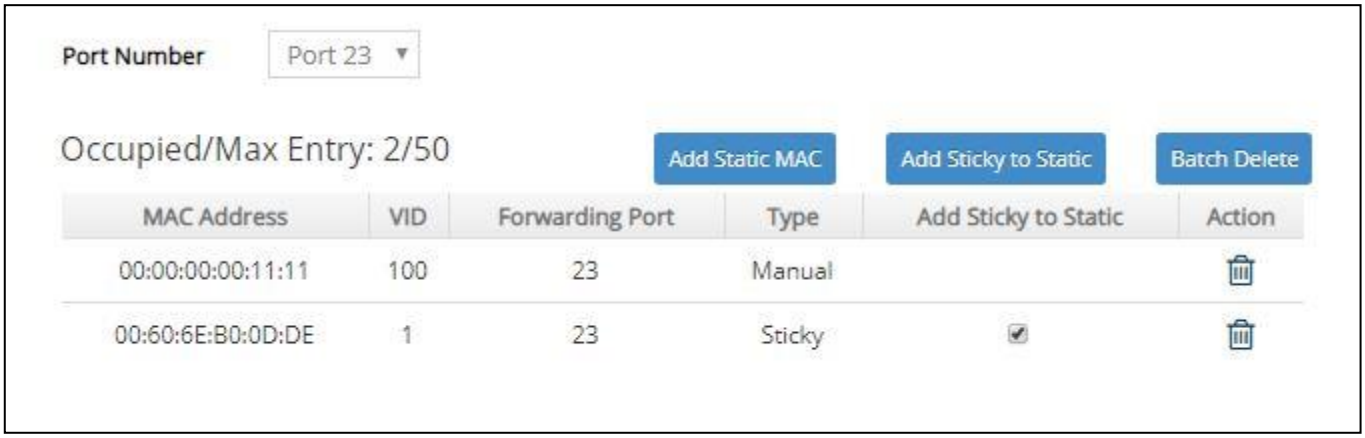
Click the option **Static MAC Table Setup** from the **MAC Address Management** menu and then the following screen page appears.



This table will display the overview of each port's static source MAC addresses typed as "Manual", which are manually added by clicking on the **Add Static MAC** button. Besides, it also lists the static ones typed as "Sticky", which are automatically learned by the selected port if this port's functions of Mac Limit and Sticky MAC address are simultaneously enabled. The transmission behavior of the packets carrying these two different types of static MAC address is in the same way on the switch.

The auto-learned "Sticky" MAC addresses denotes that they still do not write into the running configuration file, whereas the manual-added "Manual" MAC addresses denotes that they have been written into the running configuration file. Thus, if the **Save Configuration** function is executed before rebooting the Managed Switch, the MAC addresses with the type of "Sticky" will disappear and the MAC addresses with the type of "Manual" still exist on the static MAC table.

To transfer the MAC address type from "Sticky" into "Manual", please click on the checkbox belonging to the specific sticky MAC address in the **Add Sticky to Static** field (see the figure below), and then press the **Add Sticky to Static** button. The type of the sticky MAC addresses will be changed as "Manual" immediately.



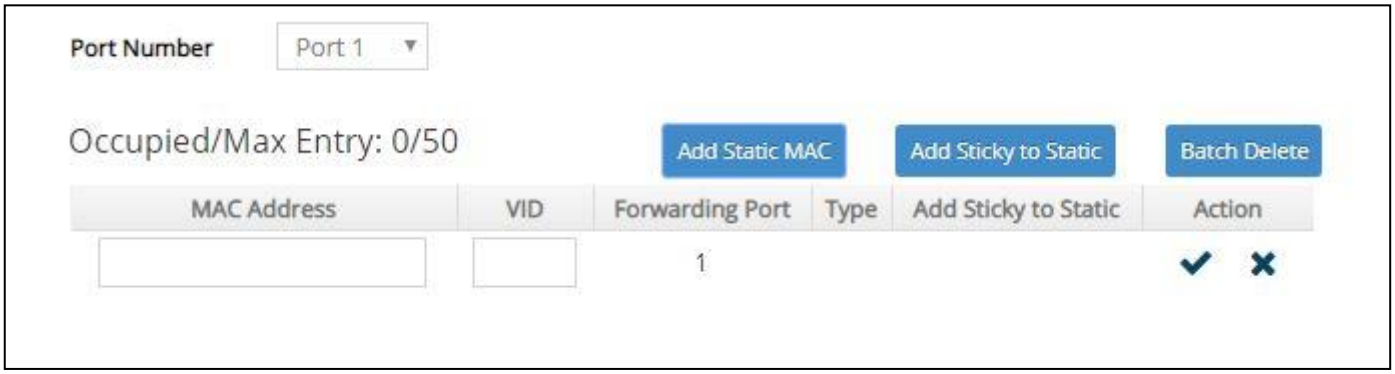
NOTE: *The Managed Switch only supports port-based MAC security and does not support switch-based MAC security. The Managed Switch can support up to 50 entries of MAC security list per port.*

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total static MAC address that have already been created of the specific port. Different ports may have different values.

Max: This shows the maximum number available for static MAC address of each port. The maximum number is 50.

Click **Add Static MAC** to add a new MAC address entry and then the following screen page appears for the further static MAC address settings.



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

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

Forwarding Port: View-only field. 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.

NOTE: *If any port (e.g. Port 27) in which the Mac Limit function is enabled whose current counts of MAC addresses has already reached the threshold, an error message of "Total secure MAX addresses on interface 27 has reached maximum limit" will be pop up while you would like to add a new static MAC address.*

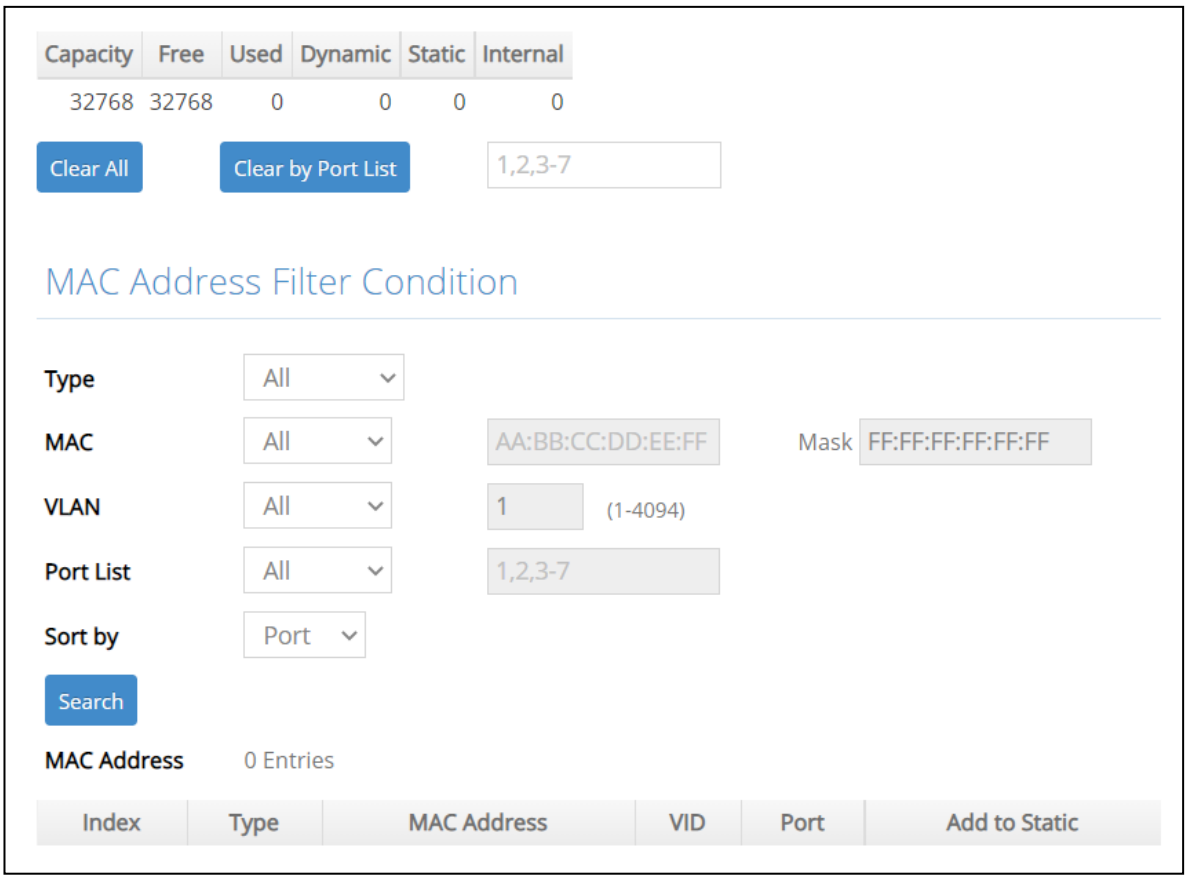
Click ✔ when the settings are completed, this new static MAC address will be listed on the static MAC address table, or click ✖ to cancel the settings.

Click the icon to modify the settings of a specified static MAC address.

Click the icon to remove a specified static MAC address entry and its settings from the static MAC address table. Or click **Batch Delete** to remove a number of /all static MAC addresses at a time by clicking on the checkbox belonging to the corresponding static MAC address in the **Action** field and then click **Delete Select Item**, the selected static MAC address/addresses will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

4.7.3 MAC Address Table

MAC Address Table displays the learned MAC addresses when MAC Address Learning is enabled. Select the option **MAC Address Table** from the **MAC Address Management** menu and then the following screen page appears.



The table that sits at the very top of the webpage displays an up-to-date summary of the MAC address table down below.

1. **Capacity:** The maximum number of the MAC address entries allowed to be kept on the Managed Switch.

2. **Free:** The available number of the MAC address entries still allowed to be kept on the Managed Switch.

3. **Used:** The number of the MAC address entries already kept on the Managed Switch.

4. **Dynamic:** The number of the dynamic MAC addresses entries already kept on the Managed Switch.

5. **Static:** The number of the static MAC addresses entries already kept on the Managed Switch.

6. **Internal:** The MAC address of the Managed Switch.

The table that sits at the very bottom of the page is composed of the MAC addresses that are automatically learned from each port of Managed Switch or manually created by the users. Click **Clear All** to clear all dynamic MAC addresses in the MAC address table. Or click **Clear by Port List** to clear the dynamic MAC addresses for the specified port(s).

MAC Address Filter Condition section delivers a flexible approach to investigating the MAC address table in accordance with the specified filter options, which are respectively described below to guide you through the filter setup. When you have done determining the filtering behavior, click **Search** to update the MAC address table.

1. **Type:** Select **All**, **Dynamic**, or **Static**, to specify which MAC address type to be displayed in the table.

2. **MAC:** Select **All**, **Include**, or **Exclude** to determine the filtering behavior for the MAC address comparison. It indicates how many bits, from left to right, the filter checks against the MAC address. To require an exact comparison to the full MAC address (to check all 48 bits), enter FF:FF:FF:FF:FF:FF; to check only the first 32 bits, enter FF:FF:FF:FF:00:00.

   AA:BB:CC:DD:EE:FF: Specify a MAC address to allow the filter to compare it against the specified MAC address mask.

   Mask: Specify a MAC address mask to allow the filter to compare it against the specified MAC address.

3. **VLAN:** Select **All**, **Include**, or **Exclude** to determine the filtering behavior, and specify the VLAN ID to be filtered with.

4. **Port List:** Select **All, Include**, or **Exclude** to determine the filtering behavior, and specify the port to be filtered with.

5. **Sort by:** Select **Port**, **MAC**, or **VLAN** to determine the arrangement of the MAC address entries displayed in the table. Each option is described below:

   Port: MAC addresses that are learned from the same port will be grouped together and displayed in ascending order.

   MAC: MAC addresses will be displayed in ascending order according to their digit sizes.

   VLAN: MAC addresses that belong to the same VLAN ID will be grouped together and displayed in ascending order.

To transfer the MAC address type from “dynamic” into "static", please click on the checkbox belonging to the specific dynamic MAC address in the **Add to Static** field, and then press the **Add to Static** button located at the top-right corner of the table. The specified dynamic MAC address will be turned into a static one when clicking **Search** to refresh the MAC address table.

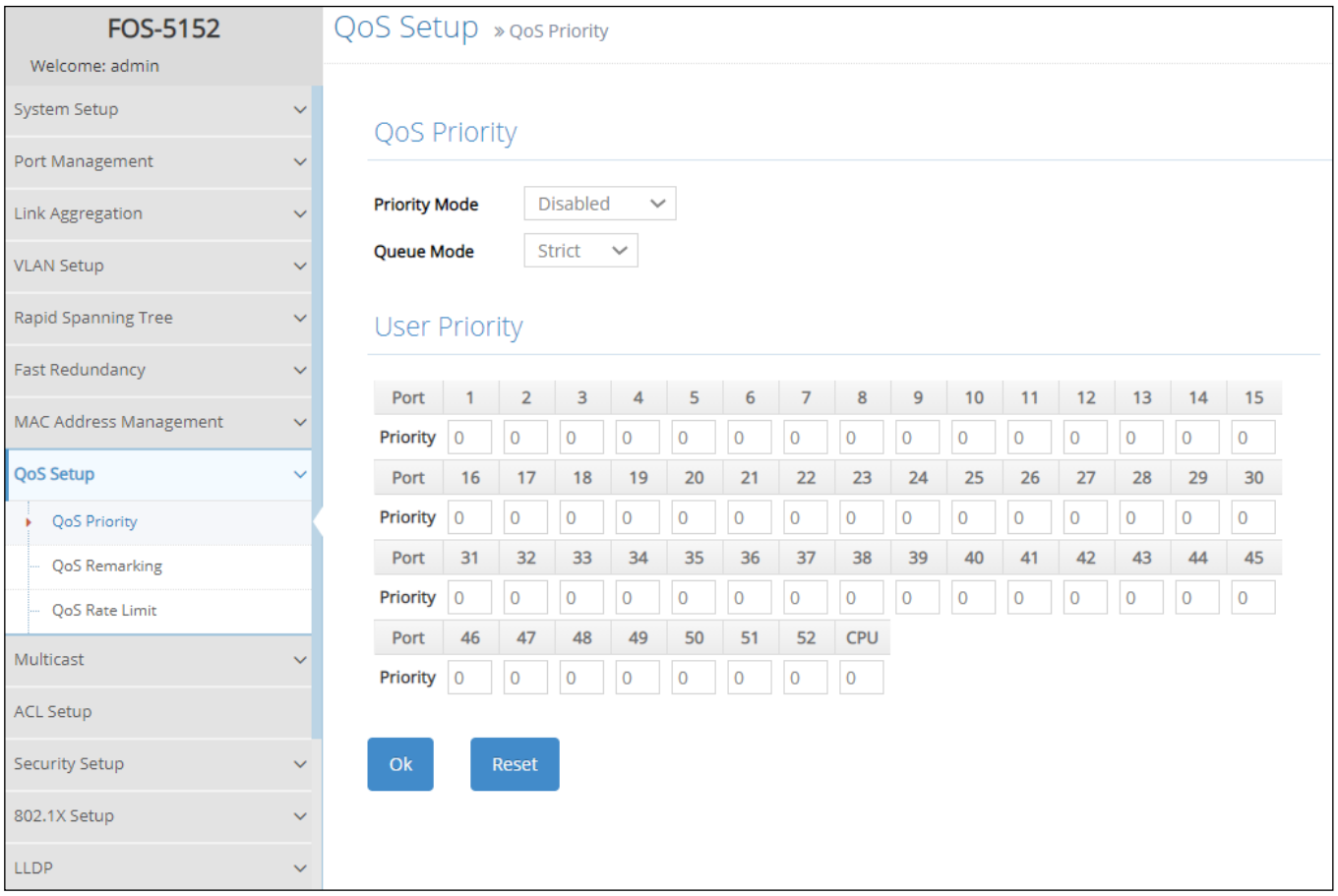
MAC Address: The total number of the MAC address entries displayed in the MAC address table according to the specified filtering options.

To view the MAC addresses that are searched, you may pull down the page list to directly go to the desired page. Or click **>**, **<**, **>>**, **<<** to move to the next/previous/last/first page of MAC address table.

4.8 QoS Setup

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. This ensures that network traffic is prioritized according to specified criteria and receives preferential treatments.

QoS enables you 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. To set up the priority of packets in the Managed Switch, click the folder **QoS Setup** from the **Main Menu** and then 3 options will be displayed for your selection.



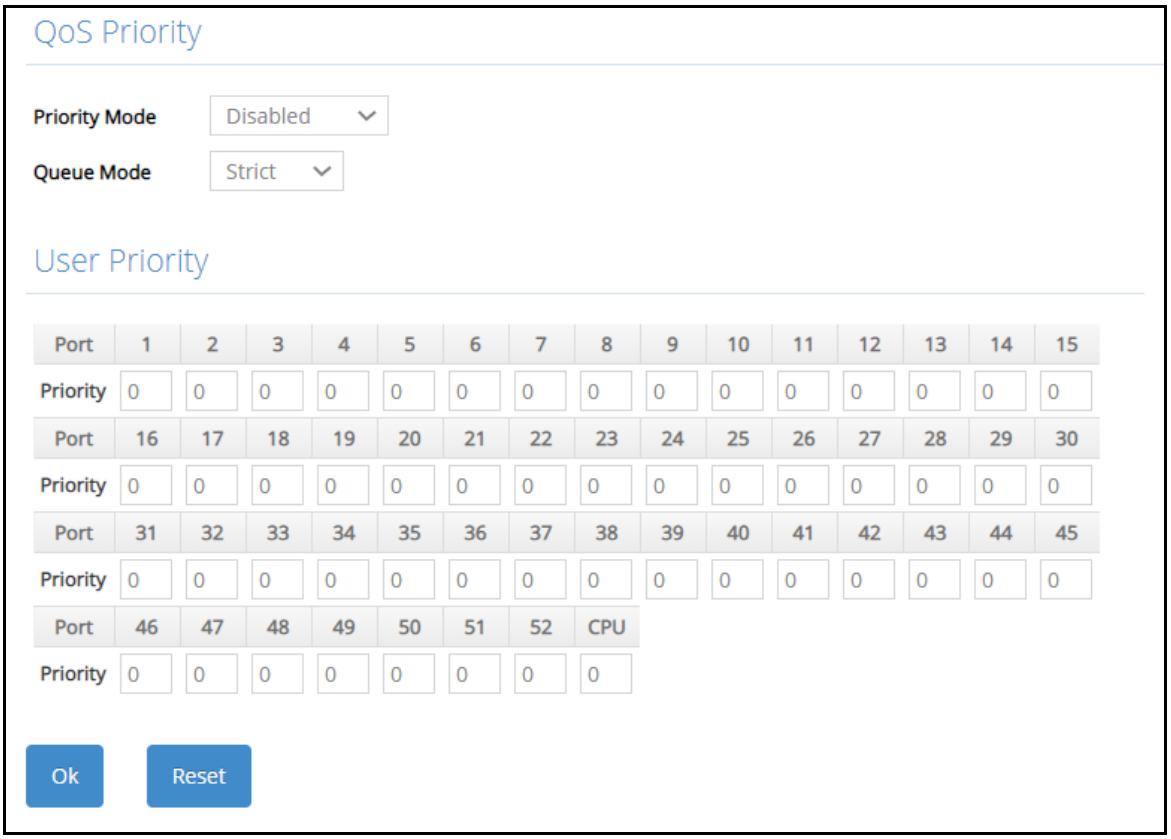
1. **QoS Priority:** To set up each port's QoS default class, Priority, Queuing Mode, Queue Weighted, and so on.

2. **QoS Remarking:** To set up QoS 802.1p Remarking and DSCP Remarking.

3. **QoS Rate Limit:** To configure each port's Ingress and Egress Rate.

4.8.1 QoS Priority

Select the option **QoS Priority** from the **QoS Setup** menu and then the following screen page appears.



Priority Mode: Select the QoS priority mode of the Managed Switch.

IEEE 802.1p: IEEE 802.1p mode utilizes p-bits in VLAN tag for differential service.

DSCP: DSCP mode utilizes TOS field in IPv4 header for differential service.

Disabled: Disable QoS.

Queue Mode: Specify the queue mode as Strict or Weight.

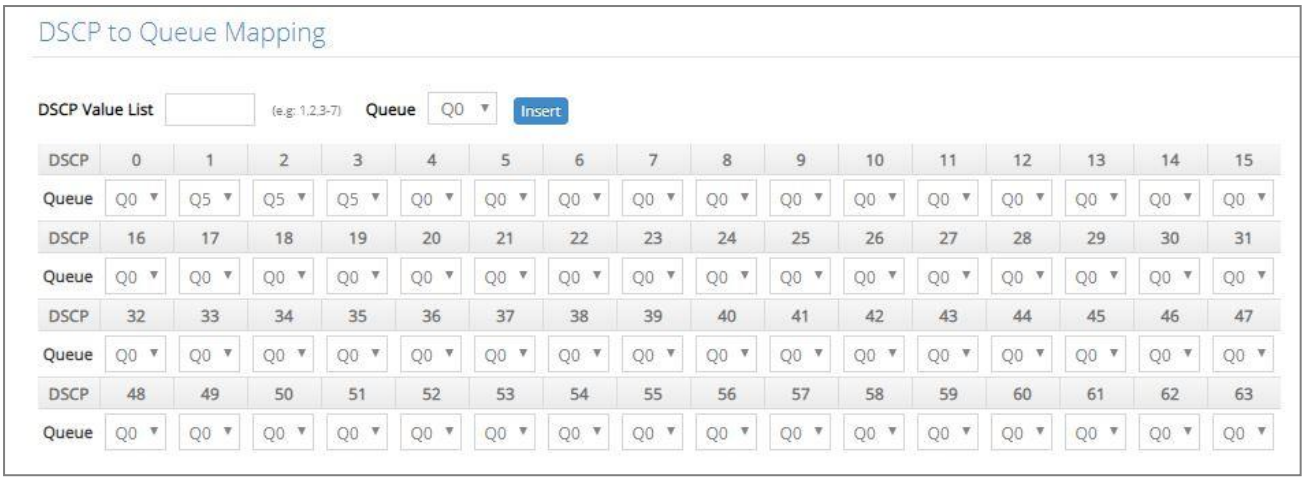
Strict: This indicates that services to the egress queues are offered in the sequential order and all traffic with higher priority queues is transmitted first before lower priority queues are serviced.

Weight: Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 8, 16, 32, 64, 127 for queues 1 through 8 respectively. The following parameter will appear when Queue Mode is selected as “Weight”.

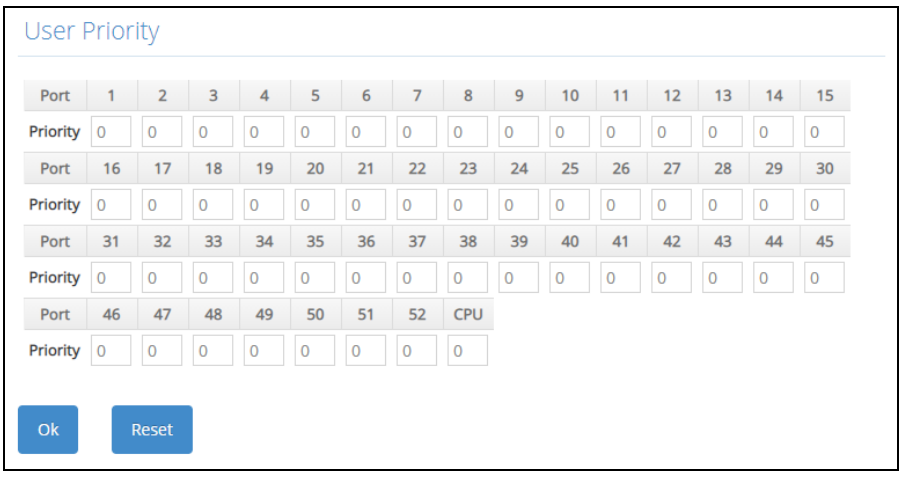
Queue Weight: Specify the Queue weight for each Queue. Valid value ranges from 1 to 127.

802.1p to Queue Mapping: Assign an 802.1p value (0~7) of 8 different levels to the specific queue.

DSCP to Queue Mapping: Assign a DSCP value (0~63) of 64 different levels to the specific queue by pulling down the **Queue** menu. Or directly input a range of the DSCP value (e.g.1, 2, 3-7) in the **DSCP Value List** field and specify them to the preferred queue from the **Queue** pull-down menu at a time. Then, press the **Insert** button, the specified DSCP value(s) will be assigned to this queue immediately.



User Priority:



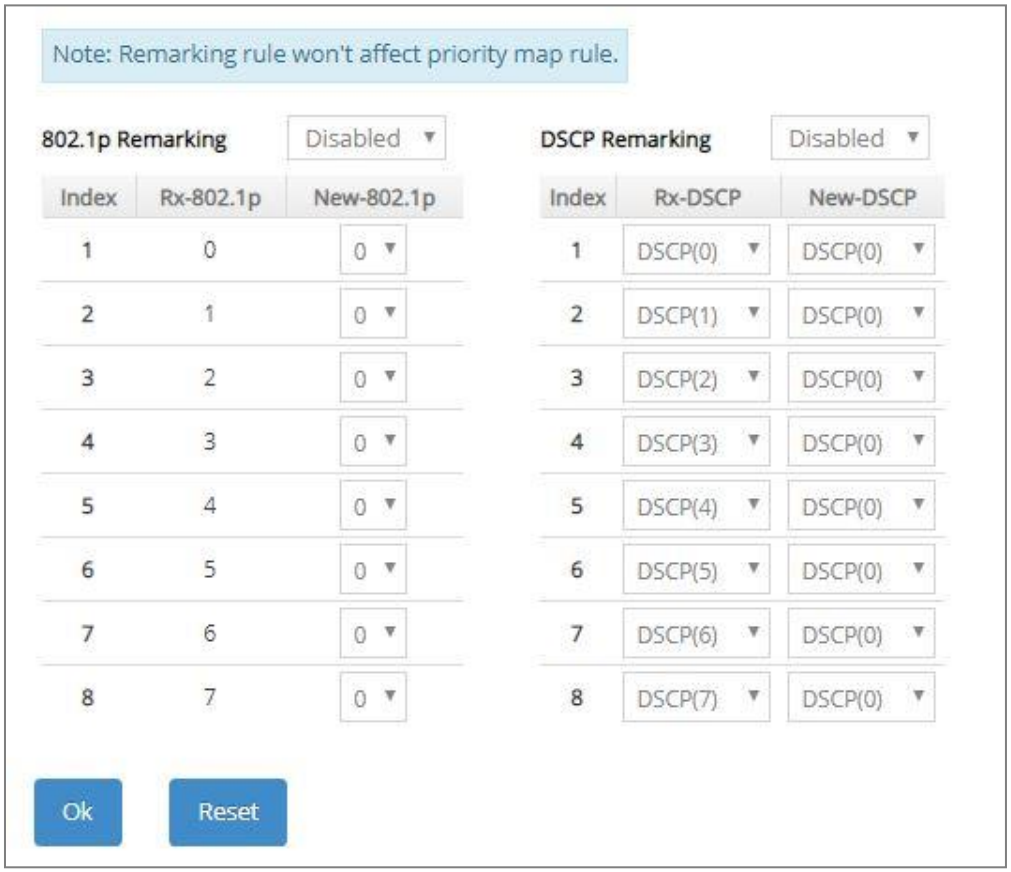
There are eight priority levels that you can choose to classify data packets. Specify one of the listed options for CoS (Class of Service) priority tag values. The default value is “0”.

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

Priority Level	normal	low	low	normal	medium	Medium	High	high
802.1p Value	0	1	2	3	4	5	6	7

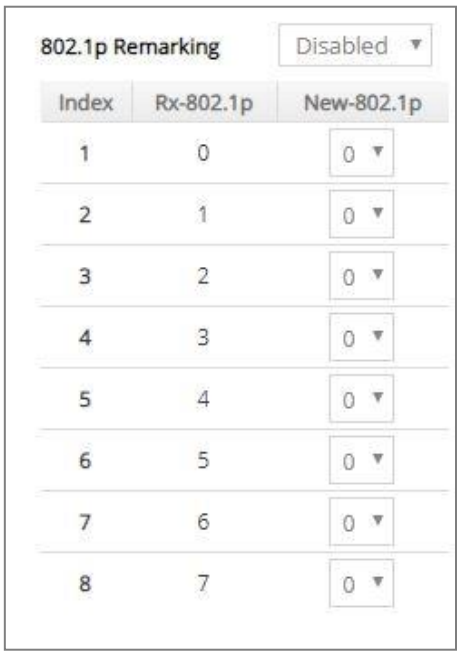
4.8.2 QoS Remarking

QoS Remarking includes 802.1p Remarking and DSCP Remarking. To configure it, select the option **QoS Remarking** from the **QoS Setup** menu and then the following screen page appears. Please note that 802.1p / DSCP remarking rule will not affect the priority mapping rule.



Configure 802.1p Remarking:

This allows you to enable or disable 802.1p remarking for each priority by pulling down the **802.1p Remarking** menu. The default setting is disabled.

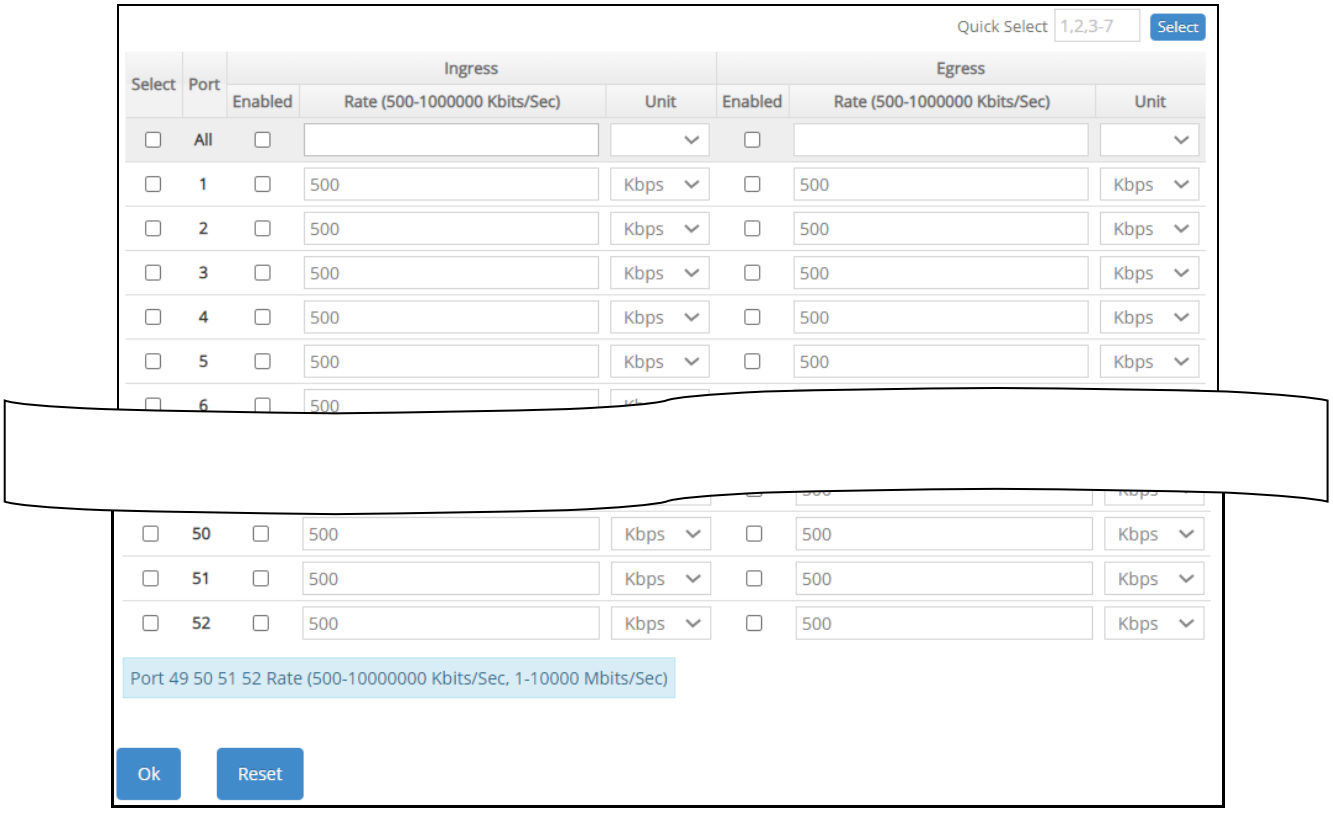


Configure DSCP Remarking:

This allows you to enable or disable DSCP remarking for each priority by pulling down the **DSCP Remarking** menu. The default setting is disabled.

4.8.3 QoS Rate Limit

Select the option **QoS Rate Limit** from the **QoS Setup** menu and then the following screen page appears. This allows users to specify each port's both inbound and outbound bandwidth. The excess traffic will be dropped.



Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the QoS Rate Limit table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Port: The number of each port.

Enabled in Ingress/Egress field**:** Enable or disable each port's QoS Rate Limit of inbound and outbound bandwidth. To enable it, just click on the checkbox of the corresponding port(s). The default setting is "unchecked", which is disabled.

Rate in Ingress/Egress field**:** Specify the transmitting rate limit of the inbound and outbound bandwidth. Valid range is from 500 ~1000000 in unit of Kbps or 1~1000 in unit of Mbps.

Unit in Ingress/Egress field**:** Either Kbps or Mbps can be selectd as the unit of the inbound and outbound bandwidth.

4.9 Multicast Configuration

Select the folder **Multicast** from the **Main Menu**, **IGMP/MLD Snooping** subfolder, **Static Multicast Setup** option and **MVR** subfolder for multicast setup will then be displayed.

4.9.1 IGMP/MLD Snooping

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

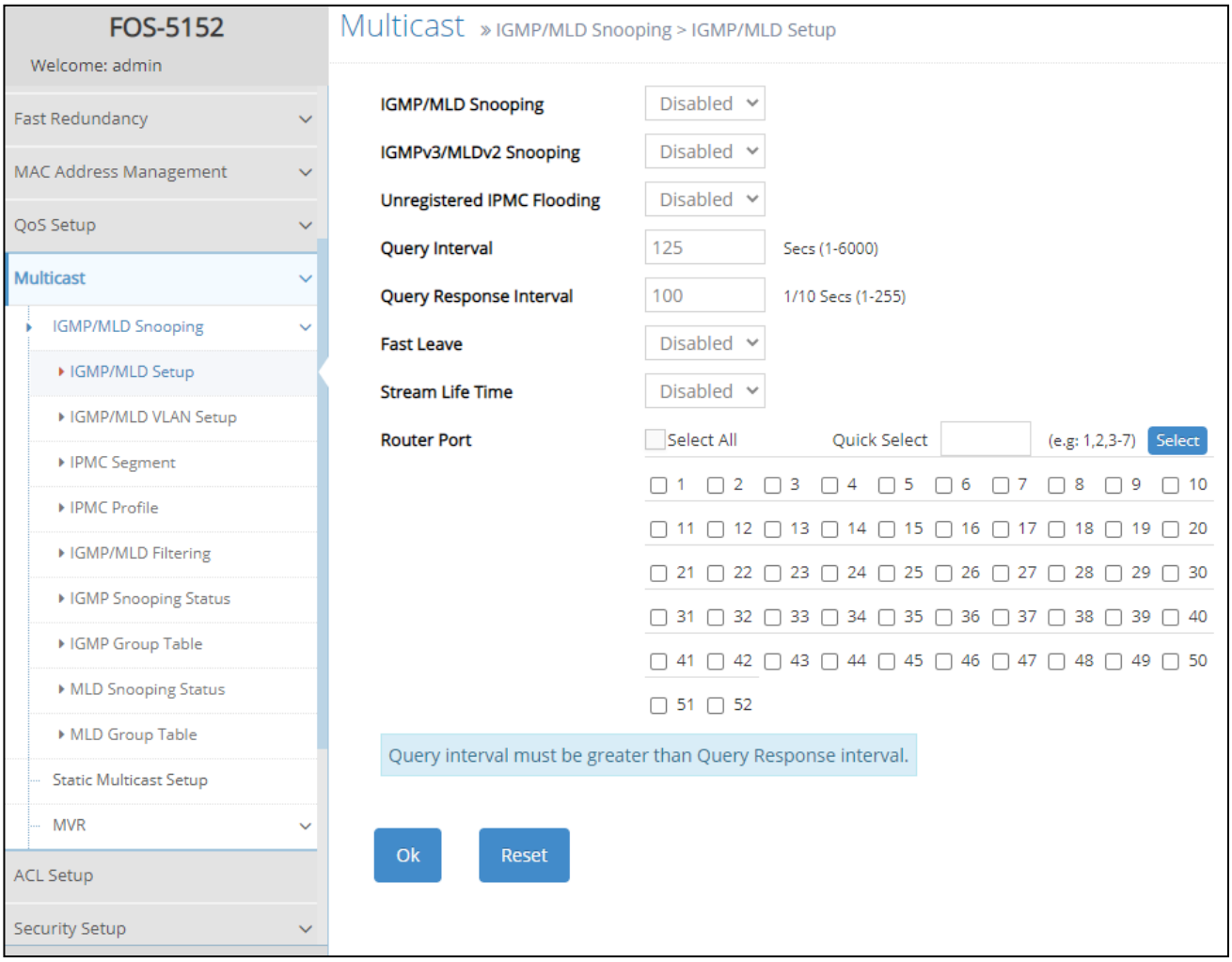
IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers by processing the layer 3 packets that IGMP packets sent in a multicast network.

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

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

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

Select the subfolder **IGMP/MLD Snooping** and then 11 options will be displayed for your selection.



1. **IGMP/MLD Setup:** To enable or disable IGMP/MLD Snooping, IGMPv3/MLDv2 Snooping, Unregistered IPMC Flooding and set up router ports.

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

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

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

5. **IGMP/MLD Filtering:** To enable or disable IGMP/MLD filter, and configure each port's IGMP/MLD filter.

6. **IGMP Snooping Status:** View the IGMP snooping status.

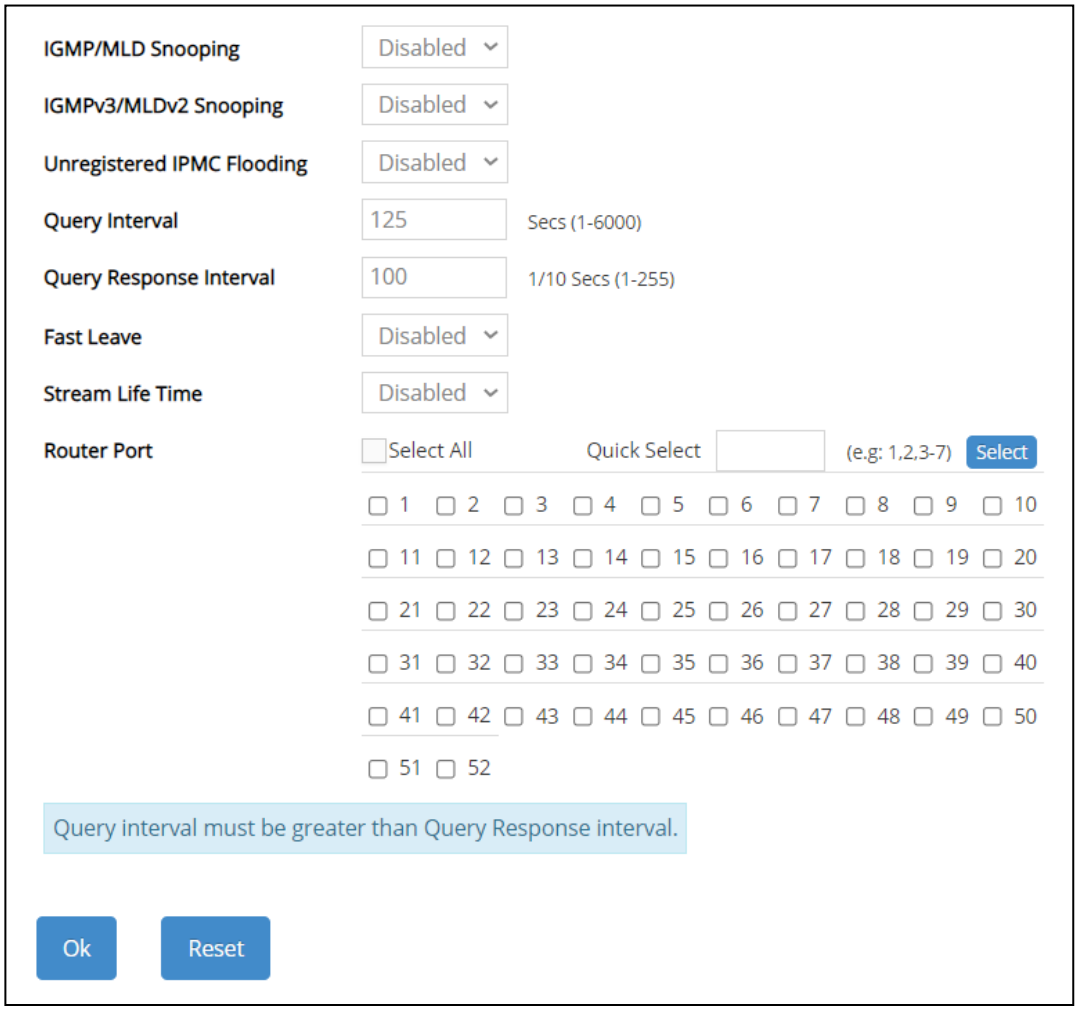
7. **IGMP Group Table:** View the IGMP Groups table.

8. **MLD Snooping Status:** View the MLD snooping status.

9. **MLD Group Table:** View the MLD Groups table.

4.9.1.1 IGMP/MLD Setup

Select the option **IGMP/MLD Setup** from the **IGMP/MLD Snooping** menu and then the following screen page appears. Please note that Query Interval value must be greater than the value of Query Response Interval.



IGMP/MLD Snooping: When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic.

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

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

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

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

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

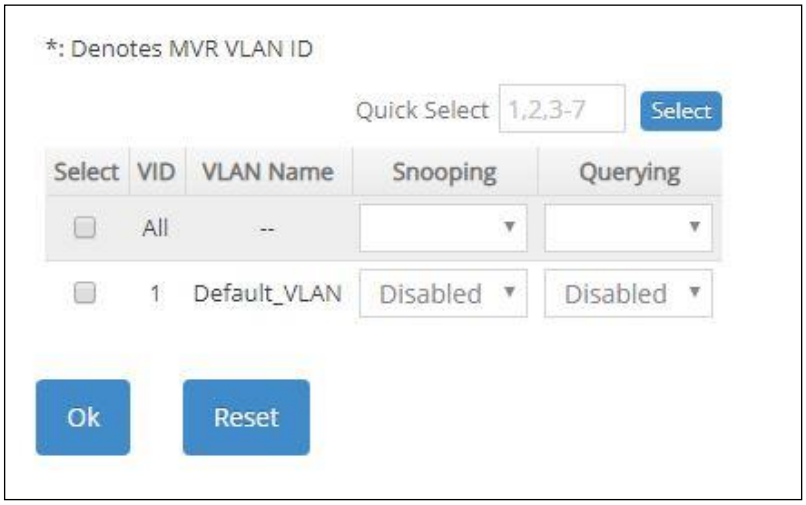
Stream Life Time: When it is enabled, the multicast traffic flow will be stopped once reaching its specified lifespan. The length of Stream Life Time is determined by the total amount of **Query Interval** and **Query Response Interval** (125 and 10 seconds in default, respectively).

Router Port: When ports are connected to the IGMP administrative routers, they should be checked. Or directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field and then press

the **Select** button, the specified port(s) will be checked immediately. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

4.9.1.2 IGMP/MLD VLAN Setup

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



Select: Enable or disable any new settings configured in the row of **All** VID to be applied as well to all VIDs at a time. To enable it, please click on its checkbox in the row of **All** VID, and then all VIDs will be checked immediately afterwards. Or quickly configure the desired VIDs at a time, you can also directly input the VID (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the IGMP/MLD VLAN Setup table, the specified VID(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** VID will be applied to these checked VIDs.

VID: VID of the specific VLAN. And VID marked * stands that it is a MVR VLAN ID.

VLAN Name: View-only field that shows the VLAN name. If the VLAN name belongs to an “Enabled” multicast VLAN ID, it will be automatically changed into the one same as MVR name configured in **MVR > MVR System Setup** function.

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

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

4.9.1.3 IPMC Segment

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

This table will display the overview of each configured IPMC segment. Up to 400 IPMC segments can be created.

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total registered IPMC segments.

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

Click **Add IPMC Segment** to register a new IPMC segment and then the following screen page appears for the further IPMC segments settings.

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

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

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

Click ✔ when the settings are completed, this new IPMC segment will be listed on the IPMC segment table, or click ✖ to cancel the settings.

Click the icon to modify the settings of a specified IPMC segment.

Click the icon to remove a specified registered IPMC segment entry and its settings from the IPMC segment table. Or click **Batch Delete** to remove a number of /all IPMC segments at a time by clicking on the checkbox belonging to the corresponding IPMC segment in the **Action** field and then click **Delete Select Item**, the selected IPMC segment(s) will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

4.9.1.4 IPMC Profile

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

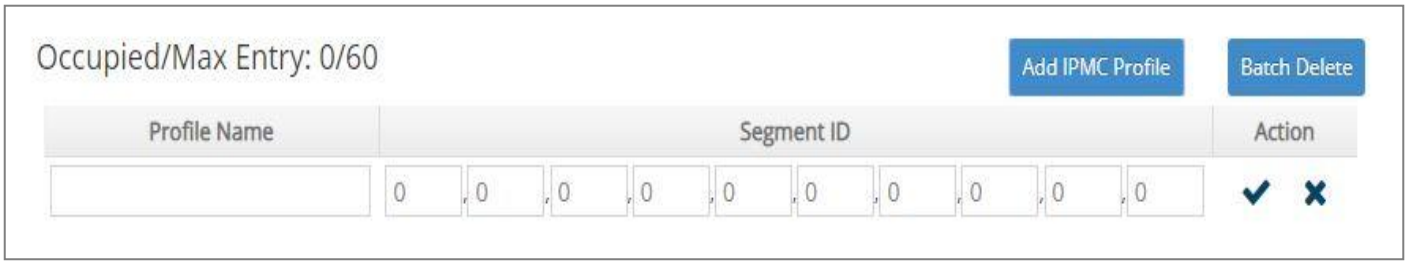
This table will display the overview of each configured IPMC profile. Up to 60 IPMC profiles can be registered.

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total registered IPMC profiles.

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

Click **Add IPMC Profile** to register a new IPMC profile and then the following screen page appears for the further IPMC profile settings.



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

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

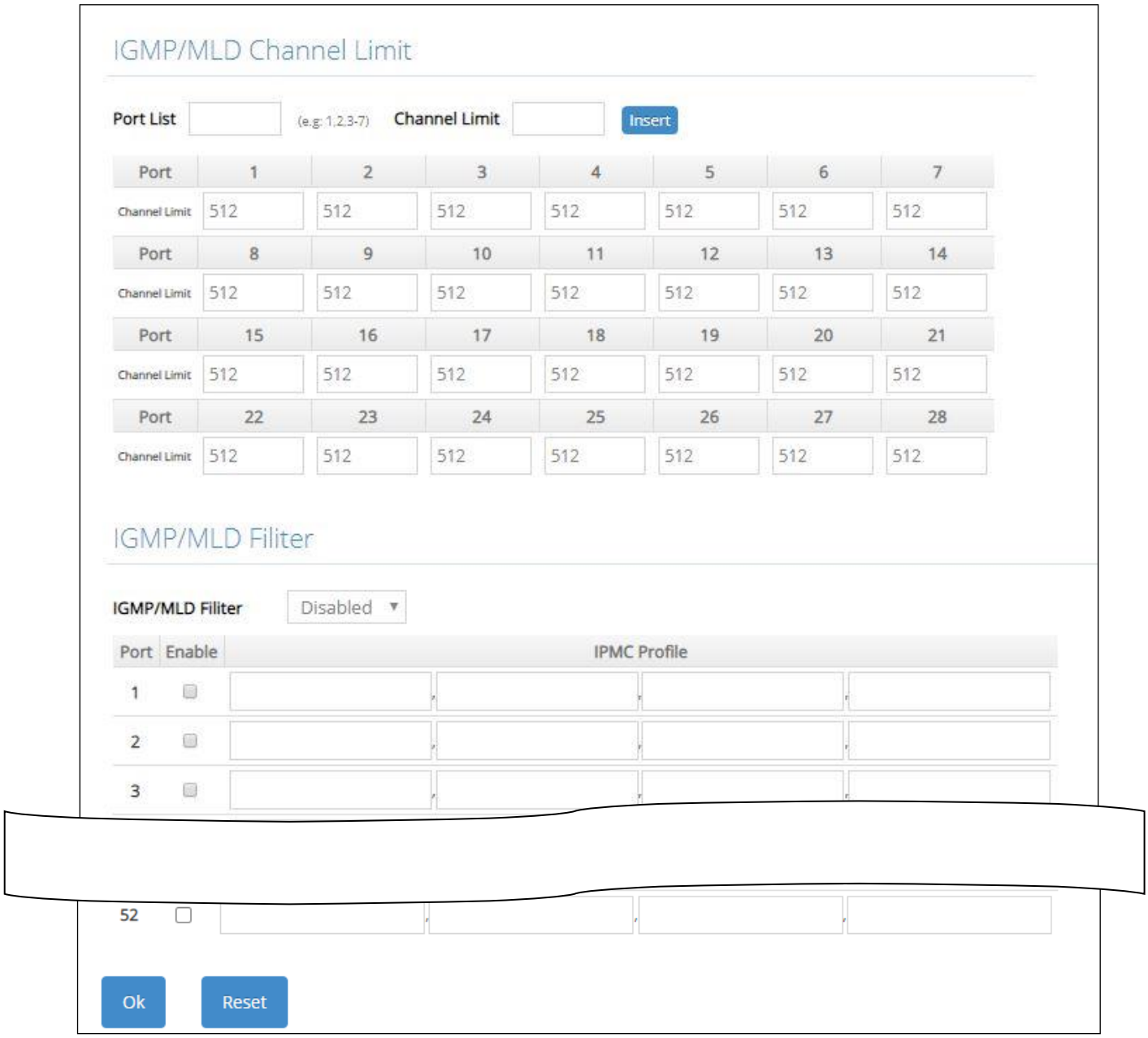
Click ✔ when the settings are completed, this new IPMC profile will be listed on the IPMC profile table, or click ✖ to cancel the settings.

Click the icon to modify the settings of a specified IPMC profile.

Click the icon to remove a specified registered IPMC profile entry and its settings from the IPMC profile table. Or click **Batch Delete** to remove a number of /all IPMC profiles at a time by clicking on the checkbox belonging to the corresponding IPMC profile in the **Action** field and then click **Delete Select Item**, the selected IPMC profile(s) will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

4.9.1.5 IGMP/MLD Filtering

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



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

Channel Limit: Specify the maximum transport multicast stream. Vaild range is 1~512. To quickly set up this parameter at a time, just directly input the port number (e.g.1, 2, 3-7) in the field of **Port List**, the specified port(s) will be given the assigned value in the **Channel Limit** field in front of the **Insert** button immediately when pressing this **Insert** button.

IGMP/MLD Filter: This option is to globally enable or disable the IGMP/MLD filter. The default setting is “Disabled”.

Enable: To enable each port’s IGMP/MLD filtering function by clicking on the checkbox of the corresponding port number. The default setting is “unchecked”, which is disabled.

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

4.9.1.6 IGMP Snooping Status

IGMP Snooping Status allows users to view a list of IGMP queries' information in VLAN(s) such as VLAN ID, Querier and Queries Transmitted/Received packets. Select the option **IGMP Snooping Status** from the **IGMP/MLD Snooping** menu and then the following screen page appears.

Refresh: Click **Refresh** to update the latest IGMP snooping status.

VLAN ID: VID of the specific VLAN. And VLAN ID marked * stands that it is a MVR VLAN ID.

The IGMP querier periodically sends IGMP general queries to all hosts and routers (224.0.0.1) on the local subnet to find out whether active multicast group members exist on the subnet.

Upon receiving an IGMP general query, the Managed Switch forwards it through all ports in the VLAN except the receiving port.

Querier: The state of IGMP querier in the VLAN.

Queries Transmitted: The total amount of IGMP general queries transmitted will be sent to IGMP hosts.

Queries Received: The total amount of received IGMP general queries from IGMP querier.

v1 Reports: The total amount of received IGMP Version 1 reports (packets).

v2 Reports: The total amount of received IGMP Version 2 reports (packets).

v3 Reports: The total amount of received IGMP Version 3 reports (packets).

v2 Leaves: The total amount of received IGMP Version 2 leaves (packets).

4.9.1.7 IGMP Group Table

In order to view the real-time IGMP multicast group status of the Managed Switch, select the option **IGMP Group Table** from the **IGMP/MLD Snooping** menu and then the following screen page appears.

Total Entry: The total number of entries displayed in the IGMP group table.

Refresh: Click **Refresh** to update the IGMP group table.

VLAN ID: The VLAN ID associated with the multicast group. VLAN ID marked * stands that it is an MVR VLAN ID.

Group: The IP address for the multicast group.

Port: The port from which the Managed Switch receives the IGMP join/report message.

Last Reporter: The IP address of the last interested member that sent the IGMP join/report message to join a particular multicast group.

Query Response: A countdown timer of the specified **Query Response Interval**. When the Managed Switch receives an IGMP join/report message from an interested member. It will first display “stopped” first. The Managed Switch will then access the IPTV multicast server and forward the multicast packets to the interested member. At this point, the timer will begin its countdown of the specified **Query Response Interval**.

Report Count: A counter of the received IGMP join/report message. Upon receiving, the Managed switch will reset **Life Time**, also a countdown timer yet of the specified Stream Life Time.

Life Time: A countdown timer of the specified Stream Life Time. Once the timer reaches zero, the multicast traffic flow will be stopped.

4.9.1.8 MLD Snooping Status

MLD Snooping Status allows users to view a list of MLD queries' information in VLAN(s) such as VLAN ID, Querier and Queries Transmitted/Received packets. Select the option **MLD Snooping Status** from the **IGMP/MLD Snooping** menu and then the following screen page appears.

Refresh: Click **Refresh** to update the latest MLD snooping status.

VLAN ID: VID of the specific VLAN. And VLAN ID marked * stands that it is a MVR VLAN ID.

Querier: The state of MLD querier in the VLAN.

Queries Transmitted: The total amount of MLD general queries transmitted will be sent to MLD hosts.

Queries Received: The total amount of received MLD general queries from MLD querier.

v1 Reports: The total amount of received MLD Version 1 reports (packets).

v2 Reports: The total amount of received MLD Version 2 reports (packets).

Done: The total amount of received MLD Version 1 done (packets).

4.9.1.9 MLD Group Table

In order to view the real-time MLD multicast group status of the Managed Switch, select the option **MLD Group Table** from the **IGMP/MLD Snooping** menu and then the following screen page appears.

Refresh: Click **Refresh** to update the latest MLD group table.

VLAN ID: VID of the specific VLAN. And VLAN ID marked * stands that it is a MVR VLAN ID.

Group: The multicast IP address of MLD querier.

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

4.9.2 Static Multicast Configuration

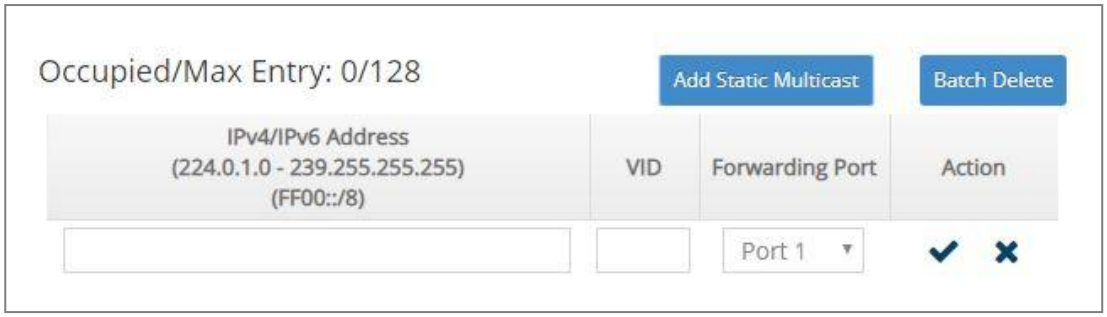
Select the option **Static Multicast Setup** from the **Multicast** menu and then the following screen page appears.

This table will display the overview of each configured static multicast entry. Up to 128 static multicast entries can be created.

Occupied/Max Entry: View-only field.

> **Occupied:** This shows the amount of total registered static multicast entries.
>
> **Max:** This shows the maximum number available for static multicast entry. The maximum number is 128.

Click **Add Static Multicast** to register a new static multicast enery and then the following screen page appears for the further static multicast settings.



IPv4/IPv6 Address: Specify the multicast stream source IPv4/IPv6 address.

VID: Specify a VLAN ID for multicast stream.

Forwarding port: Select a port number for multicast stream forwarding.

Click when the settings are completed, this new static multicast entry will be listed on the static multicast table, or click to cancel the settings.

Click the icon to modify the settings of a specified static multicast entry.

Click the icon to remove a specified registered static multicast entry and its settings from the static multicast table. Or click **Batch Delete** to remove a number of /all static multicast entries at a time by clicking on the checkbox belonging to the corresponding static multicast entry in the **Action** field and then click **Delete Select Item**, the selected static multicast entry/entries will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

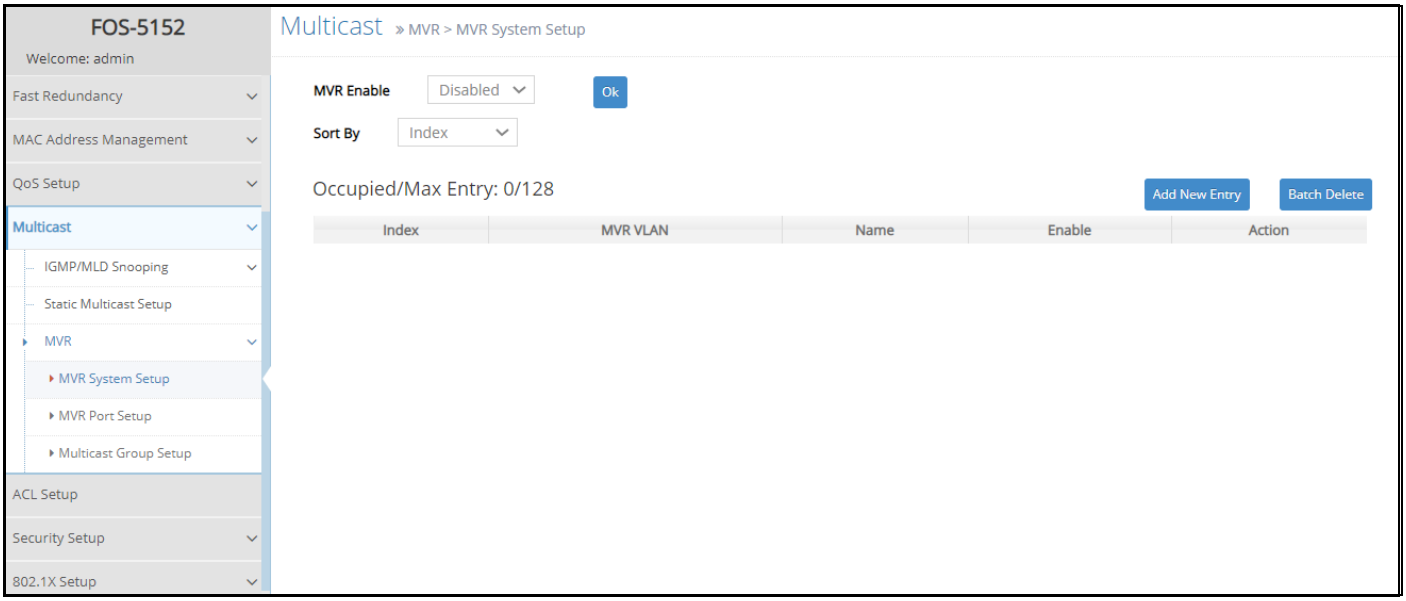
4.9.3 MVR Configuration

MVR (Multicast VLAN Registration) allows clients receiving multicast stream transmitted from the upstream device to reside in different VLANs, which is particularly suitable for networks with the high demand of bandwidth.

Instead of transmitting multiple copies of multicast traffic to clients in the different VLANs separately, an upstream device merely needs to transmit multicast traffic to a multicast VLAN if the configured MVR is enabled on Managed Switch. Therefore, the network bandwidth can greatly be saved and diminish the load of upstream device(s) without sending several identical multicast data flows downstream to each client VLAN.

MVR also allows a client on a port to subscribe/unsubscribe to a multicast stream on the multicast VLAN. MVR not only provides the ability to continuously send multicast streams to the multicast VLAN, but isolates the multicast streams from the client VLANs for the reasons of bandwidth and security.

To configure MVR, please select the subfolder **MVR** and then 3 options will be displayed.



1. **MVR System Setup:** To enable or disable MVR on Managed Switch, and add/edit the multicast VLAN.

2. **MVR Port Setup:** To set up the multicast port and its port type.

3. **Multicast Group Setup:** To create the new multicast group(s) for the created multicast VLAN.

4.9.3.1 MVR Sytstem Setup

MVR System Setup allows users to create the multicast VLANs. Select the option **MVR System Setup** from the **MVR** menu and then the following screen page appears.

This table will display the overview of each configured multicast VLAN entry. Up to 128 MVR entries can be created.

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total MVR entries registered.

Max: This shows the maximum number available for MVR entry. The maximum number is 128.

Sort By: Sort all of the registered MVR entries by selecting **Index/MVR VLAN** option from the **Sort By** pull-down menu.

Click **Add New Entry** to register a new MVR enery and then the following screen page appears for the further MVR settings.

Index: The identification number for each MVR entry.

MVR VLAN: Specify a VLAN ID to configure the specified VLAN as the multicast VLAN.

Name: Specify a MVR name for the specific multicast VLAN. Up to 15 characters can be accepted.

Enable: Enable or disable the new MVR you create. To enable this new MVR, just click on the checkbox. The default setting is “checked”, which is enabled.

Click **OK** when the settings are completed, this new MVR entry will be listed on the MVR table, or click **Cancel** to cancel the settings.

Click the icon to modify the settings of a specified MVR entry.

Click the icon to remove a specified registered MVR entry and its settings from the MVR table. Or click **Batch Delete** to remove a number of/all MVR entries at a time by clicking on the checkbox belonging to the corresponding MVR entry in the **Action** field and then click **Delete Select Item**, the selected MVR entry/entries will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

4.9.3.2 MVR Port Setup

MVR Port Setup allows users to configure the receiver/sender MVR port for the existing multicast VLANs. Select the option **MVR Port Setup** from the **MVR** menu and then the following screen page appears.

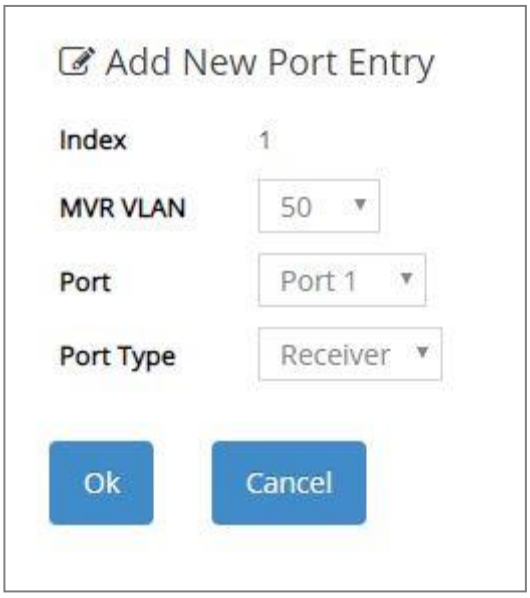
This table will display the overview of each configured MVR port entry. Up to 512 MVR port entries can be created.

Occupied/Max Entry: View-only field.

> **Occupied:** This shows the amount of total MVR port entries registered.
>
> **Max:** This shows the maximum number available for MVR port entry. The maximum number is 512.

Sort By: Sort all of the registered MVR port entries by selecting **Index/MVR VLAN/Port** option from the **Sort By** pull-down menu.

Click **Add New Entry** to register a new MVR port enery and then the following screen page appears for the further MVR port settings.



Index: The identification number for each MVR port entry.

MVR VLAN: Specify an existing the multicast VLAN for the specific MVR port entry.

Port: Specify a port number to configure the specified port as the multicast port.

Port Type: Specify the port type for the specific multicast port, either receiver or sender.

> **Receiver port:** Configure a port as a receiver port if it is a client port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages. Receiver ports cannot belong to the multicast VLAN.
>
> **Sender port:** The sender port is the multicast server port. Configure uplink ports that receive and send multicast data as sender ports. Clients cannot be directly connected to sender ports.

NOTE: *The port configured as the "Receiver Port" cannot be the "Sender Port".*

Click **OK** when the settings are completed, this new MVR port entry will be listed on the MVR table, or click **Cancel** to cancel the settings.

Click the icon to modify the settings of a specified MVR port entry.

Click the icon to remove a specified registered MVR port entry and its settings from the MVR port table. Or click **Batch Delete** to remove a number of /all MVR port entries at a time by clicking on the checkbox belonging to the corresponding MVR port entry in the **Action** field and then click **Delete Select Item**, the selected MVR port entry/entries will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

4.9.3.3 Multicast Group Setup

Multicast Group Setup allows users to configure a range of multicast IP addresses for the existing multicast VLANs. Select the option **Multicast Group Setup** from the **MVR** menu and then the following screen page appears.

This table will display the overview of each configured multicast group entry. Up to 128 multicast group entries can be created.

Occupied/Max Entry: View-only field.

> **Occupied:** This shows the amount of total multicast group entries registered.
>
> **Max:** This shows the maximum number available for multicast group entry. The maximum number is 128.

Sort By: Sort all of the registered multicast group entries by selecting **Index/MVR VLAN/Multicast** option from the **Sort By** pull-down menu.

Click **Add New Entry** to register a new multicast group enery and then the following screen page appears for the further multicast group settings.

Index: The identification number for each multicast group entry.

MVR VLAN: Specify an existing the multicast VLAN from the pull-dwon menu for the specific multicast group entry.

Multicast Group: Pull down the menu to decide the format of multicast IP address between IPv4 and IPv6 first, and then set up the range of multicast IP addresses to create a new multicast group for the specific multicast VLAN. Either you can select all multicast IP addresses by clicking on **All** option, in which the multicast traffic of all multicast IP addresses will be sent to the designated multicast VLAN.

Or specify a range of multicast IP addresses by filling in the multicast IP address that starts and ends respectively. The multicast traffic within this range of IP addresses will be sent to the

designated multicast VLAN if this option is clicked. The default setting is **All**.

NOTE: *The value of the multicast IP address that starts for the specific multicast group cannot be greater than the one that ends.*

Click **OK** when the settings are completed, this new multicast group entry will be listed on the multicast group table, or click **Cancel** to cancel the settings.

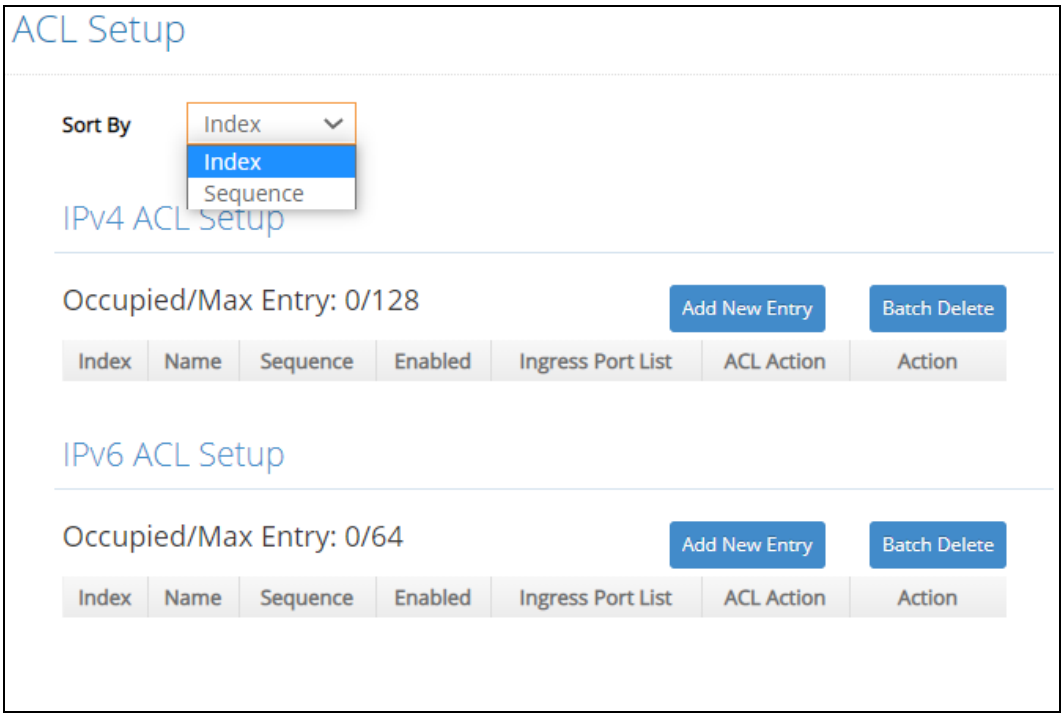
Click the icon to modify the settings of a specified multicast group entry.

Click the icon to remove a specified registered multicast group entry and its settings from the multicast group table. Or click **Batch Delete** to remove a number of/all multicast group entries at a time by clicking on the checkbox belonging to the corresponding multicast group entry in the **Action** field and then click **Delete Select Item**, the selected multicast group entry/entries will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

4.10 Access Control List (ACL) Setup

Creating an access control list allows users to define who has the authority to access information or perform tasks on the network. In the Managed Switch, users can establish entries applied to port numbers to permit or deny actions.

Select **ACL Setup** from the **Main Menu** and then the following screen page appears.



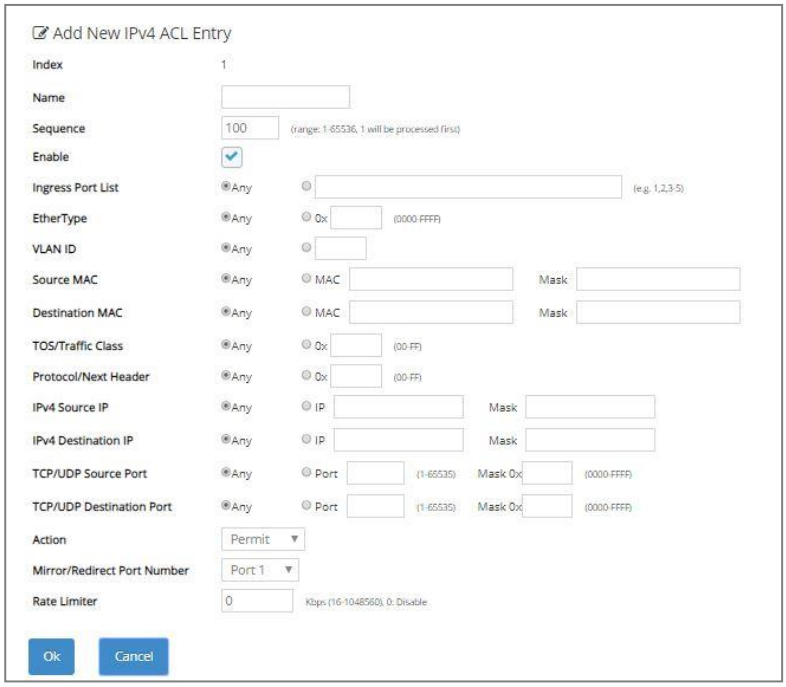
The IPv4 or IPv6 ACL tables will display the overview of each configured IPv4 or IPv6 ACL entry respectively. Up to 64 IPv4 ACL entries and 32 IPv6 ACL entries can be created.

Occupied/Max Entry: View-only field.

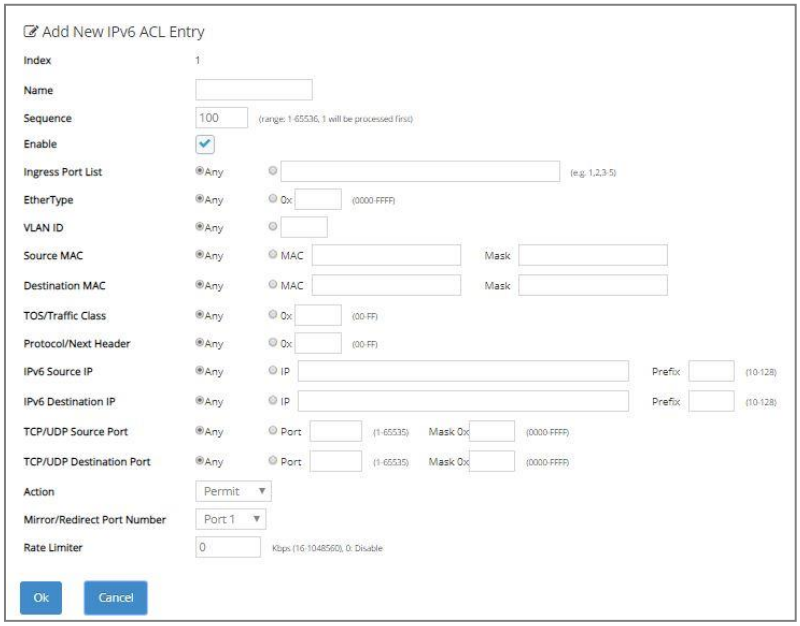
Occupied: This shows the amount of total IPv4 or IPv6 ACL entries that have already been created.

Max: This shows the maximum number available for IPv4 or IPv6 ACL entries. The maximum number for IPv4 ACL is 64 entries, and the maximum number for IPv6 ACL is 32 entries.

Separately click **Add New Entry** provided for *IPv4 ACL Setup* or *IPv6 ACL Setup* to create a new IPv4/IPv6 ACL entry and then the following screen page appears for the further ACL settings.



Add an IPv4 ACL Entry



Add an IPv6 ACL Entry

Sort By: Sort all of the created IPv4/IPv6 ACL entries by selecting **Index**/**Sequence** option from the **Sort By** pull-down menu.

Index: The identification number for each ACL entry.

Name: Specify the name of the ACL entry.

Sequence: Valid range: 1-65536, 1 will be processed first. Default: 100

Enable: Enable or disable the ACL entry.

Ingress Port List: Select “Any” or specify a port number (e.g. 1, 2, 3-5) as the ingress port.

EtherType: Select “Any” or specify an Ethernet type value (0x 0000-FFFF).

VLAN ID: Select “Any” or specify a VLAN ID.

Source MAC: Select “Any” or specify a source MAC address and Mask.

Destination MAC: Select “Any” or specify a destination MAC address and Mask.

TOS/Traffic Class: Select “Any” or specify a TOS/Traffic class (0x 00-FF).

Protocol/Next Header: Select “Any” or specify IPv4 protocol and IPv6 next header (0x 00-FF).

IPv4 Source IP (for IPv4 ACL Setup only): Select “Any” or specify an IPv4 Source IP address and Mask.

IPv4 Destination IP (for IPv4 ACL Setup only): Select “Any” or specify an IPv4 Destination IP address and Mask.

IPv6 Source IP (for IPv6 ACL Setup only): Select “Any” or specify an IPv6 Source IP address and prefix (10-128).

IPv6 Destination IP (for IPv6 ACL Setup only): Select “Any” or specify an IPv6 Destination IP address and prefix (10-128).

TCP/UDP Source Port: Select “Any” to filter frames from any source port or specify a source port number and Mask (0x 0000-FFFF).

TCP/UDP Destination Port: Select “Any” to filter frames bound for any destination port or specify a destination port number and Mask (0x 0000-FFFF).

Action: Specify the action, including Deny, Permit, Mirror or Redirect to the ACL-matched packet.

Mirror/Redirect Port Number: Specify a port number that you would like to configure for Mirror/Redirect.

Rate Limiter: Configure the rate limiter. Valid Range: 16-1048560 Kbps, the default value is “0”. “0” means “Disable”.

Click **OK** when the settings are completed, this new ACL entry will be listed on the corresponding ACL table, or click **Cancel** to cancel the settings.

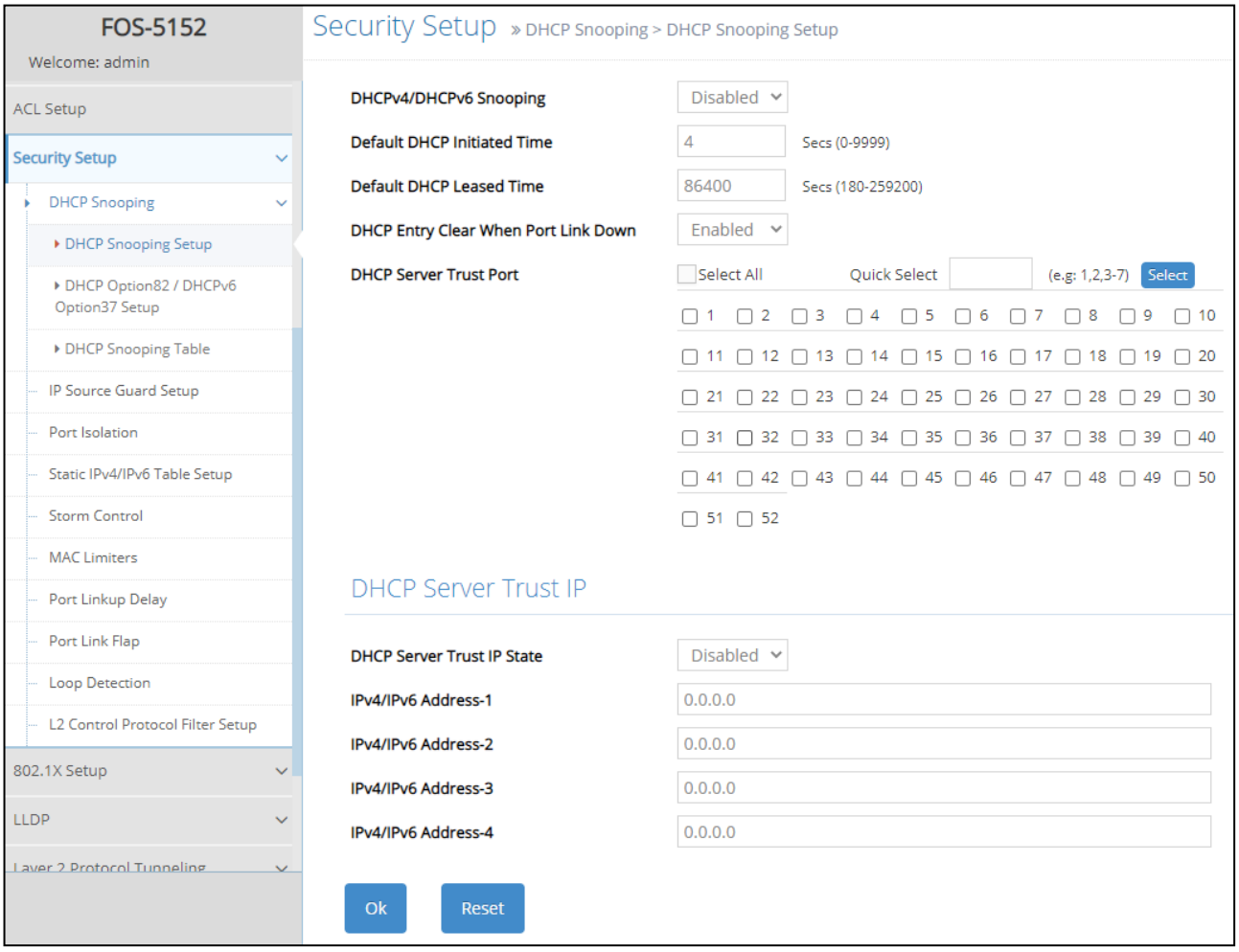
Click the  icon to modify the settings of a specified ACL entry.

Click the  icon to remove an existing ACL entry and its settings from the IPv4 or IPv6 ACL table. Or click **Batch Delete** to remove a number of /all ACL entries at a time by clicking on the checkbox belonging to the corresponding ACL entry in the **Action** field and then click **Delete Select Item**, the selected ACL entries will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

4.11 Security Setup

In this section, several Layer 2 security mechanisms are provided to increase the security level of your Managed Switch. Layer 2 attacks are typically launched by or from a device that is physically connected to the network. For example, it could be a device that you trust but has been taken over by an attacker. By default, most security functions available in this Managed Switch are turned off, to prevent your network from malicious attacks, it is extremely important for you to set up appropriate security configurations. This section provides several security mechanisms to protect your network from unauthorized access to a network or redirect traffic for malicious purposes, such as Source IP Spoofing and ARP Spoofing.

Select the folder **Security Setup** from the **Main Menu** and then 8 options within this folder will be displayed



1. **DHCP Snooping:** To set up DHCP Snooping and DHCP server trust ports, enable or disable DHCP Option 82 (for DHCPv4) and Option 37 (for DHCPv6) relay agent global setting, show each port's configuration, set up suboptions such as circuit-ID and remote-ID, and view the DHCP learning table, etc.

2. **IP Source Guard Setup:** To set up each client port for DHCP Snooping.

3. **Port Isolation:** Set up port's communication availability that they can only communicate with a given "uplink".

4. **Static IPv4/IPv6 Table Setup:** To create static IPv4/IPv6 table for DHCP snooping setting.

5. **Storm Control:** To prevent the Managed Switch from unicast, broadcast, and multicast storm.

6. **MAC Limiters:** Set up MAC Address limit and view the MAC Limit status of each port.

7. **Loop Detection:** Enable or disable Loop Detection function, set up Loop Detection configuration and view the Loop Detection status of each port.

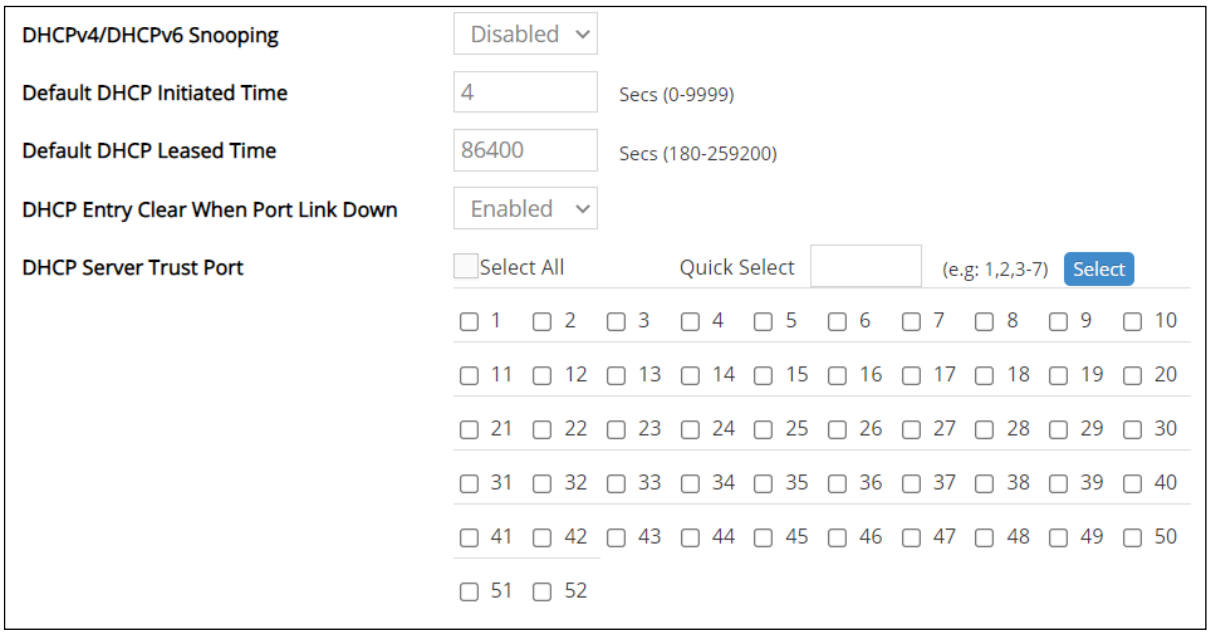
8. **L2 Control Protocol Filter Setup:** Enable or disable L2 Control Protocol.

4.11.1 DHCP Snooping Configuration

Select the option **DHCP Snooping** from the **Security Setup** folder and then three functions, including DHCP Snooping Setup, DHCP Option 82 / DHCPv6 Option 37 Setup and DHCP Snooping Table will be displayed for your selection.

4.11.1.1 DHCP Snooping Setup

The following screen page appears if you choose **DHCP Snooping Setup** function.



DHCPv4/DHCPv6 Snooping: Enable or disable DHCPv4/DHCPv6 Snooping function.

Default DHCP Initiated Time: Specify the time value (0~9999 Seconds) that packets might be received.

Default DHCP Leased Time: Specify packets' expired time (180~259200 Seconds).

DHCP Entry Clear When Port Link Down: Enable or disable DHCPv4/DHCPv6 snooping entry clear. When it's enabled, the entries of a DHCPv4/DHCPv6 clients kept on the Managed Switch will be removed once the link of the learning port is down.

DHCP Server Trust Port: Specify designated port(s) to be Trust Port that can give you "offer" from DHCP server. Check any port box to enable it or directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field and then press the **Select** button, the specified port(s) will be checked immediately. Besides, you can choose all ports at a time by clicking on the checkbox in front of

Select All as well.

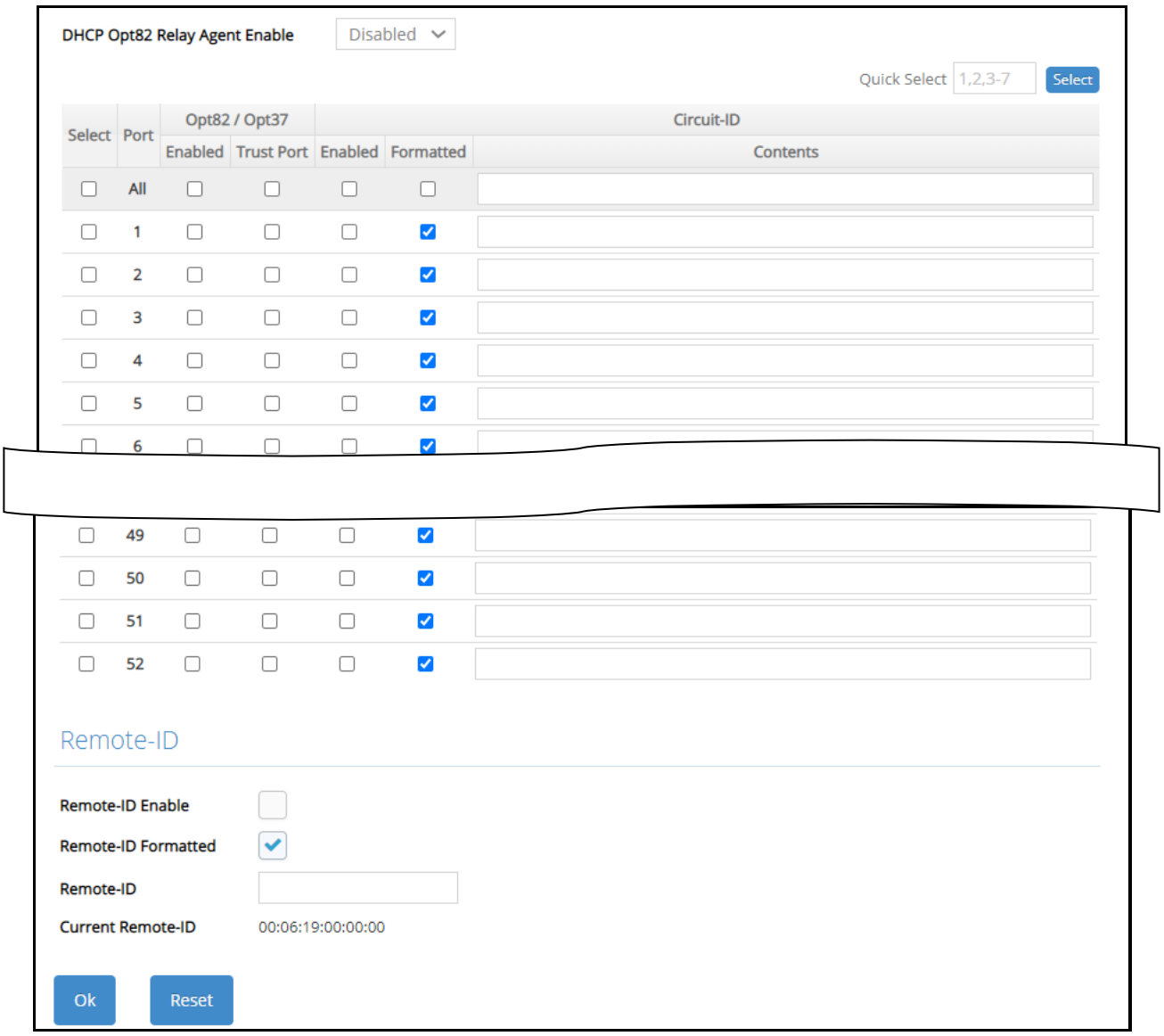
DHCP Server Trust IP State: After enabling Trust Port, you may additionally specify Trust IP address for identification of DHCP server. Click the drop-down menu and select “Enabled”, then specify Trust IP address.

4.11.1.2 DHCP Option 82 / DHCPv6 Option 37 Setup

The Managed Switch can add information about the source of client DHCP requests that relay to DHCP server by adding Relay Agent Information. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. The feature of DHCP Relay Agent Information adds Agent Information field to the Option 82 field that is in the DHCP headers of client DHCP request frames.

Besides, the Managed Switch adds the option 82 information in the packet when it receives the DHCP request. In general, the switch MAC address (the remote-ID suboption) and the port identifier, vlan-mod-port or snmp-ifindex are included in the option 82 information. You can configure the remote ID and circuit ID.

The following screen page appears if you choose **DHCP Option 82 / DHCPv6 Option 37 Setup** function.



DHCP Opt82 Relay Agent Enable: To globally enable or disable DHCP Option 82 Relay Agent global setting. When enabled, Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers recognizing the Relay Agent Information option may use the Information to implement IP address or other parameter assignment policies. Switch or Router (as the DHCP relay agent) intercepting the DHCP requests, appends the circuit ID + remote ID into the option 82 fields (or Option 37 when DHCPv6) and forwards the request message to DHCP server.

Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the DHCP Option 82 / DHCPv6 Option 37 Setup table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Port: The number of each port.

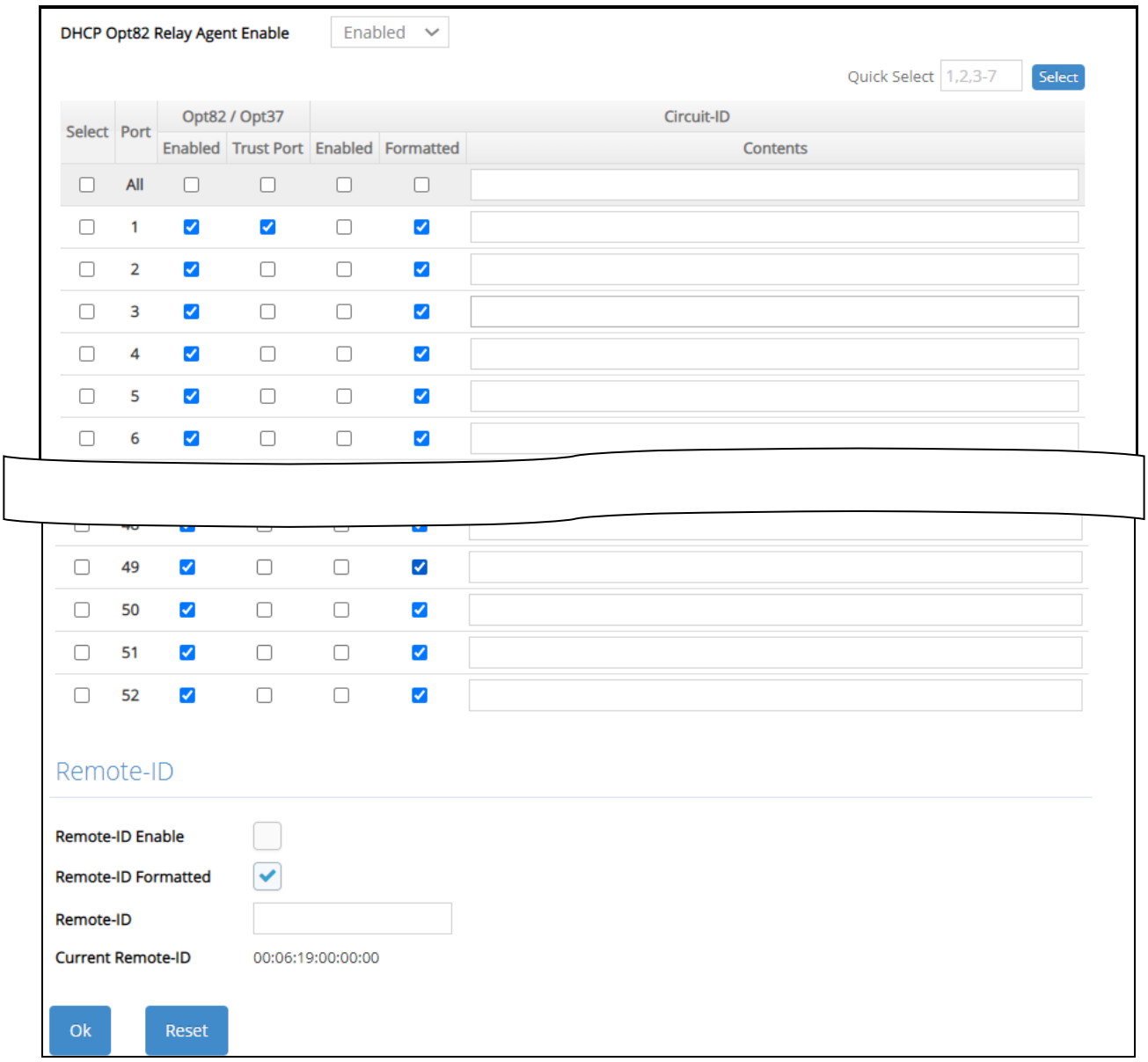
Enabled in Opt82/Opt37 field**:**

Enable (check): Add Agent information.

Disable (uncheck): Forward.

Trust Port in Opt82/Opt37 field**:** Click on the checkbox of the corresponding port number if you would like ports to become trust ports. The trusted ports will not discard DHCP messages.

For example,



A DHCP request is from Port 1 that is marked as both Opt82 port and trust port.

A. If a DHCP request is with Opt82 Agent information and then the Managed Switch will forward it.
B. If a DHCP request is without Opt82 Agent information and then the Managed Switch will add Opt82 Agent information and forward it.

A DHCP request is from Port 2 that is marked as Opt82 port.

A. If a DHCP request is with Opt82 Agent information and then the Managed Switch will drop it because it is not marked as a trust port.
B. If a DHCP request is without Opt82 Agent information and then the Managed Switch will add Opt82 Agent information and then forward it.

Circuit ID Suboption: This suboption may be added by DHCP relay agents that terminate switched or permanent circuits. It encodes an agent-local identifier of the circuit from which a DHCP client-to-server packet was received. It is intended for use by agents in relaying DHCP responses back to the proper circuit. Servers may use the circuit ID for IP and other parameter assignment policies.

Remote-ID Suboption: This suboption may be added by DHCP relay agents that terminate switched or permanent circuits and have machanisms to identify the remote host end of the circuit. DHCP servers may use this option to select parameters specific to particular users, hosts, or subscriber modems. The relay agent may use this field in addition to or instead of the Agent Circuit ID field to select the circuit on which to forward the DHCP reply.

Enabled in Circuit-ID field**:** Click on the checkbox of the corresponding port number you would like to configure with circuit ID.

Formatted in Circuit-ID field**:** Also click on the checkbox to add the circuit ID type and length of the circuit ID packet or uncheck to hide the circuit ID type and length of the circuit ID packet. The default setting is checked.

Contents in Circuit-ID field**:** Specify the VLAN and port identifier using a VLAN ID in the range of 1 to 4094. Besides, you can configure the circuit ID to be a string of up to 63 characters. The default circuit ID is the port identifier, the format of which is vlan-mod-port.

Remote-ID Enable: Click on the checkbox to enable Remote ID suboption or uncheck to disable it.

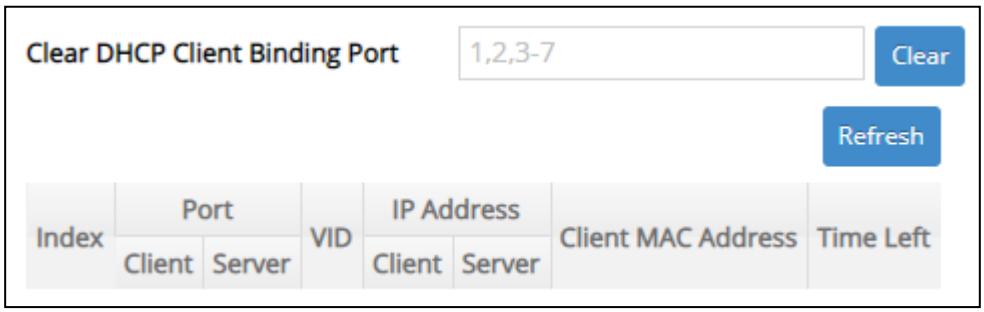
Remote-ID Formatted: Click on the checkbox to add the Remote ID type and length of the Remote ID packet or uncheck to hide the Remote ID type and length of the Remote ID packet. The default setting is checked.

Remote-ID: You can configure the remote ID to be a string of up to 63 characters. The default remote ID is the switch's MAC address.

Current Remote-ID: Display the current remote ID of the switch.

4.11.1.3 DHCP Snooping Table

DHCP Snooping Table displays the Managed Switch's DHCP Snooping table. The following screen page appears if you choose **DHCP Snooping Table** function.



Clear DHCP Client Binding Port: Clear the DHCPv4/DHCPv6 snooping entry. Specify the DHCP client binding port, and click **Clear** to remove the intended DHCPv4/DHCPv6 snooping entry.

Refresh: Click **Refresh** to update the DHCP snooping table.

Port of Client: View-only field that shows where the DHCP client binding port is.

Port of Server: View-only field that shows the port where the IP addrsss is obtained from.

VID: View-only field that shows the VLAN ID of the client port.

IP Address of Client: View-only field that shows the client IP address.

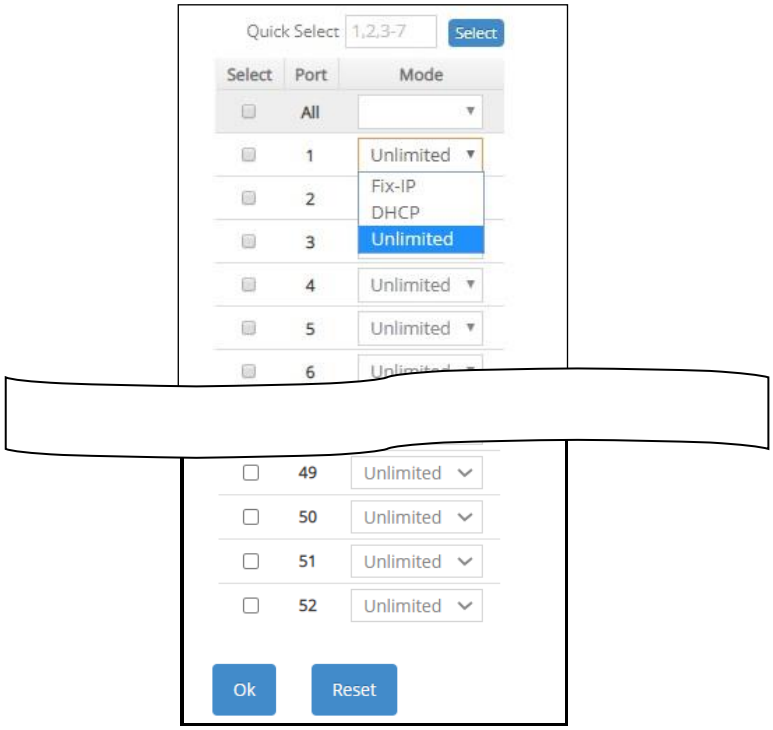
IP Address of Server: View-only field that shows the DHCP server IP address.

Client MAC Address: View-only field that shows the client MAC address.

TimeLeft: View-only field that shows DHCP client lease time.

4.11.2 IP Source Guard Setup

Select the option **IP Source Guard Setup** from the **Security Setup** menu and then the following screen page appears.



Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the IP Source Guard Setup table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Port: The number of each port.

Source Guard Mode: To specify the authorized access type for each port. There are three options available.

Unlimited: Non-Limited (Allows both static IP and DHCP-assigned IP).

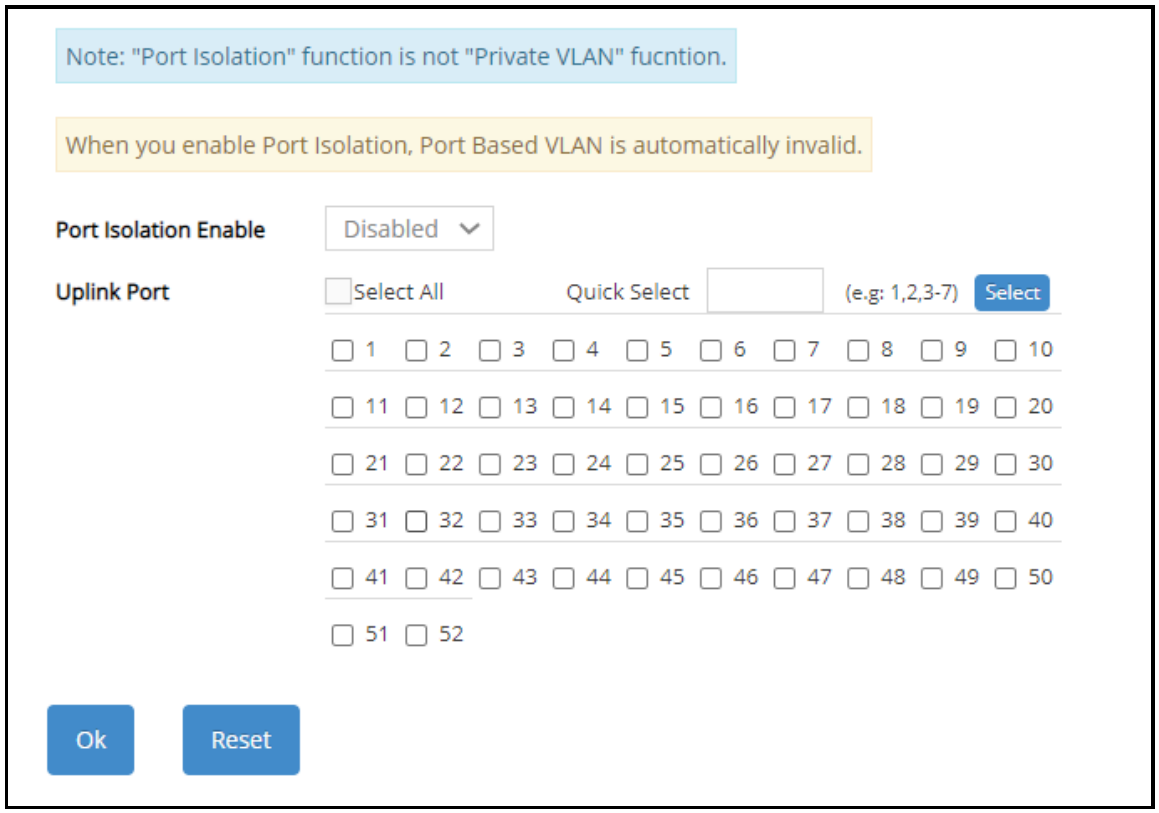
DHCP: DHCP-assigned IP address only.

Fix-IP: Only static IP (You must create Static IP table first. Refer to **Static IPv4/IPv6 Table Setup** for further information.).

4.11.3 Port Isolation

This is used to set up port's communication availability that they can only communicate with a given "uplink". Please note that if the port isolation function is enabled, the Port-based VLAN will be invaild automatically. Also note that "Port Isolation" function is not "Private VLAN" fucntion.

Select the option **Port Isolation** from the **Security Setup** menu and then the following screen page appears.



Port Isolation Enable: Enable or disable port isolation function. If port isolation is set to enabled, the ports cannot communicate with each other.

Uplink Port: By clicking on the checkbox of the corresponding port number to select the ports as uplinks that are allowed to communicate with other ports of the Managed Switch. Or directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field and then press the **Select** button, the specified port(s) will be checked immediately. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

4.11.4 Static IPv4/IPv6 Table Setup

Click the option **Static IPv4/IPv6 Table Setup** from the **Security Setup** menu and then the following screen page appears.

This table will display the overview of each configured static IPv4/IPv6 IP address and port mapping. Up to 48 static IP addresses can be created.

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total registered static IP addresses.

Max: This shows the maximum number available for static IP address registration. The maximum number is 48.

Click **Add IPv4/IPv6 Table** to register a new static IP address entry and then the following screen page appears for the further static IP address settings.

IPv4/IPv6 Address: Specify an IPv4/IPv6 address that you accept.

VLAN ID: Specify the VLAN ID. (0 means without VLAN ID)

Port: Specify the connection port number. (Port 1~28)

Click ✔ when the settings are completed, this new static IP address will be listed on the static IPv4/IPv6 table, or click ✖ to cancel the settings.

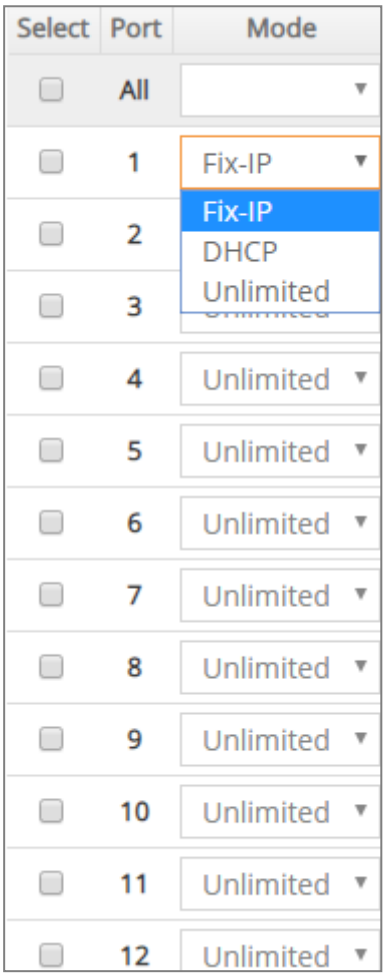
Click the icon to modify the settings of a specified static IP address.

Click the icon to remove a specified static IP address entry and its settings from the static IPv4/IPv6 table. Or click **Batch Delete** to remove a number of /all static IP addresses at a time by clicking on the checkbox belonging to the corresponding static IP address in the **Action** field and then click **Delete Select Item**, the selected static IP address/addresses will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

4.11.4.1 Configure DHCP Snooping

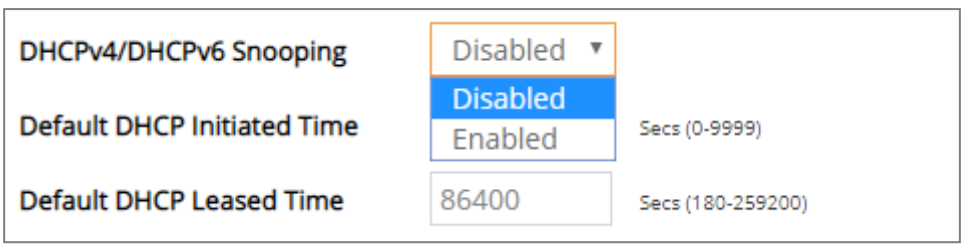
When you would like to use DHCP Snooping function, follow the steps described below to enable a client to receive an IP from DHCP server.

Step 1. Select each port's IP type



Select "Unlimited" or "DHCP".

Step 2. Enable DHCP Snooping



Step 3. Connect your clients to the Managed Switch

After you complete Step 1 & 2, connect your clients to the Managed Switch. Your clients will send a DHCP Request out to DHCP Server soon after they receive a DHCP offer. When DCHP Server

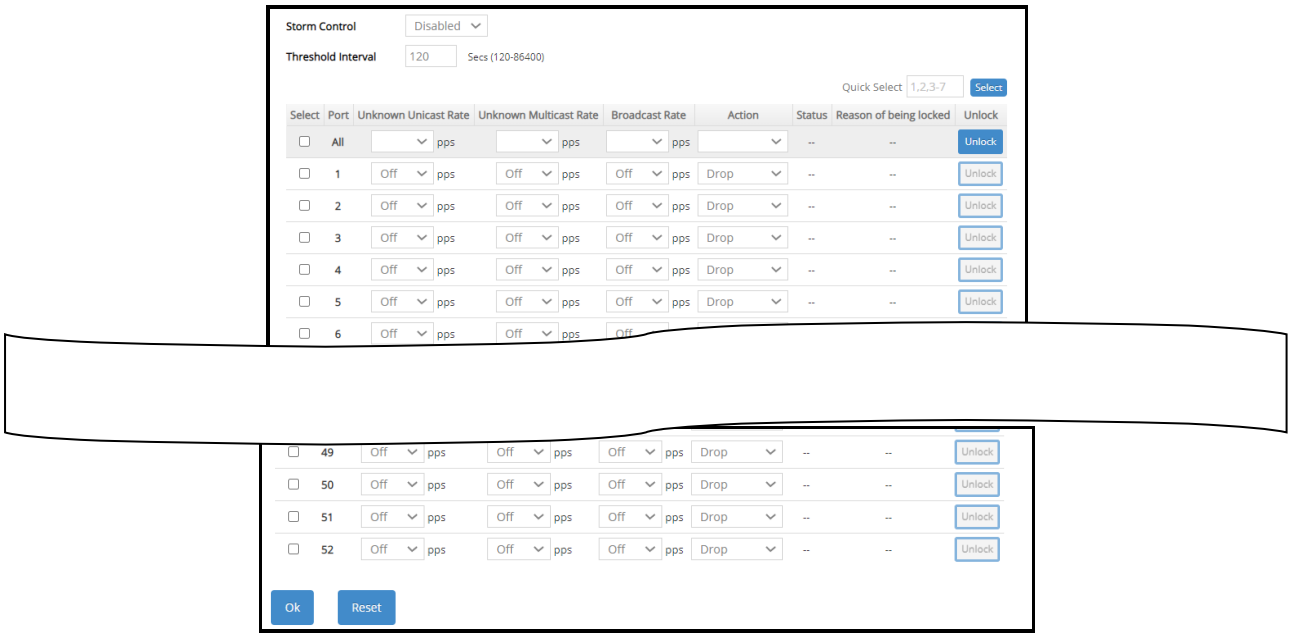
responds with a DHCP ACK message that contains lease duration and other configuration information, the IP configuration process is complete.

If you connect clients to the Managed Switch before you complete Step 1 & 2, please disconnect your clients and then connect your clients to the Managed Switch again to enable them to initiate conversations with DHCP server.

4.11.5 Storm Control

When a device on the network is malfunctioning or application programs are not well designed or properly configured, broadcast/unknown multicast/unknown unicast 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/unknown multicast/unknown unicast traffic on a per port basis so as to protect network from broadcast/unknown multicast/ unknown unicast storms. Any broadcast/unknown multicast/unknown unicast packets exceeding the specified value will then be dropped.

Select the option **Storm Control** from the **Security Setup** menu to set up storm control parameters for each port and then the following screen page appears.



Storm Control: Enable or disable the storm control function globally.

Threshold Interval: To set up the time interval of sending the alarm trap or system log if broadcast/unknown multicast/unknown unicast packets flood continuously. Valid range: 120-86400 seconds. Default is 120 seconds.

Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the Storm Control setup table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Port: The number of the port.

Three options of frame traffic are provided to allow users to enable or disable the storm control:

Unknown Unicast Rate: Enable or disable unknown Unicast traffic control and set up unknown Unicast Rate packet per second (pps) for each port. 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k can be chosen from the pull-down menu of each port.

Unknown Multicast Rate: Enable or disable Unknown Multicast traffic control and set up Unknown Multicast Rate packet per second (pps) for each port. 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k can be chosen from the pull-down menu of each port.

Broadcast Rate: Enable or disable Broadcast traffic control and set up broadcast Rate packet per second (pps) for each port. 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k can be chosen from the pull-down menu of each port.

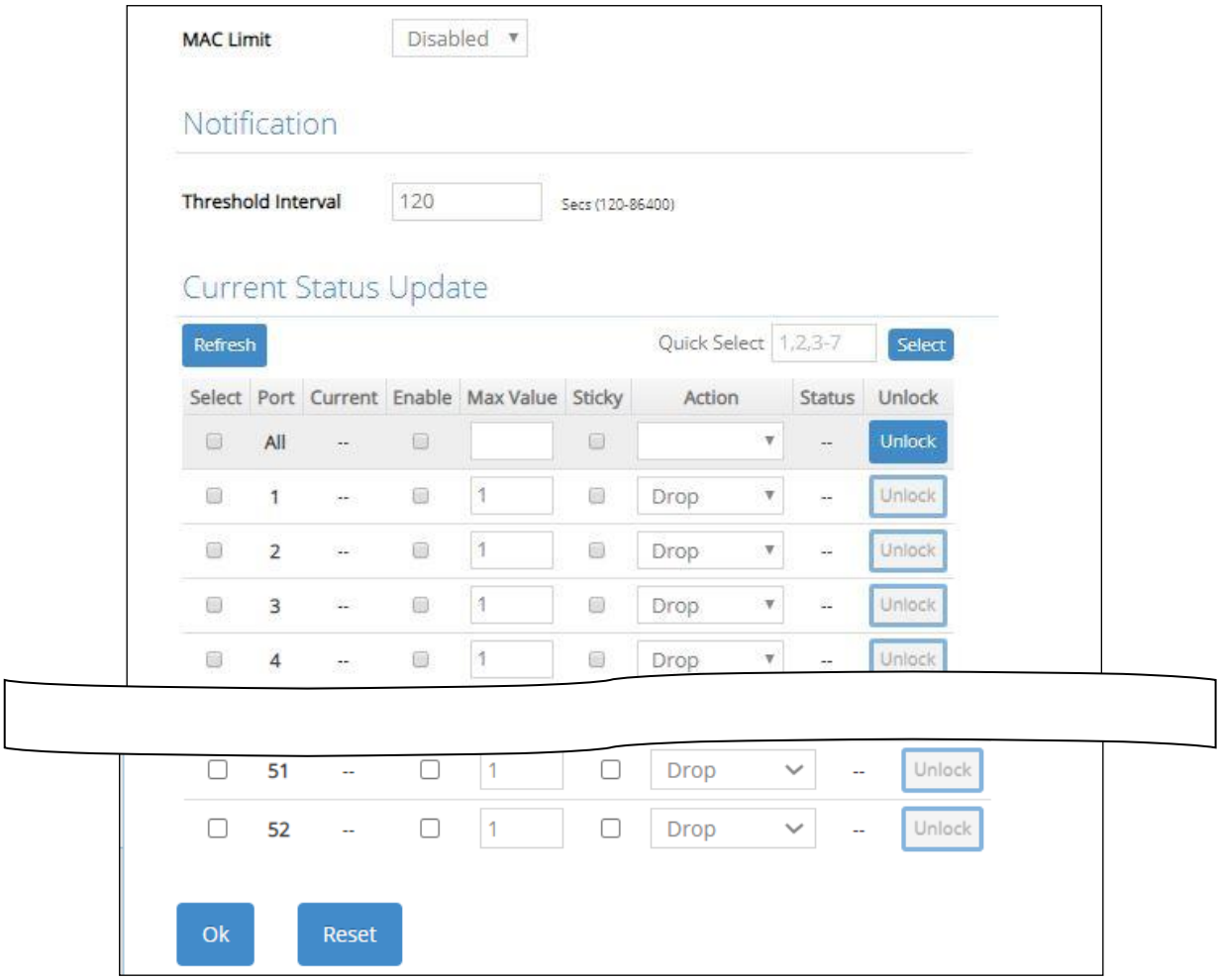
4.11.6 MAC Limiters

This is to set number of threshold within which MAC address can be learned. After it reaches the threshold, any other incoming MAC address would be dropped or port would be shutdown until the recovery mechanism activates. Please note that MAC address table will be erased if the Mac Limit function is enabled.

Besides, the Sticky MAC address function is also provided to keep the event that the packets with the same source MAC address are received by different ports from being taken place. In case this function of the specified port is enabled (the port is also known as the sticky MAC port), then, other ports of the switch cannot receive the packets with the same source MAC address learned by this sticky MAC port anymore. If other ports receive the packets with the same source MAC address again, these packets will be dropped by the switch.

Generally, any auto-learned MAC address from the switch will be a dynamic MAC address. Through this Sticky MAC address function, however, the MAC address learned by the sticky MAC port will automatically be turned into a static one in MAC address table. But, this kind of static MAC address is regarded as a “Sticky” type of MAC address, and it still does not write into the running configuration file. To transfer the MAC address type from “Sticky” into "Manual", and write it into the running configuration file, you may refer to Section 4.6.2 “Static MAC Table Setup”.

Select the option **MAC Limiters** from the **Security Seup** menu to set up MAC Limit, Sticky and Action parameters for ports and then the following screen page appears.



MAC Limit: Globally enable the MAC Limit function of the switch. After that, proceed to further port settings as shown below.

Threshold Interval for Notification**:** To set up the time interval of sending the alarm trap or system log if the number of source MAC address learned exceeds the limit continuously.

Refresh: Click **Refresh** to update the MAC Limiters status.

Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the Storm Control setup table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Port: The number of each port.

Current: The current number of MAC addresses that have been learned by each port.

Enable: Click on the checkbox of the corresponding port number to enable the MAC Limit function on the specific port(s). Please note that port mac address table will be erased if the Mac Limit function is enabled.

Max Value: Specify the maximum number of source MAC address that can be learned. The range of number that can be configured is 1~50.

Sticky: Enable or disable the Stick MAC address function for a port individually. Click on the checkbox of the corresponding port number to enable this function on the specific port(s). Default setting is “Disabled”.

Action: Either “Drop” or “Shutdown” two types of the action can be chosen by clicking on the pull-down menu. The selected action will be taken when the MAC addresses learned exceed the limit you configure. Please note that if the port acts as the uplink port, it is highly recommended NOT to configure this value as “Shutdown” when its MAC Limit is enabled. Default setting is “Drop”.

Status: View-only field that shows each port’s locked/unlocked status of MAC Limit. The port will only be locked if its MAC Limiter is enabled, the port’s action is configured as “shutdown”, and the number of current MAC address learned exceeds the threshold. It will show “--" when the “Drop” action of the port is chosen.

Unlock: If the MAC Limit-enabled port’s action is set as “Shutdown” and the number of **Max Value** ≧ the number of **Current**, the **Unlock** button cannot be pressed; however, if the number of **Max Value** < the number of **Current**, the **Unlock** button can be pressed to unlock the specific port.

NOTE1: *Once a sticky MAC port‘s counts of MAC address has reached the threshold (e.g. 30 counts), the packet (e.g. No.31) with the same source MAC address received by other port will not be dropped and this MAC address will be learned as a dynamic one in MAC address table.*

NOTE2: *If the user needs to modify the limit of MAC address to a value (e.g. 5 counts) less than the threshold while the port’s counts of MAC address have reached the threshold (e.g. 30 counts). An error message of “Maximum is less than number of currently secured MAC addresses” will be pop up.*

4.11.7 Loop Detection Configuration

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:

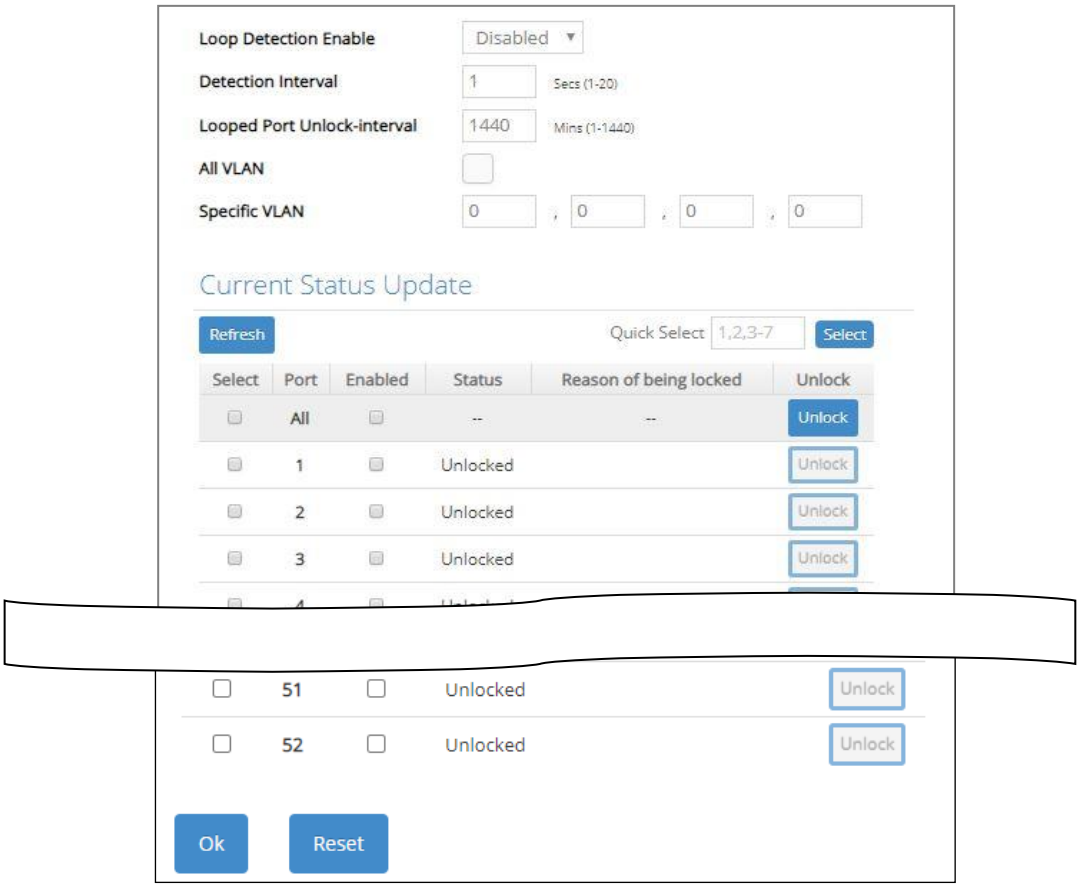
1. It blocks the relevant port to prevent broadcast storms, and send out SNMP trap to inform the network administrator. In other words, the system stops forwarding all the traffic via the looped port. However, the system will process the Loop Detection, RSTP and LLDP packets received on the looped port.
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 receive 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 in orange even the connected network cable is unplugged out of looped port.*

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



Loop Detection Enable: Enable or disable 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 20 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-vids configured in the **VLAN Interface** under **IEEE 802.1q Tag VLAN** (Refer to Section 4.4.4.2)

NOTE: *When All VLAN checkbox 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.*

Refresh: Click **Refresh** to update the Loop Detection status.

Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the Loop Detection setup table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Port: The number of each port.

Enabled: Click on the checkbox of the corresponding port No. to enable the Loop Detection function on the specific port(s).

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

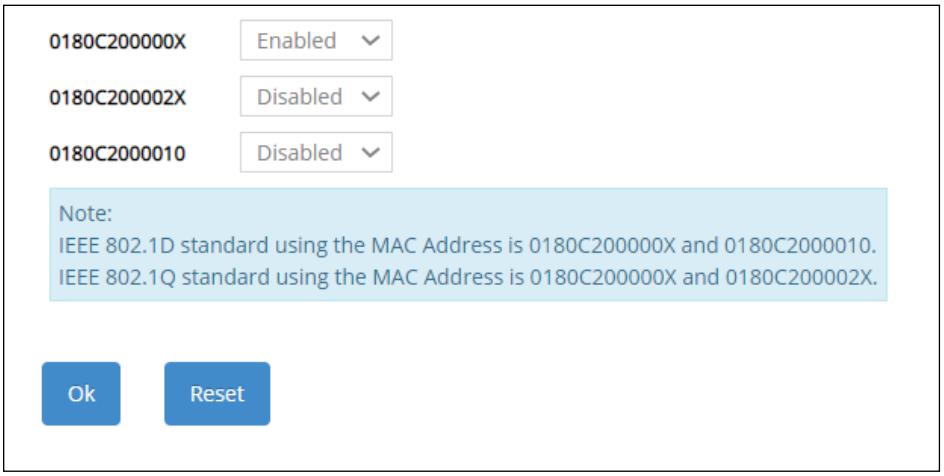
Status: View-only field that shows the loop status of each port.

Reason of being locked: View-only field that shows the cause why the port is locked.

Unlock: Press the **Unlock** button to unlock the specific port if this port is locked.

4.11.8 L2 Control Protocol Filter Setup

Select the option **L2 Control Protocol Filter Setup** from the **Security Setup** menu and then the following screen page appears.



Layer 2 Control Protocol:

0180C200000X: Select either “No Filter Out” or “Filter Out”. When “Filter Out” is selected, packets from the address ranging from 0180C2000000 to 0180C200000F will be dropped. Multicast MAC addresses from 0180C2000000 to 0180C200000F are reserved for use by 802.1/802.3 protocols. The purpose for each multicast address is described briefly below:

0180C200002X: Select either “No Filter Out” or “Filter Out”. When “Filter Out” is selected, packets from the address ranging from 0180C2000020 to 0180C200002F will be dropped. Multicast addresses from 0180C2000020 to 0180C2000022 are for GMRP, GVRP, and GARP respectively.

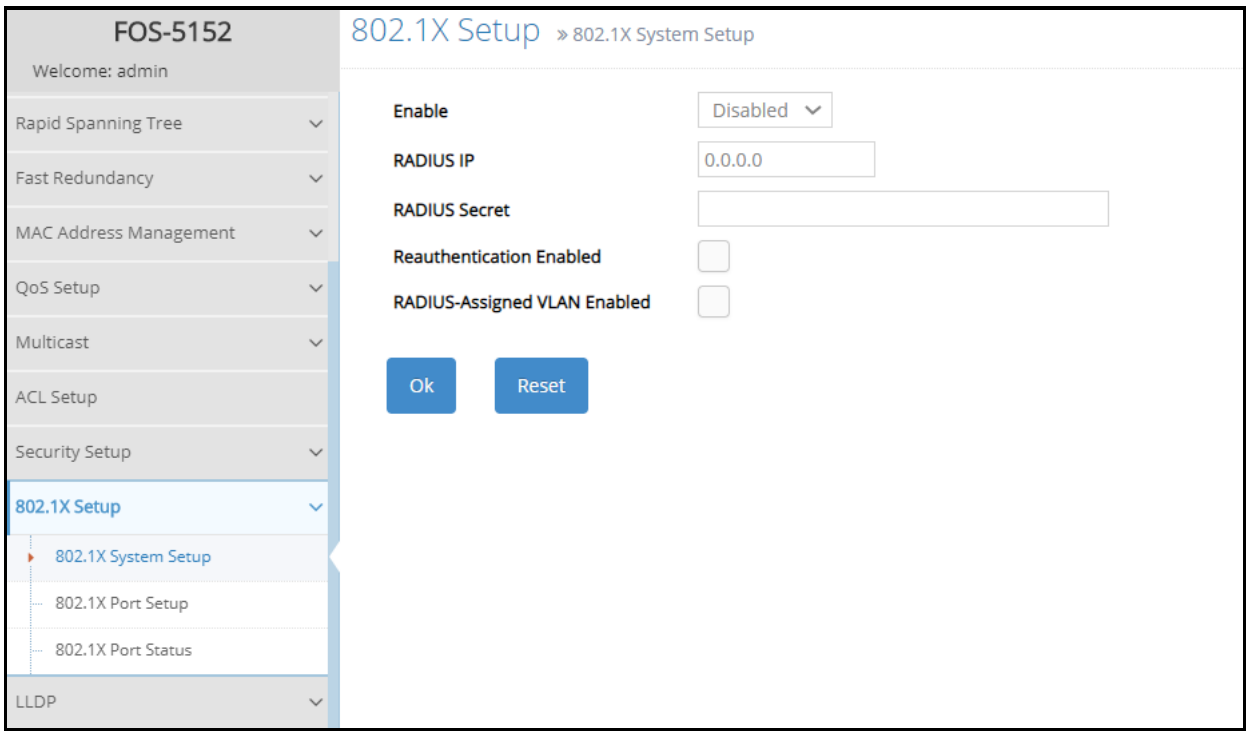
0180C2000010: Select either “No Filter Out” or “Filter Out”. When “Filter” is selected, packets from the address 0180C2000010 will be dropped.

4.12 802.1X Setup

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.

Click the folder **802.1X Setup** from the **Main Menu** and then 3 options within this folder will be displayed as follows.



1. **802.1X System Setup:** Set up system 802.1X/MAB RADIUS IP, RADIUS Secret, Reauthentication, and so on.

2. **802.1X Port Setup:** Set up port 802.1X/MAB configuration (includes the port authorization state, MAB, reAuth, reAuthPeriod, EAP Timeout, etc.) and the port reauthentication.

3. **802.1X Port Status:** View port status and statistics.

4.12.1 802.1X System Setup

The following screen page appears if you choose **802.1X System Setup** function.

Enable: Enable or disable IEEE 802.1X/MAB 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 the IPv4 address of RADIUS authentication server.

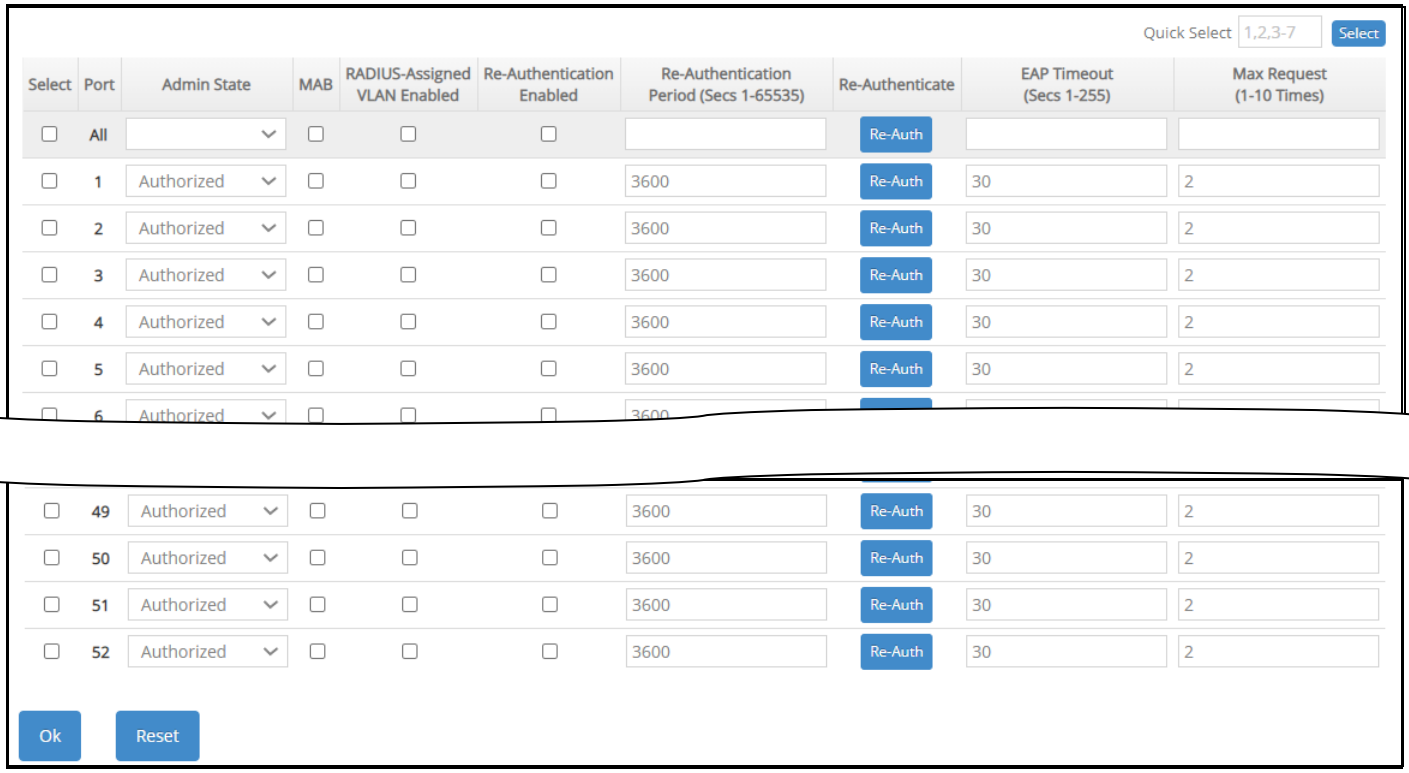
RADIUS Secret: The identification number assigned to each RADIUS authentication server with which the client shares a secret.

Reauthentication Enabled: Enable or disable Reauthentication.

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

4.12.2 802.1X Port Setup

The following screen page appears if you choose **802.1X Port Setup** function.



Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the 802.1X Port Setup table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

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.

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.

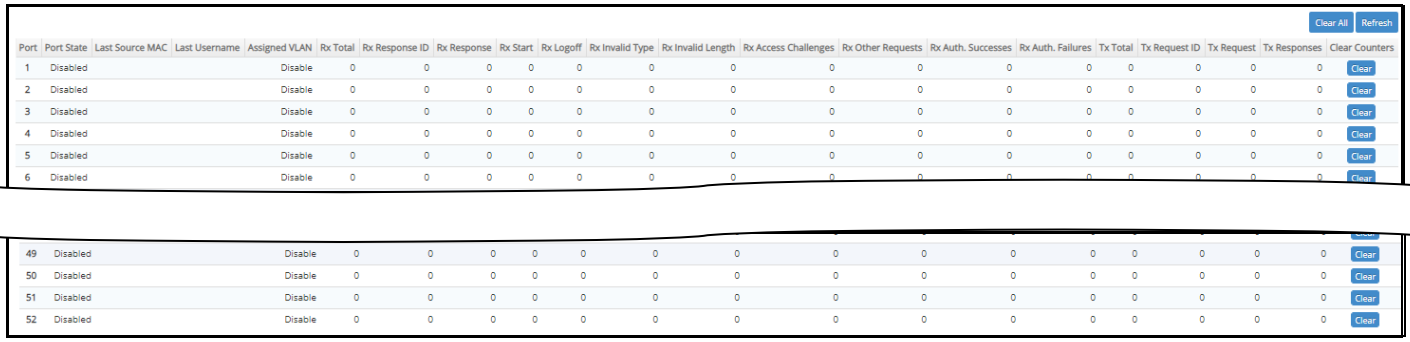
Re-Authenticate: By clicking on the **Re-Auth** button of the corresponding port number, the authentication message will be sent immediately to re-authenticate the speified port right now.

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: 30 seconds.

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.

4.12.3 802.1X Port Status

802.1X Port Status allows users to view a list of all 802.1x ports' information. The following screen page appears if you choose **802.1X Port Status** function. In this webpage, you can find the following information about 802.1X ports and view the real-time 802.1X port statistics of the Managed Switch.



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

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.

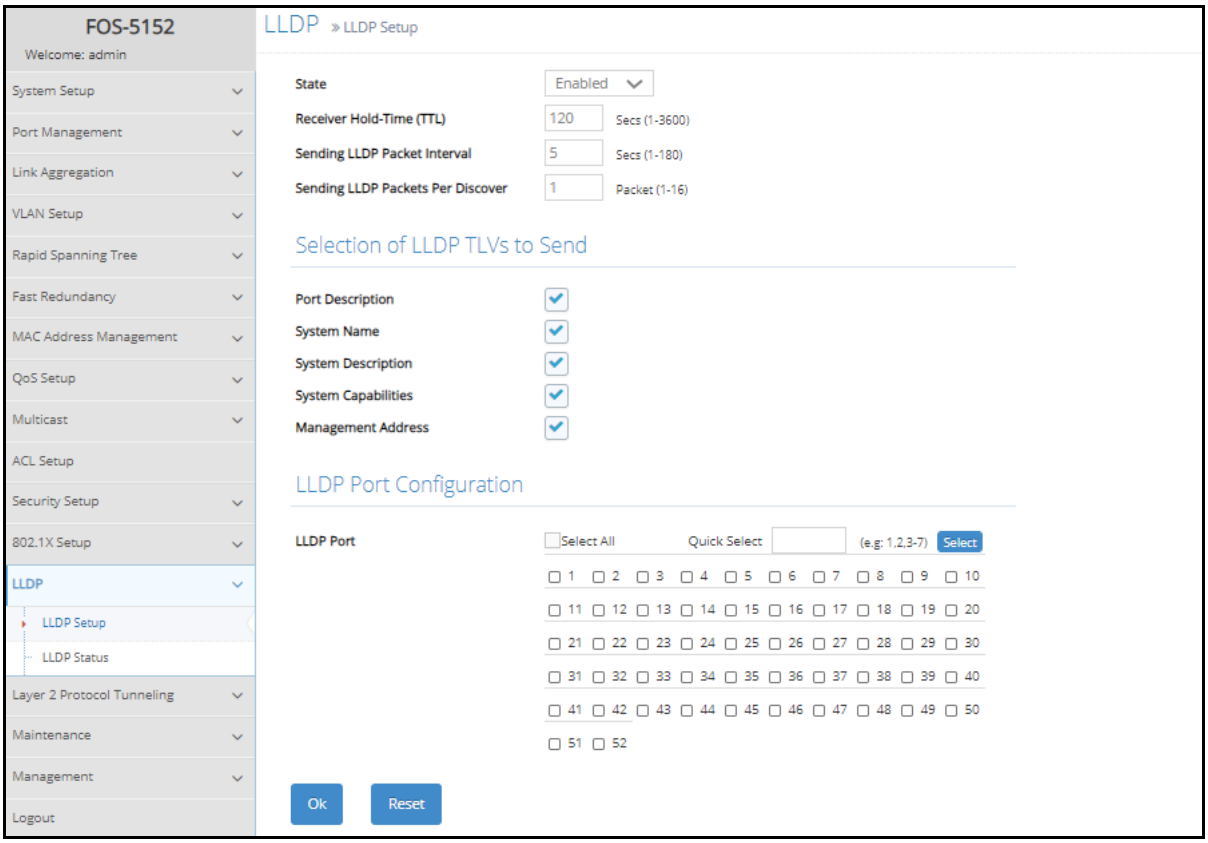
Assigned VLAN: Display the VLAN assigned by 802.1x Server.

Rx Auth. Successes/Failures: Display the counters of success or failure in authentication.

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 contain type, length and value descriptions, and are referred to as 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 folder **LLDP** from the **Main Menu** and then 2 options within this folder will be displayed as follows.

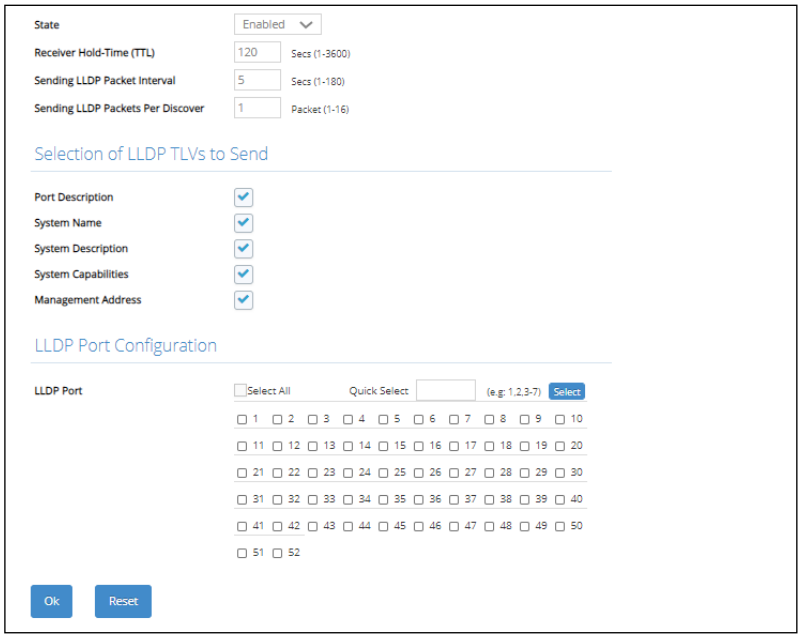


1. **LLDP Setup:** Enable or disable LLDP on ports and set up LLDP-related attributes.

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

4.13.1 LLDP Setup

Click the option **LLDP Setup** from the **LLDP** menu and then the following screen page appears.



State: Globally enable or disable LLDP function.

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 in seconds for updated LLDP packets to be sent.

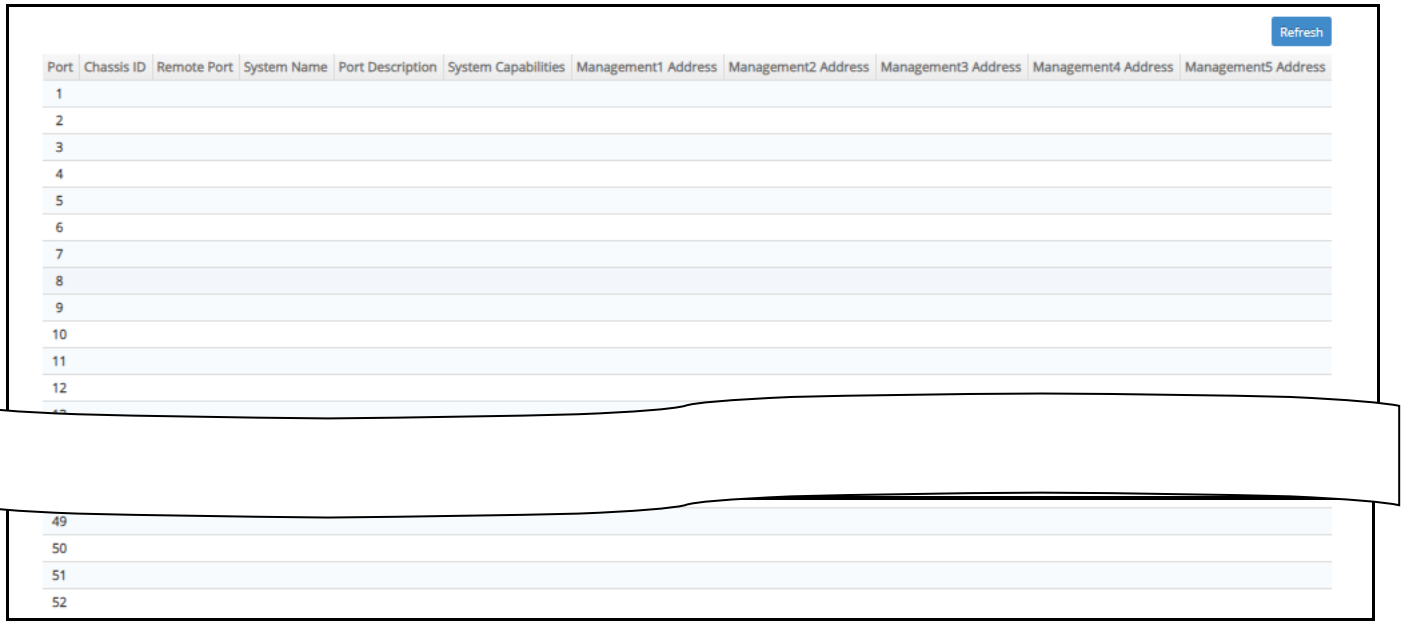
Sending LLDP Packets Per Discover: Enter the amount of packets sent in each discover.

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

LLDP Port: Click on the checkbox of corresponding port number to enable LLDP function on the specific port(s). Or directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field and then press the **Select** button, the specified port(s) will be checked immediately. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

4.13.2 LLDP Status

Click the option **LLDP Status** from the **LLDP** menu and then the following screen page appears.



Refresh: Click **Refresh** to update the LLDP Status table.

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

4.14 Layer 2 Protocol Tunneling Configuration

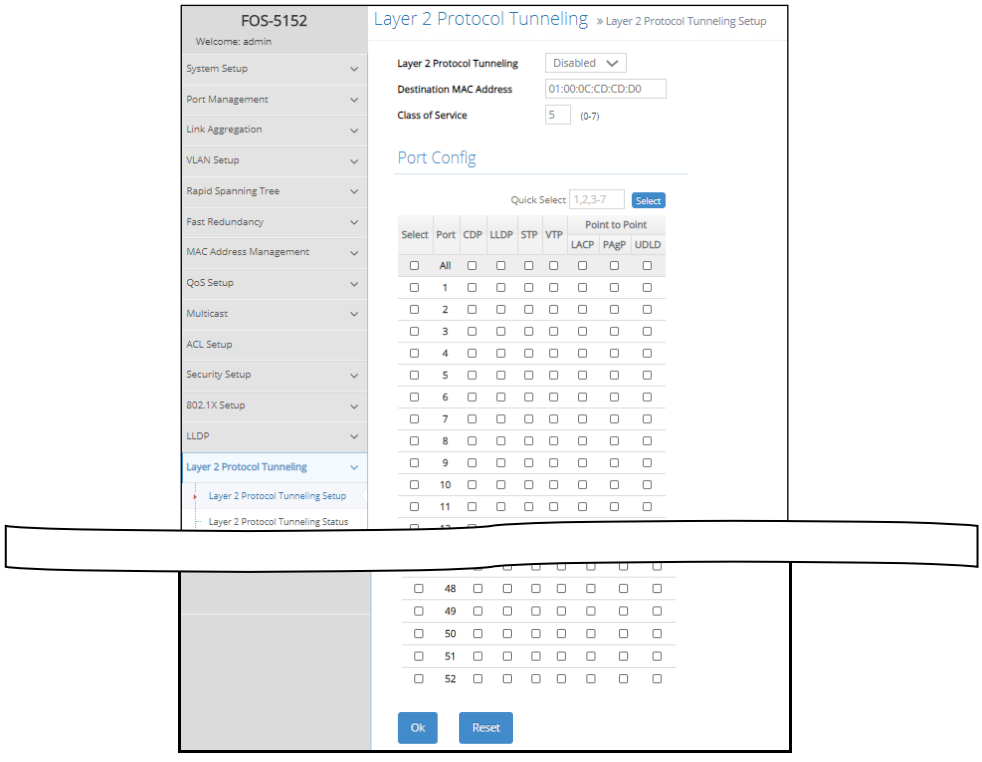
L2PT (Layer 2 Protocol Tunneling) allows Layer 2 protocol data units (PDUs), including CDP(Cisco Discovery Protocol), LLDP(Link Layer Discovery Protocol), STP(Spanning Tree Protocol), VTP(Vlan Trunking Protocol), LACP(Link Aggregation Control Protocol), PAgP(Port Aggregation Protocol), and UDLD(Unidirectional Link Detection), to be tunneled through a network.

Without L2PT, the handling of the PDUs will create different spanning tree domains (different spanning tree roots) for the customer switches. To provide a single spanning tree domain for the customer switches, a generic scheme to tunnel BPDUs was created for control protocol PDUs. This process is referred to as Generic Bridge PDU Tunneling (GBPT).

GBPT provides a scalable approach to PDU tunneling by software encapsulating the PDUs in the ingress edge switches and then multicasting them in hardware. All switches inside the service provider network treat these encapsulated frames as data packets and forward them to the other end. The egress edge switch listens for these special encapsulated frames and decapsulates them; they are then forwarded out of the tunnel.

The encapsulation involves the rewriting of the destination media access control (MAC) address in the PDU. An ingress edge switch rewrites the destination MAC address of the PDUs received on a Layer 2 tunnel port with the desired multicast address.

To set up L2PT, click the folder **Layer 2 Protocol Tunneling** from the **Main Menu** and then two options will be displayed for your selection

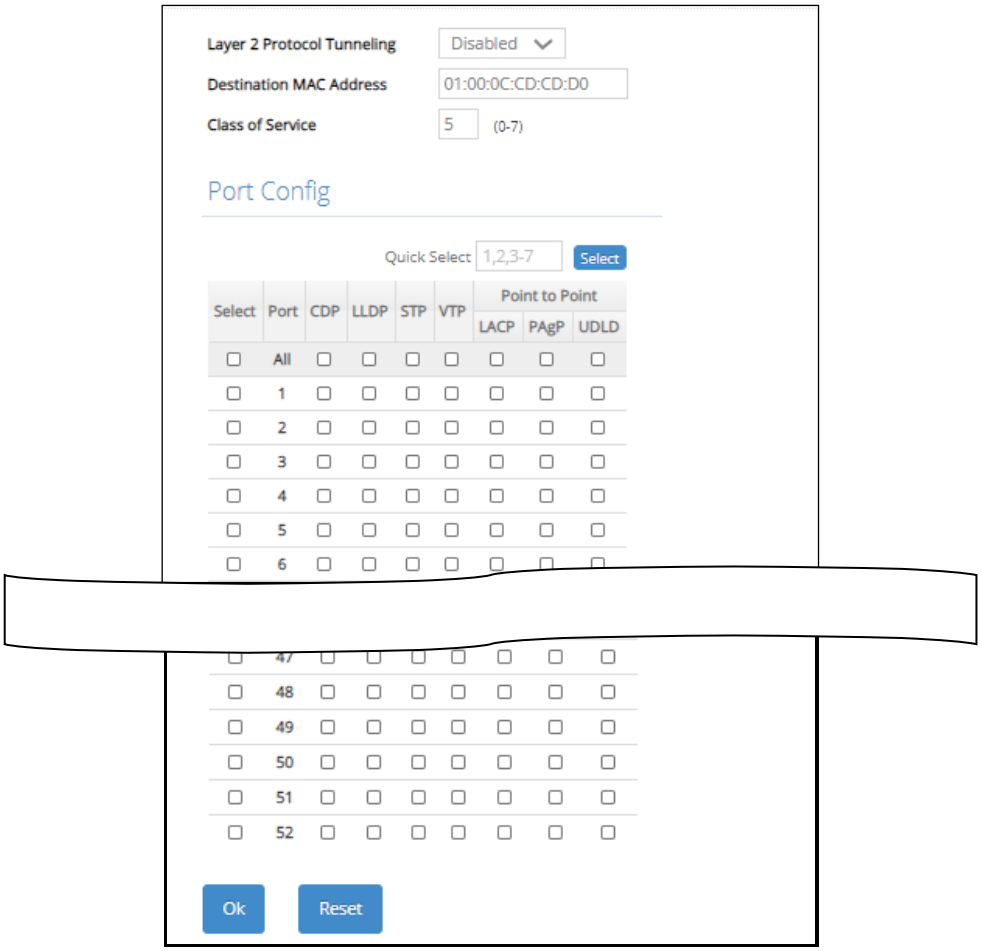


1. **Layer 2 Protocol Tunneling Setup:** Enable or disable L2PT function and set up acceptable BPDUs for GBPT (Generic Bridge PDU Tunneling).

2. **Layer 2 Protocol Tunneling Status:** View the state of Layer 2 protocol data units (PDUs) and their encapsulation, decapsulation and drop counters of each port.

4.14.1 Layer 2 Protocol Tunneling Setup

Select the option **Layer 2 Protocol Tunneling Setup** from the **Layer 2 Protocol Tunneling** menu and then the following screen page appears.



Layer 2 Protocol Tunneling: Enable or disable the Layer 2 Protocol Tunneling fuction globally.

Destination MAC Address: Specify a MAC address for GBPT. User- defined. Default is 01:00:0C:CD:CD:D0.

Class of Service: There are eight priority levels (0~7) that you can choose to classify data packets. Specify the preferred priority bit value as L2PT class of service (cos). The default value is “5”.

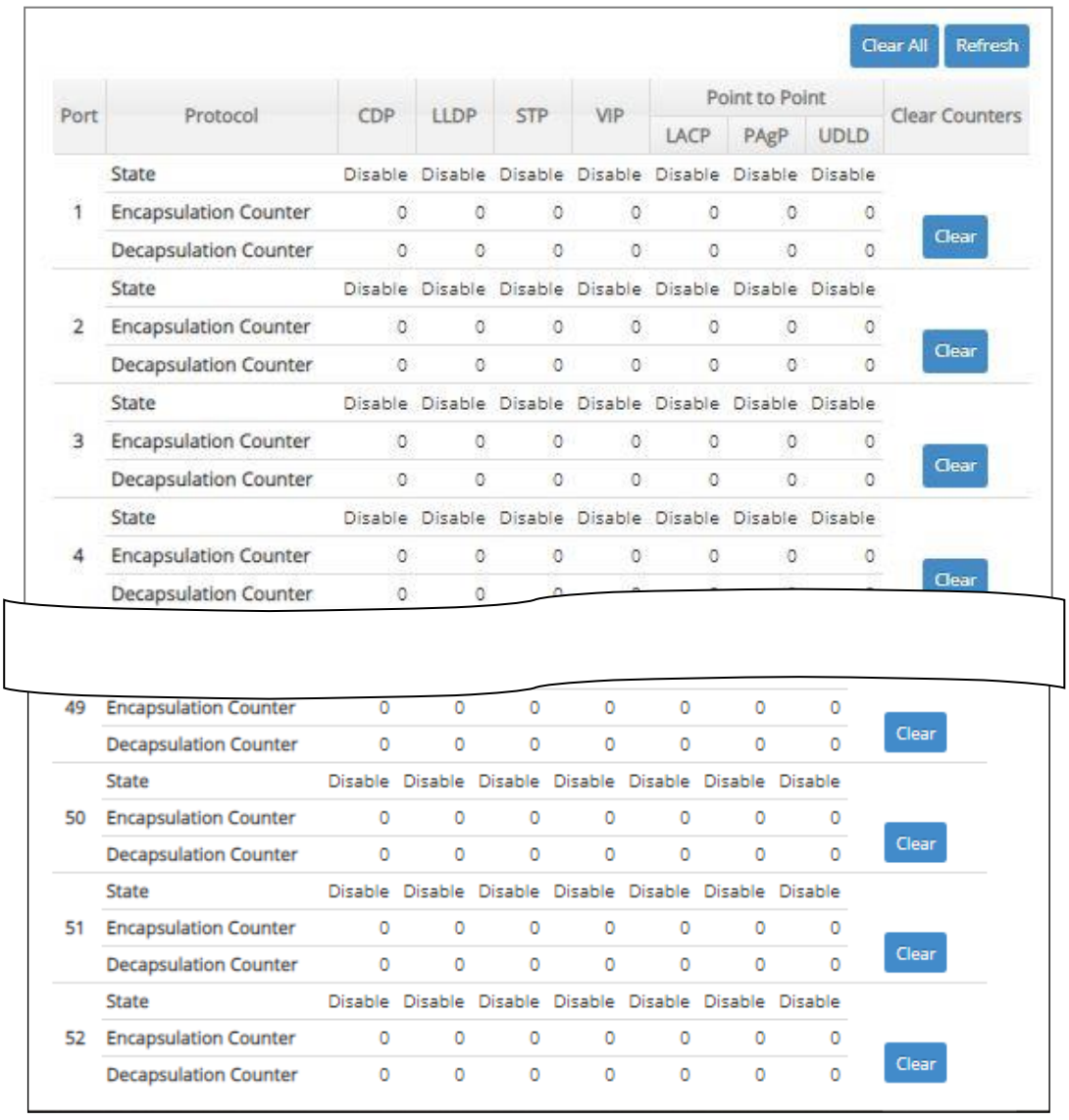
Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the Layer 2 Protocol Tunneling Setup table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Port: The number of each port.

CDP, LLDP, STP, VTP, LACP, PAgP, UDLD: Configure the Layer 2 port as a Layer 2 protocol tunnel port by clicking on the corresponding PDUs’ checkbox for the preferred port.

4.14.2 Layer 2 Protocol Tunneling Status

Layer 2 Protocol Tunneling Status displays the state of each Layer 2 protocol data units (PDUs) and the statistics of each PDU's encapsulation as well as decapsulation. Select **Layer 2 Protocol Tunneling Status** option from the **Layer 2 Protocol Tunneling** menu and then the following screen page appears.



Port	Protocol	CDP	LLDP	STP	VIP	Point to Point			Clear Counters
						LACP	PAgP	UDLD	
	State	Disable	Disable	Disable	Disable	Disable	Disable	Disable	
1	Encapsulation Counter	0	0	0	0	0	0	0	Clear
	Decapsulation Counter	0	0	0	0	0	0	0	
	State	Disable	Disable	Disable	Disable	Disable	Disable	Disable	
2	Encapsulation Counter	0	0	0	0	0	0	0	Clear
	Decapsulation Counter	0	0	0	0	0	0	0	
	State	Disable	Disable	Disable	Disable	Disable	Disable	Disable	
3	Encapsulation Counter	0	0	0	0	0	0	0	Clear
	Decapsulation Counter	0	0	0	0	0	0	0	
	State	Disable	Disable	Disable	Disable	Disable	Disable	Disable	
4	Encapsulation Counter	0	0	0	0	0	0	0	Clear
	Decapsulation Counter	0	0						
49	Encapsulation Counter	0	0	0	0	0	0	0	Clear
	Decapsulation Counter	0	0	0	0	0	0	0	
	State	Disable	Disable	Disable	Disable	Disable	Disable	Disable	
50	Encapsulation Counter	0	0	0	0	0	0	0	Clear
	Decapsulation Counter	0	0	0	0	0	0	0	
	State	Disable	Disable	Disable	Disable	Disable	Disable	Disable	
51	Encapsulation Counter	0	0	0	0	0	0	0	Clear
	Decapsulation Counter	0	0	0	0	0	0	0	
	State	Disable	Disable	Disable	Disable	Disable	Disable	Disable	
52	Encapsulation Counter	0	0	0	0	0	0	0	Clear
	Decapsulation Counter	0	0	0	0	0	0	0	

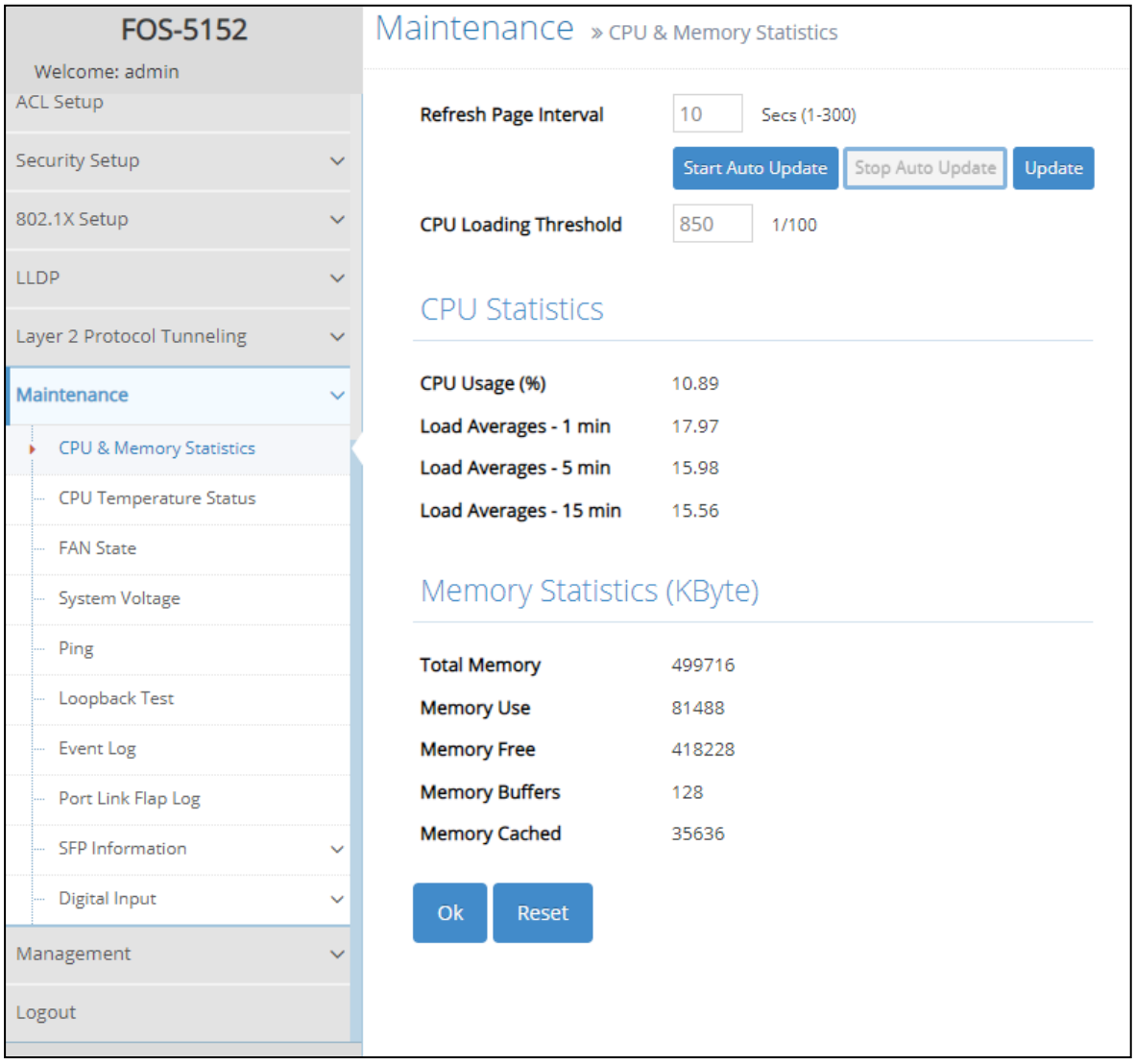
Clear All: Clear all ports' encapsulation, decapsulation and drop statistics of each PDU.

Refresh: Click **Refresh** to update the Layer 2 Protocol Tunneling Status table.

Clear button in **Clear Counters** field: Clear the encapsulation, decapsulation and drop statistics of each PDU for the corresponding port.

4.15 Maintenance

Maintenance allows users to monitor the real-time operation status of the Managed Switch for maintenance or diagnostic purposes and easily operate and maintain the system. Select the folder **Maintenance** from the **Main Menu** and then 9 options within this folder will be displayed for your selection.



1. **CPU & Memory Statistics:** Manually or automatically update statistics of CPU & Memory and view them.

2. **CPU Temperature Status:** Manually or automatically update the current CPU temperature as well as the CPU temperature record, and configure the cpu-temperature alarm notification.

3. **FAN State:** Manually or automatically update the current fan speed and status of FAN 1~3.

4. **System Voltage:** Manually or automatically update the current voltage and status of Managed Switch's internal powers.

5. **Ping:** Ping can help you test the network connectivity between the Managed Switch and the host. You can also specify the counts and size of Ping packets.

6. **Loopback Test:** Loopback Test helps you diagnose the connectivity of the networking cable between the devices.

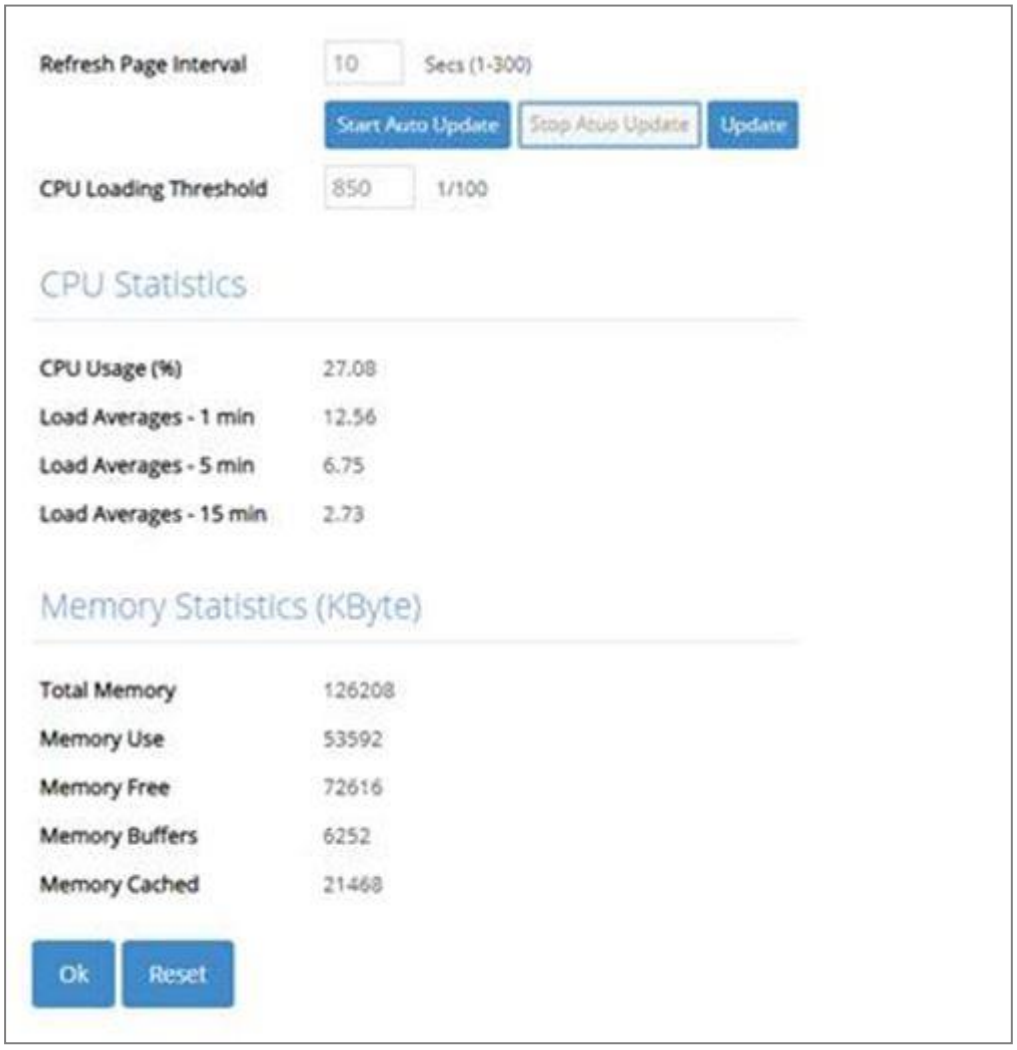
7. **Event Log:** Event log can keep a record of system's log events such as system warm start, cold start, link up/down, user login/logout, etc. They will be kept only when your CPU version is A06 with Boot ROM version A08 or later version. If your CPU or Boot ROM version is older than the one mentioned above, all events will lose when the system is shut down or rebooted.

8. **SFP Information:** View the current port's SFP information, e.g. speed, Vendor ID, Vendor S/N, etc.. SFP port state shows current DMI (Diagnostic monitoring interface) temperature, voltage, TX Bias, etc..

9. **Digital Input:** Set up the normal status of the digital input.

4.15.1 CPU and Memory Statistics

CPU & Memory Statistics is to manually or automatically update statistics of CPU and Memory. Select the option **CPU & Memory Statistics** from the **Maintenance** menu and then the following screen page appears.



Refresh Page Interval: Automatically updates statistics of CPU & Memory 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.

Update: Click **Update** to refresh the latest statistics of CPU & Memory at a time.

CPU Loading Threshold: Specify CPU loading threshold. Valid range: 10-3000 (Unit: 1/100)

CPU Usage (%): The percentage of current CPU usage of the system.

Load Averages – 1 min: The average active tasks percentage in last 1 minute.

Load Averages – 5 min: The average active tasks percentage in last 5 minutes.

Load Averages – 15 min: The average active tasks percentage in last 15 minutes.

Total Memory: It shows the entire memory in kilobytes.

Memory Use: The memory in kilobytes that is in use.

Memory Free: The memory in kilobytes that is idle.

Memory Buffers: The memory in kilobytes temporarily stored in a buffer area. Buffer allows the computer to be able to focus on other matters after it writes up the data in the buffer; as oppose to constantly focus on the data until the device is done.

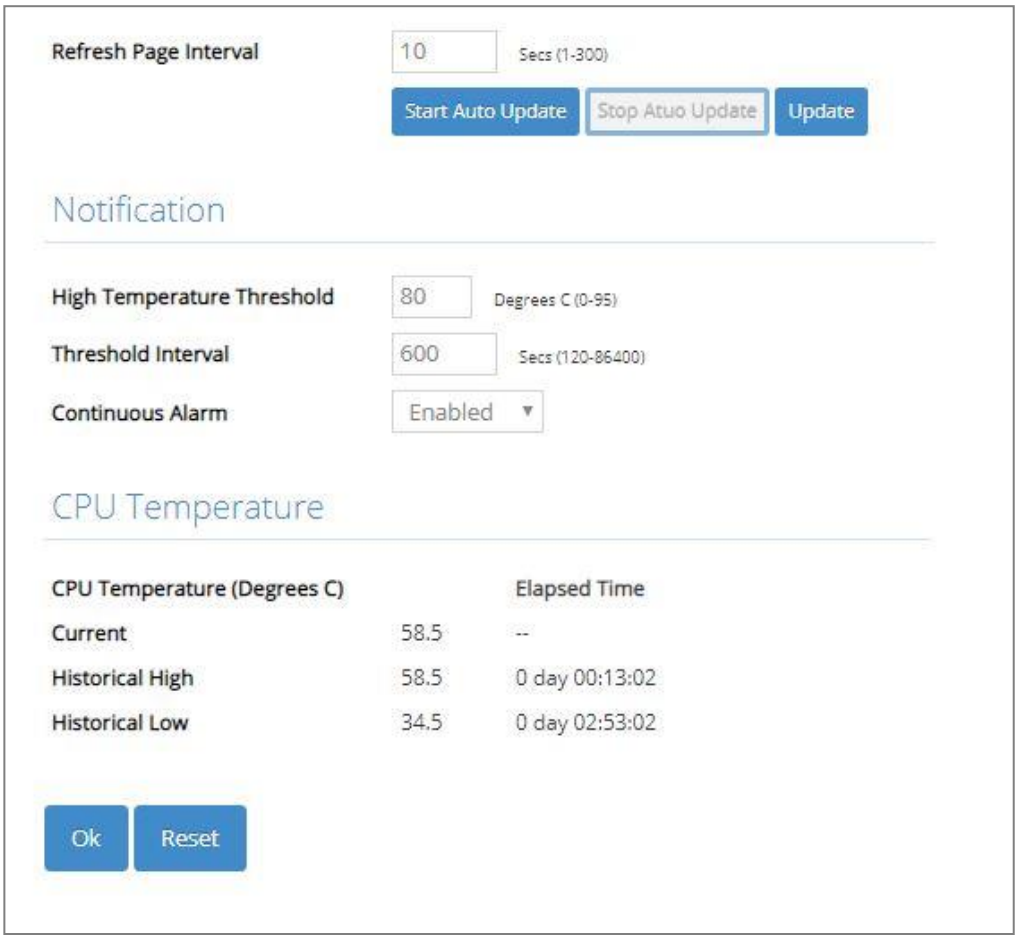
Memory Cached: The memory in kilobytes stored in a cache area that is where the data can be accessed faster in the future. The data can be retrieved more quickly from the cache than from its source origin.

4.15.2 CPU Temperature Status

With the built-in temperature sensor, the Managed Switch is capable of detecting whether CPU temperature is at normal status or not. In addition, by the the notification via trap, syslog and event log, the user can realize the real-time CPU temperature to prevent the device’s lifespan from being shorten due to the abnormal operation environment.

The alarm message will be sent in the event of abnormal situations, including CPU temperature is over the temperature threshold, CPU temperature exceeds the range of threshold (from 0 to 95 degrees centigrade), or the temperature sensor fails to detect CPU temperature. A normal message will also be sent to notify the user when CPU temperature higher the threshold returns to the normal status.

Select the option **CPU Temperature Status** from the **Maintenance** menu and then the following screen page appears.



Refresh Page Interval: Automatically updates CPU temperature of the system 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.

Update: Click **Update** to refresh the latest CPU temperature at a time.

High Temperature Threshold: Specify CPU temperature threshold. Valid range: 0~95 degrees centigrade.

If the detected CPU temperature is over the threshold you configure, the alarm message ”CPU temperature is over threshold” will be sent based on the configuration in the folloiwng **Threshold Interval** and **Continuous Alarm** parameters.

NOTE: *Any new changes done on this parameter will be taken effect immediately during the system execution, the temperature sensor will begin to check CPU temperature and decide whether to send the alarm/normal message or not upon the last status. Refer to Table 4-1.*

Last Status / Detected Status	Normal	Over the Threshold
Normal	No message will be sent.	Send the “CPU temperature is at or under threshold” normal message.
Over the Threshold	Send the “CPU temperature is over threshold” alarm message.	No message will be sent.

Table 4-1

Threshold Interval: Specify the time interval of sending cpu-temperature alarm message in seconds.

NOTE: *Any new changes done on this parameter will be taken effect immediately during the system execution, the temperature sensor will begin to check CPU temperature and decide whether to send the alarm/normal message or not upon the last status. Refer to Table 4-2.*

Last Status / Detected Status	Normal	Over the Threshold
Normal	No message will be sent.	Send the “CPU temperature is at or under threshold” normal message.
Over the Threshold	Send the “CPU temperature is over threshold” alarm message.	Send the “CPU temperature is over threshold” alarm message.

Table 4-2

Continuous Alarm: Enable or disable the continuous alarm message sending function for CPU temperature of the system. Default is “Enabled”.

In case this function is enabled, the alarm message will be sent continuously upon the time interval configured in **Threshold Interval** parameter to notify the user once CPU temperature is at the abnormal status.

In case this function is disabled, the alarm message will be sent only one time to notify the user once CPU temperature is at the abnormal status.

Click **OK**, the new configuration will be taken effect immediately.

Current: Display CPU temperature currently detected by the temperature sensor. It will be shown

in red color if the current CPU temperature is higher than the value you configured in the **High Temperature Threshold** parameter, or show “Failed” in red color if the temperature sensor fails.

Historical High: Display the highest record of CPU temperature that had ever been reached since this system boot-up. It will show “Failed” in red color if the temperature sensor fails.

Historical Low: Display the lowest record of CPU temperature that had ever been reached since this system boot-up. It will show “Failed” in red color if the temperature sensor fails.

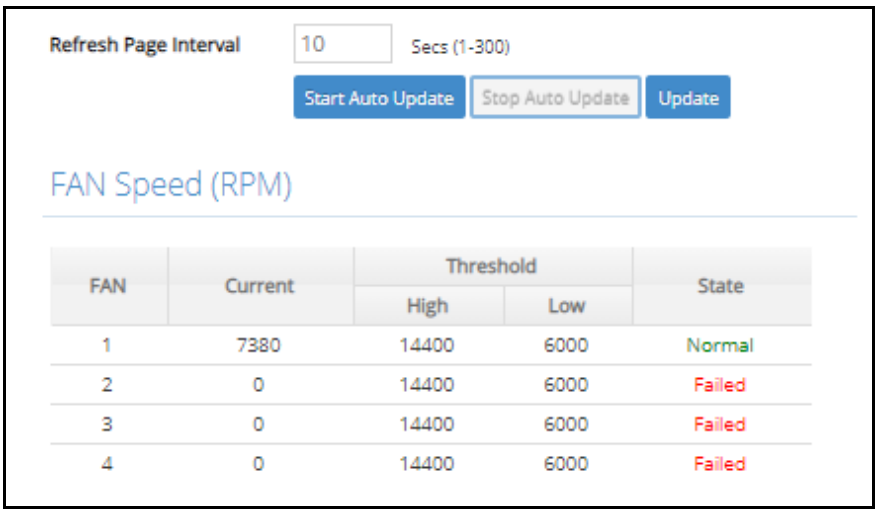
Elapsed Time of Historical High: The period of time passed by since the highest CPU temperature has been reached.

Elapsed Time of Historical Low: The period of time passed by since the lowest CPU temperature has been reached.

4.15.3 FAN State

FAN State is to manually or automatically update 3 fans’ (FAN1, FAN2 and FAN3 that are located on the rear panel of Managed Switch) speed and status for the system diagnostics. With the built-in fan sensor of the Managed Switch, the user can diagnose device’s heat dissipation is good or not by monitoring the real-time speed of these 3 fans.

Select the option **FAN State** from the **Maintenance** menu and then the following screen page appears.



Refresh Page Interval: Automatically updates statistics and state of 3 fans’ speed 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.

Update: Click **Update** to refresh the latest statistics and state of 3 fans’ speed at a time.

Current: Display each fan's speed currently detected by the fan sensor.

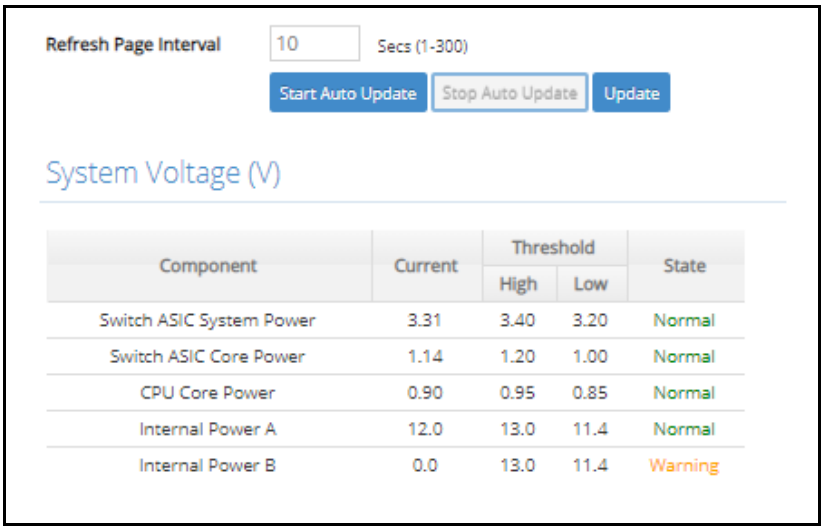
Threshold (Low): View-only field that shows the lowest speed value (5040 RPM) of each Managed Switch's fan.

State: It will show "Failed" in red color when the current fan speed is zero, "Warning" in orange color when the fan speed is at or under the low threshold (**≦** 5040 RPM), or "Normal" in green color when the fan speed is higher than the low threshold (**>**5040 RPM).

4.15.4 System Voltage

System Voltage, also offered for the system diagnostics, is to let the user know that whether the system is in healthy status or not through the diagnosis of system's internal powers such as ASIC system power, ASIC core power and Power A & B (Power B is only available in models with two fixed power modules).

Like the aforementioned **FAN State** function, the user can manually or automatically update the voltages as well as status of the above powers and realize their real-time information with the voltage sensor built in Managed Switch. Select the option **Systsem Voltage** from the **Maintenance** menu and then the following screen page appears.



Refresh Page Interval: Automatically updates statistics and state of Managed Switch's ASIC system power, ASIC core power, CPU core power and Power A & B 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.

Update: Click **Update** to refresh the latest statistics and state of Managed Switch's ASIC system power, ASIC core power and Power A & B at a time.

Current: Display the voltage currently detected by the voltage sensor for the ASIC system power, ASIC core power and Power A & B of Managed Switch.

Threshold (High): View-only field that shows the highest voltage value of ASIC system power (3.40 V), ASIC core power (1.20 V), and Power A & B (13.0 V).

Threshold (Low): View-only field that shows the lowest voltage value of ASIC system power (3.20 V), ASIC core power (1.00 V), and Power A & B (11.40 V).

State:

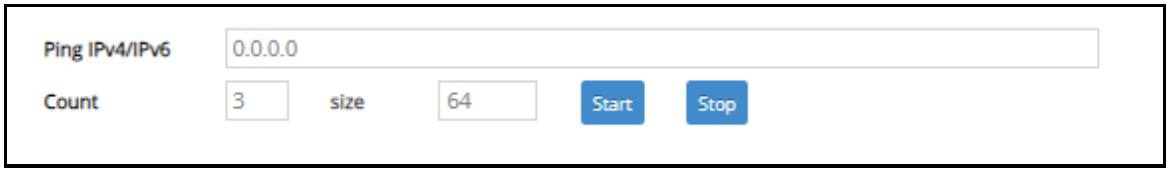
In ASIC system power, "Warning" will be shown in orange color if its voltage is at or over the High threshold **(≥ 3.40 V)** or is at or under the Low threshold **(≤ 3.20 V)**. Or it will show "Normal" in green color if its voltage is higher than the Low threshold and lower than the High threshold (**3.20 V < X < 3.40 V)**.

In ASIC core power,"Warning" will be shown in orange color if its voltage is at or over the High threshold **(≥ 1.20 V)** or is at or under the Low threshold **(≤ 1.00 V)**. Or it will show "Normal" shown in green color if its voltage is higher than the Low threshold and lower than the High threshold **(1.00 V < X < 1.20 V**).

In Power A/B, "Warning" will be shown in orange color if its voltage is at or over the High threshold **(≥ 13.0 V)** or is at or under the Low threshold **(≤ 11.40 V)**. Or it will show "Normal" shown in green color if its voltage is higher than the Low threshold and lower than the High threshold **(11.40 V < X < 13.0 V**).

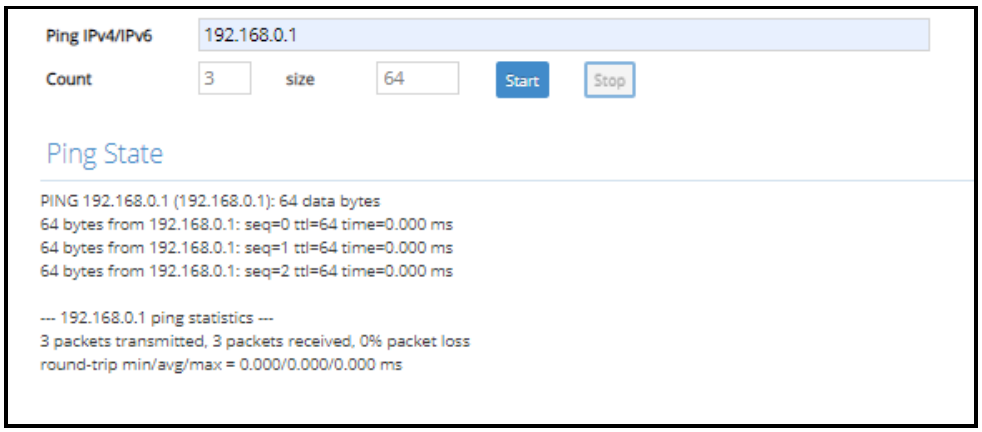
4.15.5 Ping

Ping can help you test the network connectivity between the Managed Switch and the host. Select the option **Ping** from the **Maintenance** menu and then the following screen page appears.



Enter the IPv4/IPv6 address of the host you would like to ping. You can also specify the count and size of the Ping packets. Click **Start** to start the Ping process or **Stop** to pause this Ping process.

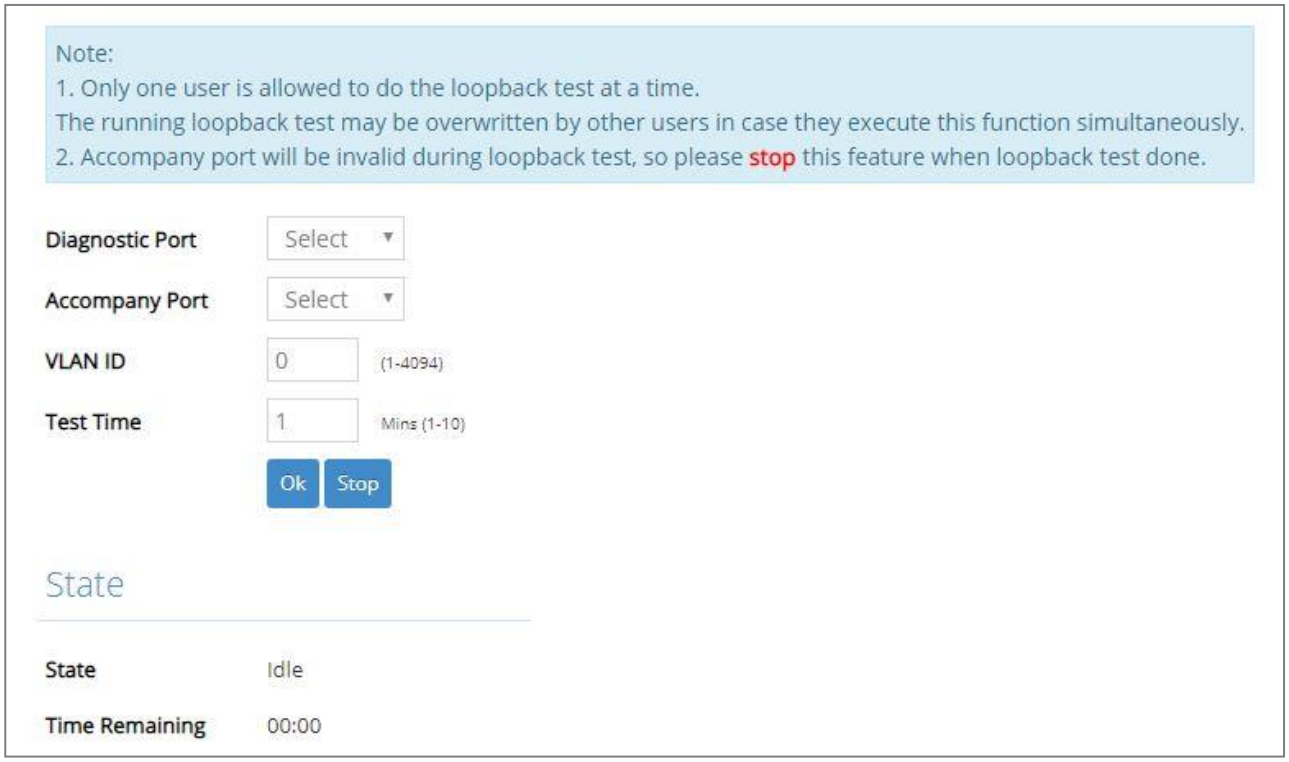
For example,
In the setting of Ping IPv4 IP address "192.168.0.1" with Count number "3" and packet size "64 Bytes", you can get the result of Ping State in the following graph, including ping packet state and statistic.



4.15.6 Loopback Test

Loopback Test is a passive test in which the packets need to be proactively sent from a communication device to the other end supporting the loopback test function as well, and returns the packets throught the same port to this device as a way to detect whether the connectivity of the networking cable between these devices works normally or not. With this built-in test function, it will shorten the troubleshooting time if any damage or the short circuit occurs.

Select the option **Loopback Test** from the **Maintenance** menu and then the following screen page appears.To have this function activated, you should respectively select the diagnostic port and accompany port, and fill in the proper VLAN ID. The test will be proceeded as configured when you click **OK**, and will be ended until the given test time expires. To pause this test, please click **STOP** on this webpage.



Diagnostic Port: Pull down the menu to select the desired port number as the diagnostic port for the loopback test. The diagnostic port you select should be configured as the VLAN TRUNK mode.

Accompany Port: Pull down the menu to select the desired port number as the accompany port for the loopback test. The accompany port should be in the link-down status.

NOTE: The port you select as the diagnostic port in the loopback test cannot be the same as the accompany port.

VLAN ID: Specify the VLAN ID. Except the diagnostic port and the accompany port, this specified VLAN ID cannot be used by other ports.

Test Time: Specify the time that the loopback test will last. Valid range: 1~10 miniutes. Default: 1 miniute.

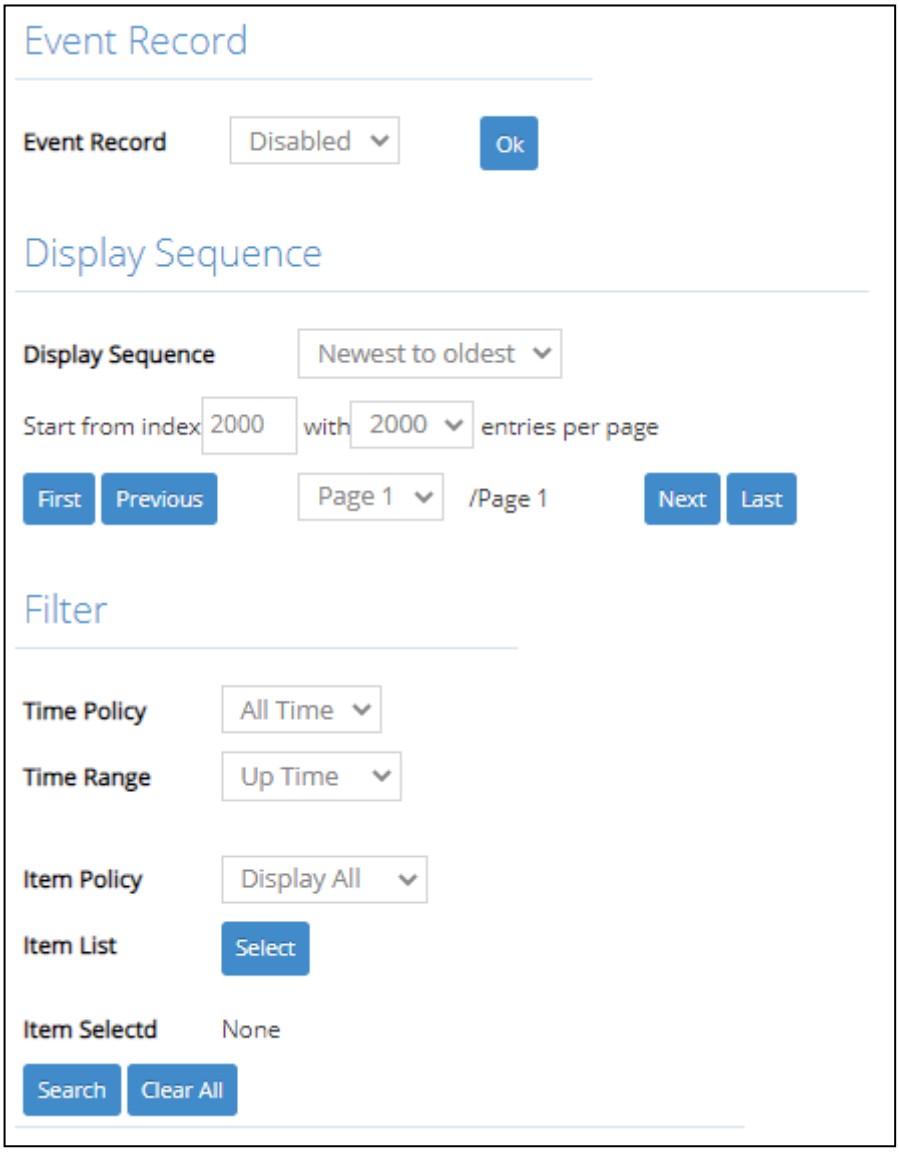
State: Show the current status of the loopback test. Either “idle” or “active” will be displayed.

Time Remaining: Show the the time (in the format of “mm:ss”) left that the loopback test will expire. By clicking **OK** on the webpage, the loopback test will start the countdown based on the value you configure in the paramerter of Test Time.

4.15.7 Event Log

Event log keeps a record of switch-related information. A network manager can investigate the information captured in the Event Log and therefore analyze the network traffic, usage, and security.

Select the option **Event Log** from the **Maintenance** menu and then the following screen page appears.



Event Record: Configure the Event Record function. Once it’s **enabled**, the Managed Switch will fully preserve the entire event log after reboot, while the Managed Switch will erase the entire event log if Event Record is **disabled**. Click **OK** when you have finished the configuration.

Display Sequence: Configure the display sequence of the event log table.

1. Select **Newest to oldest** or **Oldest to newest** to specify the arrangement of the event log display.

2. Set **Start from index** as a particular event index. Any event of which the index is smaller than the specified index will not be displayed if you specify the arrangement of **Oldest to newest**; any event of which the index is bigger than the specified index will not be displayed if you specify the arrangement of **Newest to oldest.**

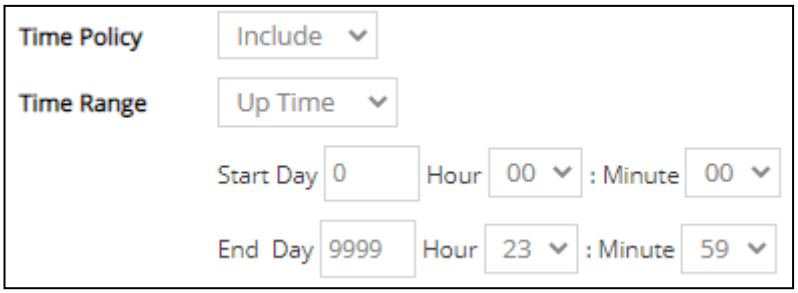
3. Click the pull-down menu of **entries per page** to select the maximum number of event entries displayed on each page.

Click **First**, **Last** or select the intended page from the pull-down menu of **Page** to achieve page jumps; click **Previous** or **Next** to maneuver the display of the event log table.

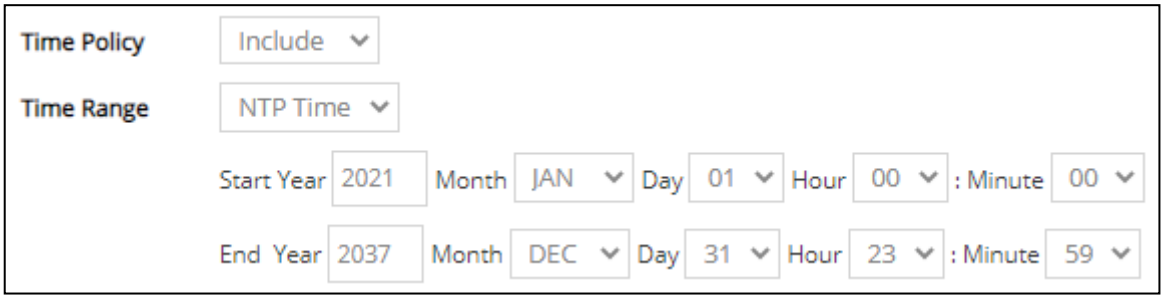
Filter: Configure each filter setting to customize the display of the event log table.

1. **Time Policy:** Select **All Time**, **Exclude**, or **Include** to determine the filtering behavior.

2. **Time Range:** Select **Up Time** or **NTP Time** to filter the events according to the Managed Switch's uptime or NTP time.

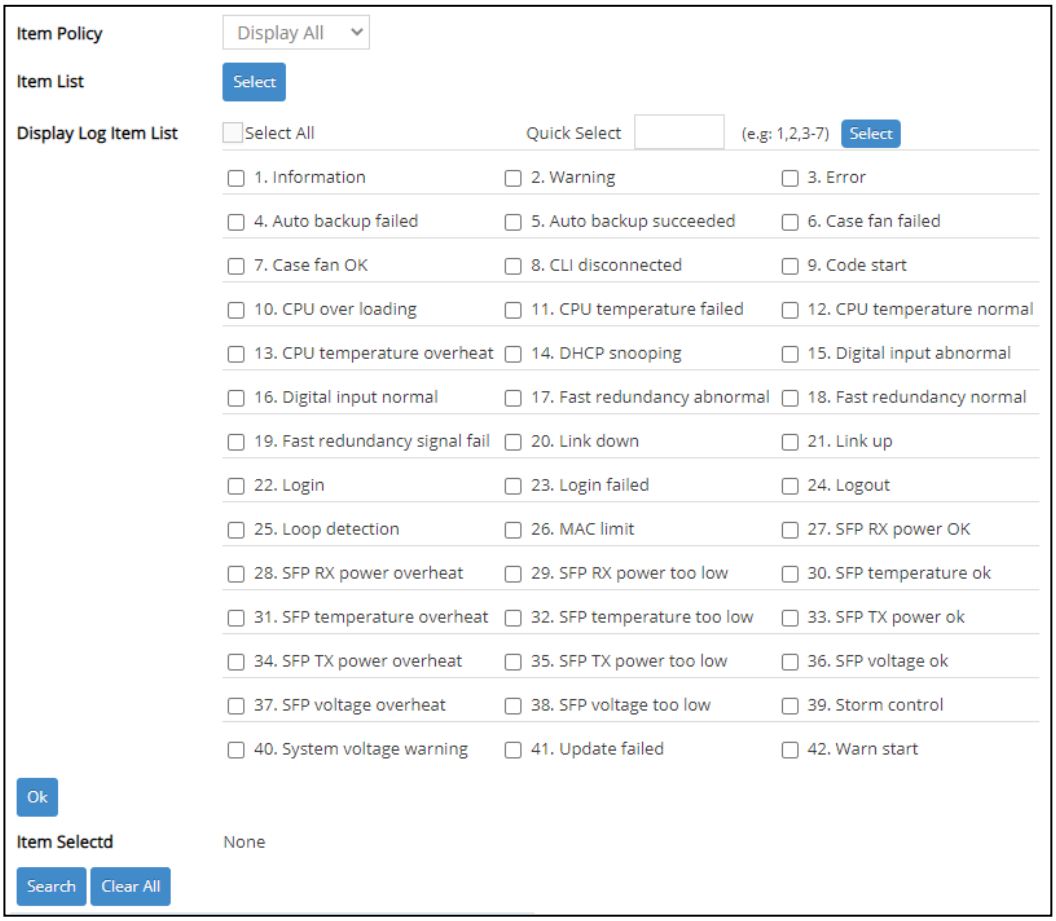


Start/End Day Hour Minute: When **Time Policy** is selected as **Exclude** or **Include**, specify the time period in which the intended events occurred according to the Managed Switch's uptime.



Start/End Year Month Day Hour Minute: When **Time Policy** is selected as **Exclude** or **Include**, specify the time period in which intended events occurred according to NTP time.

3. **Item Policy:** Select **Display All**, **Exclude Log**, or **Include Log** to determine the behavior of the event category filtering.

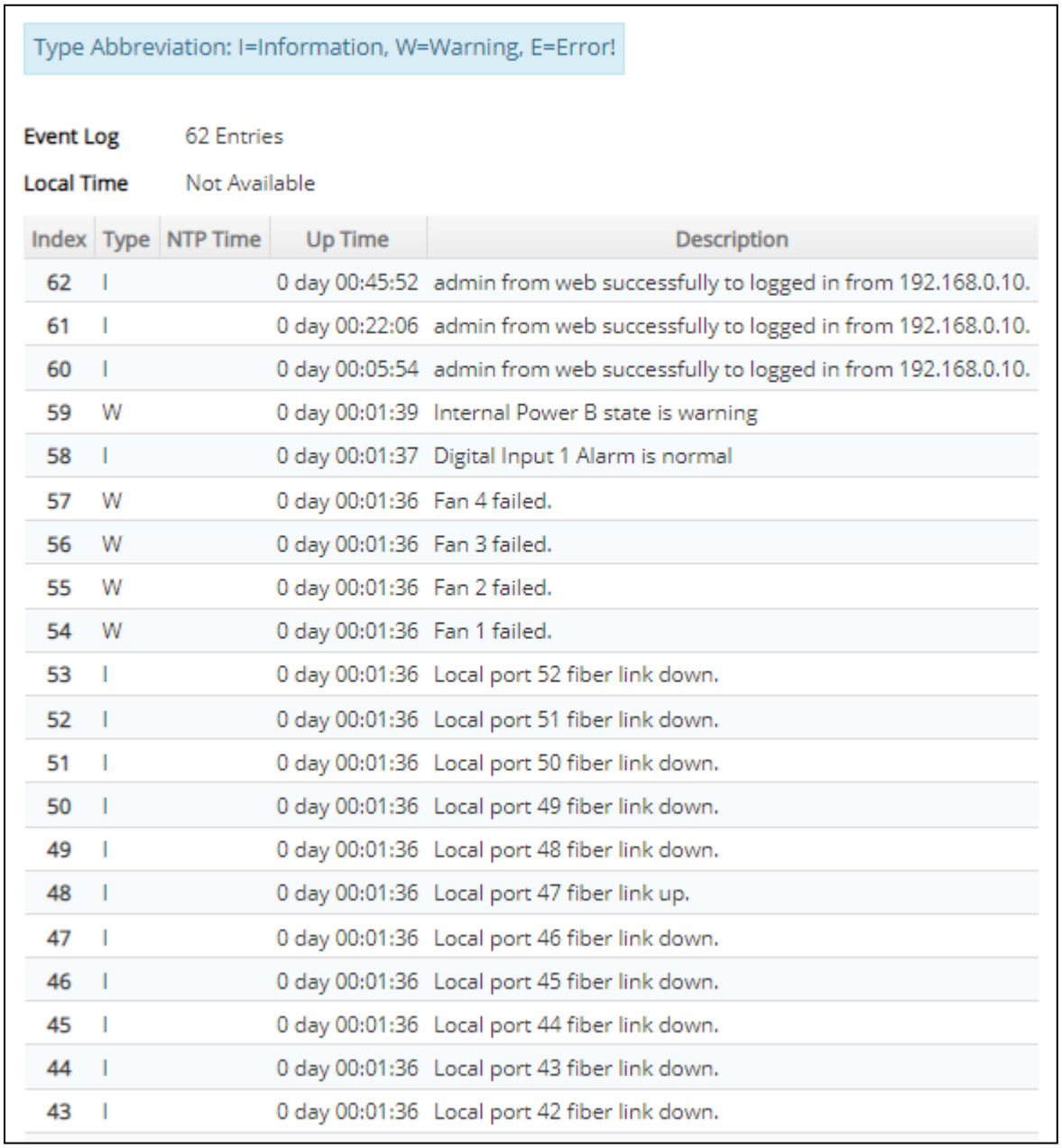


4. **Item List:** Click **Select** to specify certain/all event categories from the collapsible section to enable event filtering.

5. **Display Log Item List**: Click each checkbox of one particular event category to select the intended event categories. Or quickly configure the desired event categories at a time by directly inputting the item number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the **Display Log Item List** table. The specified event categories will be checked immediately once you click the **Select** button next to the **Quick Select** field. Click **Ok** to finish the selection.

6. **Item Selected:** Display the event category you select from the **Item List**; display “none“ when no event category is selected.

Click **Search** to update the event log table sitting at the bottom of the webpage when you are done configuring the filtering settings; Click **Clear All** to clear the record of all event logs.



1. **Event Log:** Display the total number of event entries displayed according to the specified filtering settings.

2. **Local Time:** Display the current local time according to the specified local time zone on the Managed Switch.

3. **Index:** The index number of the event entry.

4. **Type:** The type of the event. “I” is the abbreviation of “Information”, “W” is the abbreviation of “Warning”, and “E” is the abbreviation of “Error”.

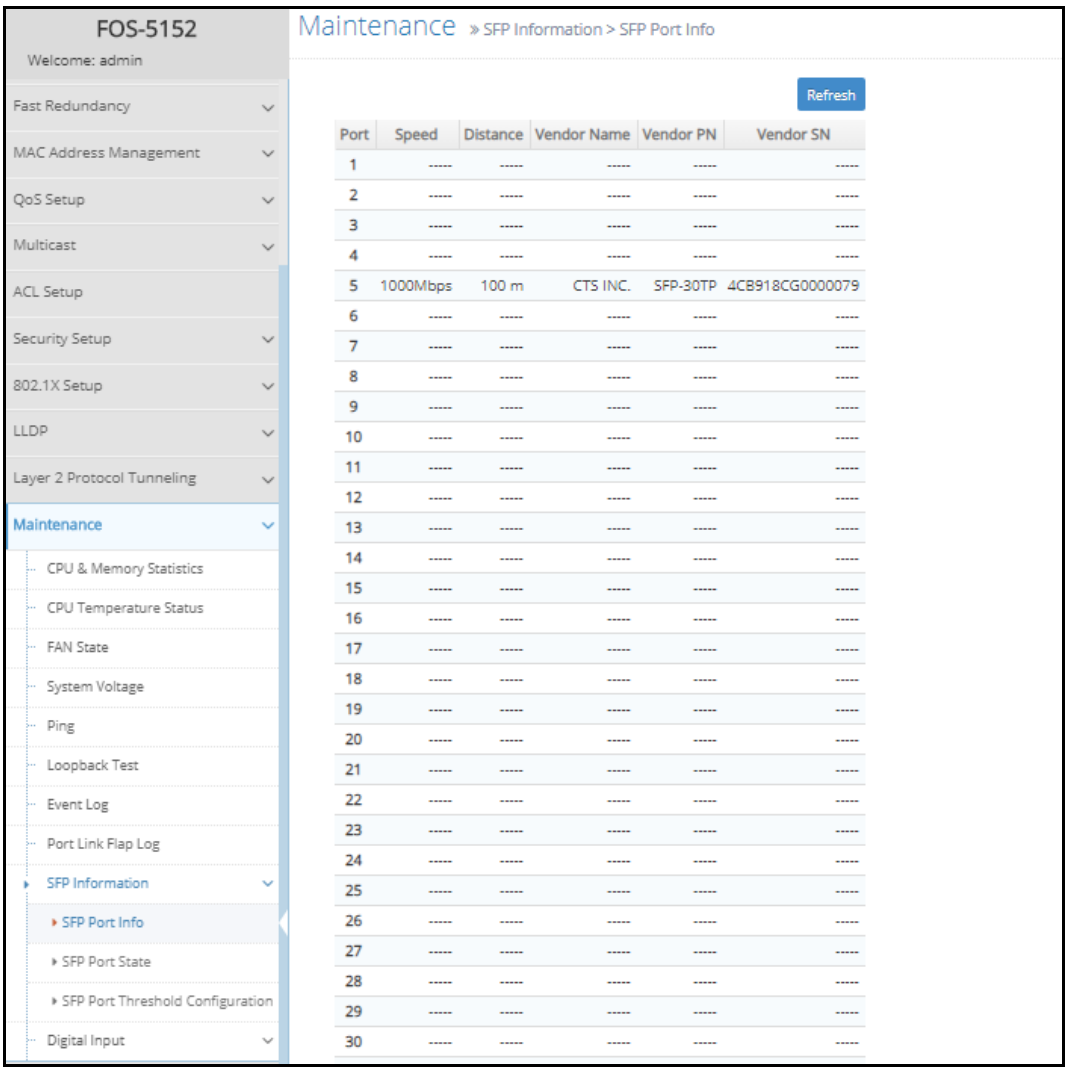
5. **NTP Time:** The NTP time when the event occurred.

6. **Up Time:** The Manage Switch’s uptime when the event occurred.

7. **Description:** A brief account of the event.

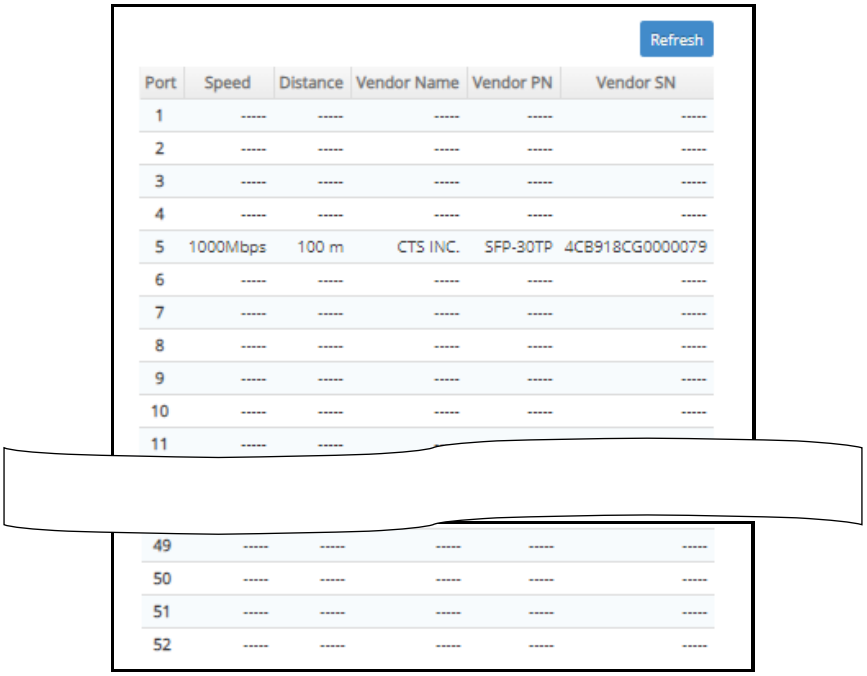
4.15.8 SFP Information

Select the option **SFP Information** from the **Maintenance** menu and then two functions, including SFP Port Info and SFP Port State within this subfolder will be displayed.



4.15.8.1 SFP Port Info

SFP Port Info displays each port's slide-in SFP/SFP+ Transceiver information e.g. the speed of transmission, the distance of transmission, vendor Name, vendor PN, vendor SN, etc. The following screen page appears if you choose **SFP Port Info** function.



Refresh: Click **Refresh** to update the SFP Port Info status.

Port: The number of the SFP/SFP+ module slide-in port.

Speed: Data rate of the slide-in SFP/SFP+ Transceiver.

Distance: Transmission distance of the slide-in SFP/SFP+ Transceiver.

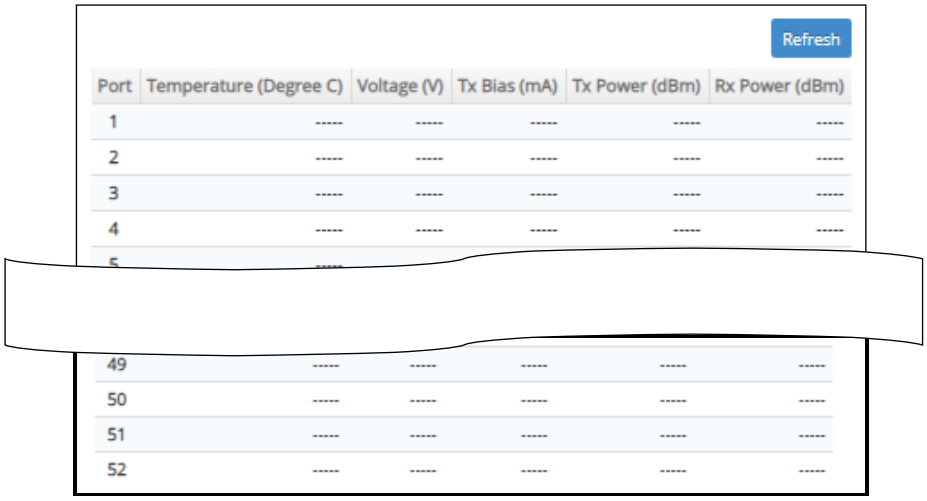
Vendor Name: Vendor name of the slide-in SFP/SFP+ Transceiver.

Vendor PN: Vendor PN of the slide-in SFP/SFP+ Transceiver.

Vendor SN: Vendor SN of the slide-in SFP/SFP+ Transceiver.

4.15.8.2 SFP Port State

SFP Port State displays each port's slide-in SFP/SFP+ Transceiver information e.g. the currently detected temperature, voltage, TX Bias, etc.. The following screen page appears if you choose **SFP Port State** function.



Refresh: Click **Refresh** to update the SFP Port State status.

Port: The number of the SFP/SFP+ module slide-in port.

Temperature (Degree C): The operation temperature of slide-in SFP/SFP+ module currently detected.

Voltage (V): The operation voltage of slide-in SFP/SFP+ module currently detected.

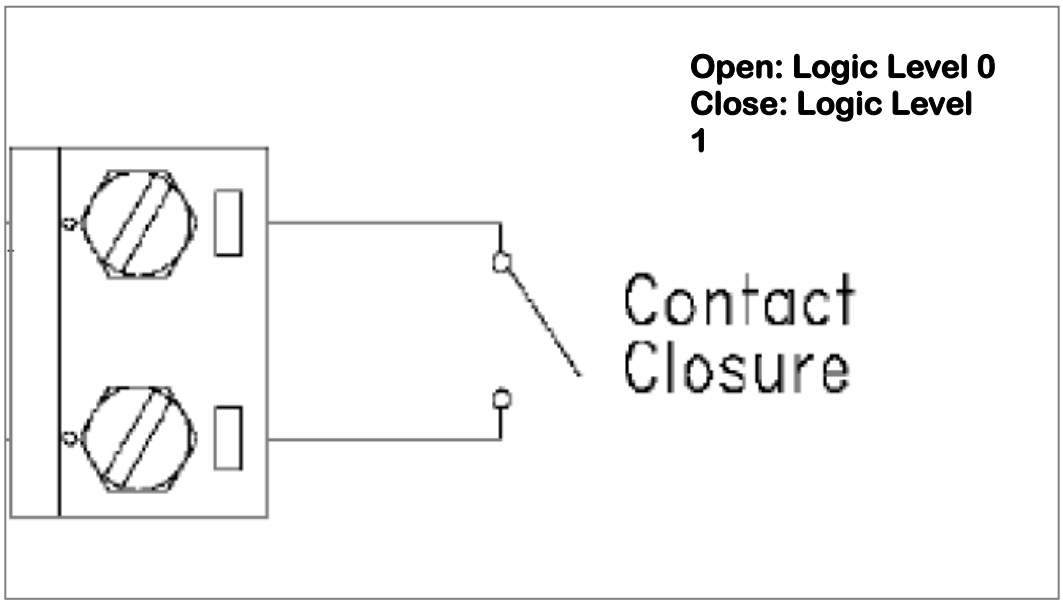
TX Bias (mA): The operation current of slide-in SFP/SFP+ module currently detected.

TX Power (dBm): The optical transmission power of slide-in SFP/SFP+ module currently detected.

RX Power (dBm): The optical receiving power of slide-in SFP/SFP+ module currently detected.

4.15.9 Digital Input

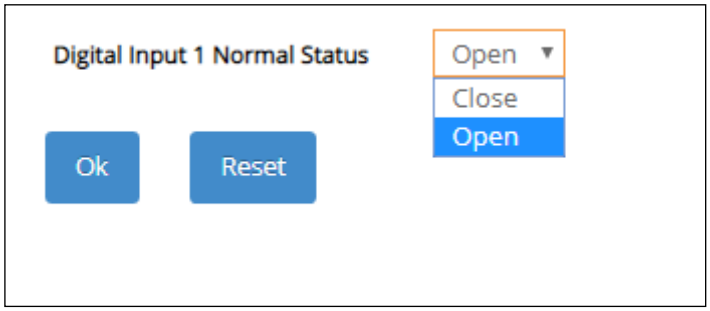
The DI (Digital Input) with a dry contact is a voltage-free connector that is used to decide whether the trigger occurs or not by detecting its open/close status. Refer to the following figure for the DI configuration.



Select the option **Digital Input** from the **Maintenance** menu and then two functions, including Digital Input Config and Digital Input Status within this subfolder will be displayed.

4.15.9.1 Digital Input Configuration

To set up digital input function, select the option **Digital Input Config** from the **Digital Input** menu and then the following screen page appears.



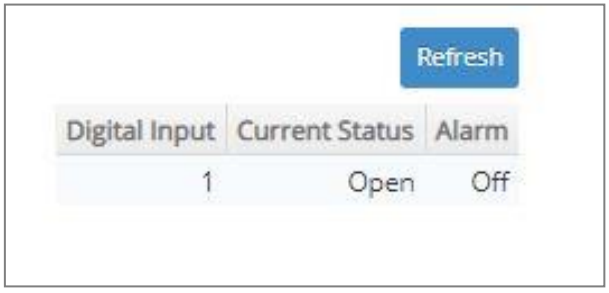
There is one Digital Input Normal Status option shown on the screen page. Normal Status refers to where the contact remains in one state unless actuated. The contact can either be normally open until closed by operation of the switch, or normally closed and opened by the switch action. You may choose either “Open” or “Close” as the normal status of electrical circuit by clicking this pull-down menu.

NOTE: *Digital Input event log can be seen both in the Event Log webpage under the Maintenance Menu and SNMP trap (Digital Input Start trap is enabled) if the alarm is activated.*

Digital Input 1 Normal Status: Set up the normal status between “Open” or “Close” status for the digital input of the Managed Switch. Click **OK**, the new configuration will be taken effect immediately.

4.15.9.2 Digital Input Status

Select **Digital Input Status** from the **Digital Input** menu and then the following screen page appears.



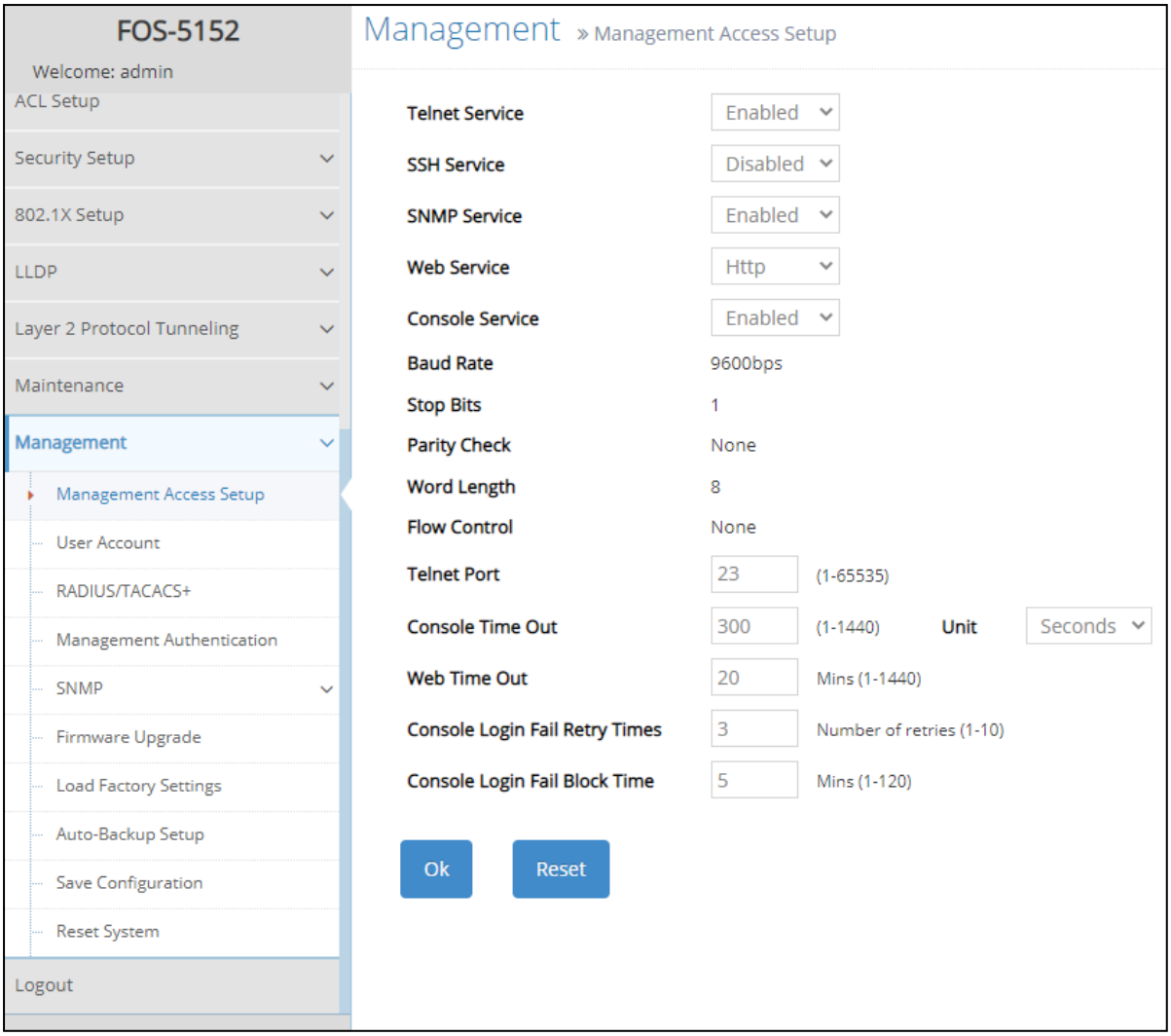
Click **Refresh** to update the digital input and alarm status.

Current Status: View-only field that shows the current status of Digital Input 1.

Alarm: View-only field that shows the current alarm status.

4.16 Management

In order to do the firmware upgrade, load the factory default settings, etc.. for the Managed Switch, please click the folder **Management** from the **Main Menu** and then 8 options will be displayed for your selection.



1. **Management Access Setup:** Enable or disable the specified network services, view the RS-232 serial port setting, specific Telnet and Console services.

2. **User Account:** View the registered user list, add a new user or remove an existing user.

3. **RADIUS/TACACS+:** Set up the RADIUS/TACACS+ server authentication method against which a user accessing the Managed Switch can be authenticated.

4. **Management Authentication:** Set up a planned authentication scheme to be accordingly applied by the Managed Switch authenticating a user's credentials.

5. **SNMP:** Allow administrator to configure password and encryption method of user accounts generated in User Authentication for SNMPv3; view the registered SNMP community name list, add a new community name or remove an existing community name; view the registered SNMP trap destination list, add a new trap destination or remove an existing trap destination; view the Managed Switch trap configuration, enable or disable a specific trap.

6. **Firmware Upgrade:** This allows users to update the latest firmware, save current configuration or restore previous configuration to the Managed Switch.

5. **Load Factory Settings:** Load Factory Setting will reset the configuration including or excluding the IP and Gateway addresses of the Managed Switch back to the factory default settings.

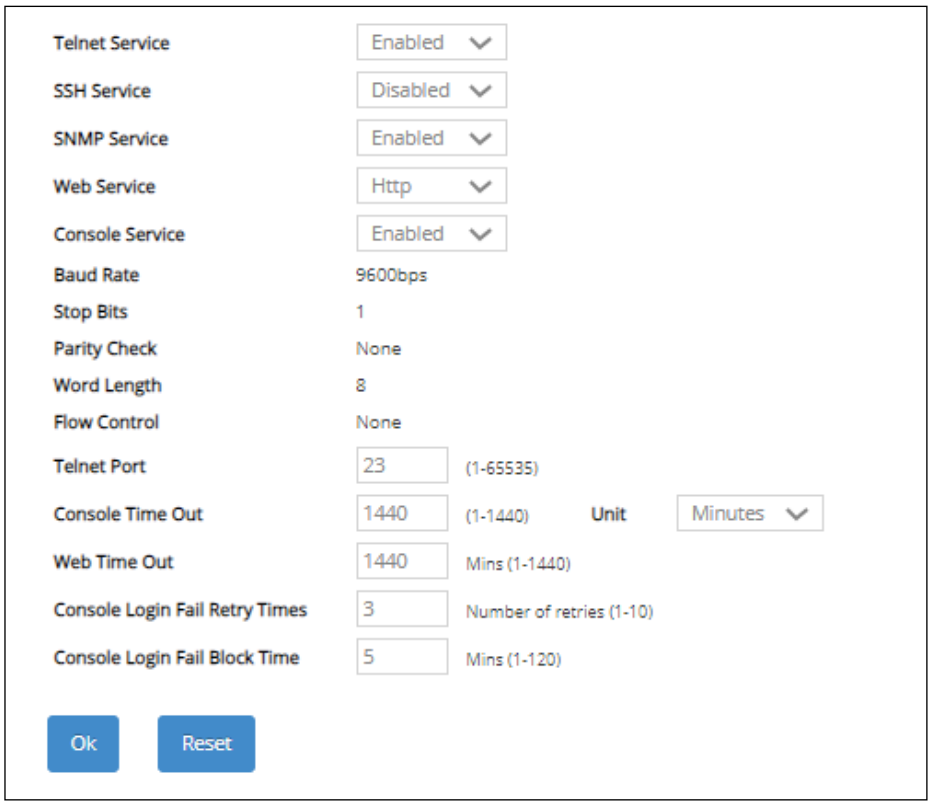
6. **Auto-Backup Setup:** Periodically execute the automatic backup of the start-up configuration files based on the given time you set up.

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

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

4.16.1 Management Access Setup

Click the option **Management Access Setup** from the **Management** menu and then the following screen page appears.



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

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

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

Web Service: To enable or disable the Web Management service. Either **Http** or **Https** option can be selected to enable this service. The difference between these two options is as follows:

- When the **Http** option is chosen, the user is allowed to access the Managed Switch only by inputting its IP address with the format of http://192.168.0.1 in URL.

- When the **Https** option is chosen, this communication protocol is encrypted using Transport Layer Security(TLS) or Secure Sockets Layer (SSL) for secure communication over a computer network.

  HTTPS is provided for authentication of the accessed website and protection of the privacy and integrity of the exchanged data while in transit. It protects against attacks by hackers. The user is allowed to access the Managed Switch either by inputting its IP address with the format of https://192.168.0.1 or http://192.168.0.1 that will be automatically transferred into https://192.168.0.1 in URL.

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

Baud Rate: 9600 bps, RS-232 setting, view-only field.

Stop Bits: 1, RS-232 setting, view-only field.

Parity Check: None, RS-232 setting, view-only field.

Word Length: 8, RS-232 setting, view-only field.

Flow Control: None, RS-232 setting, view-only field.

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

Console Time Out: Specify the desired time that the Managed Switch will wait before disconnecting an inactive console/telnet session. Valid range:1-1440 seconds or minutes.

Unit: Specify the unit for the **Console Time Out** parameter.

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

Console Login Fail Retry Times: Specify the desired times that the Managed Switch will allow the user to retry to login the system via console if the console login fails. Valid range: 1-10.

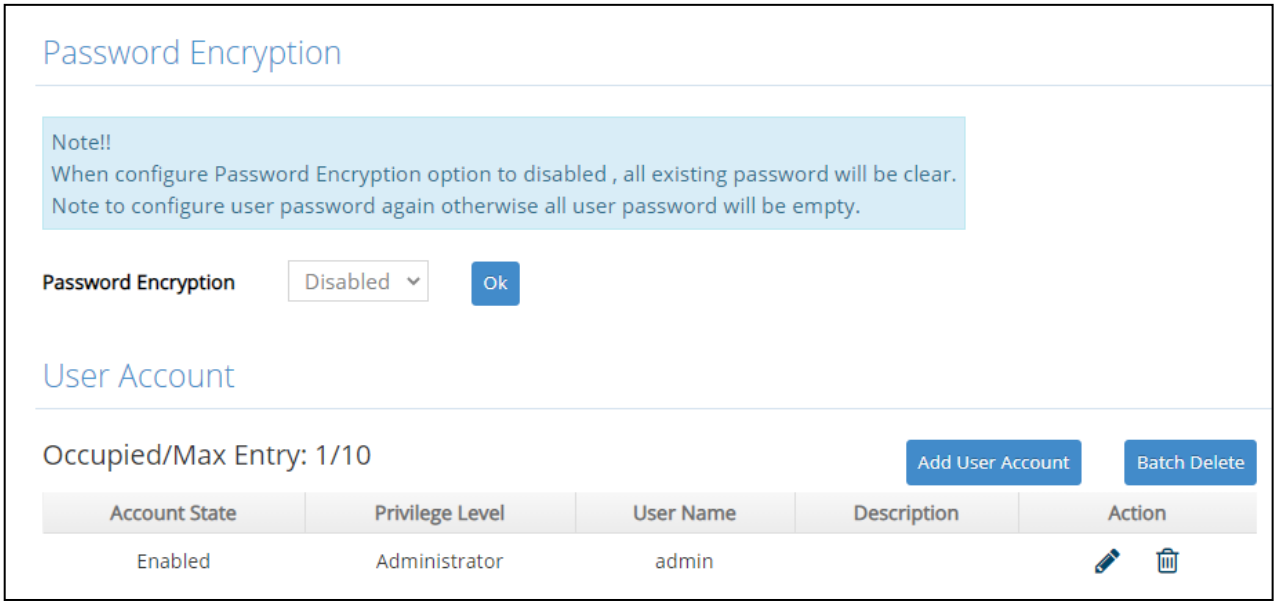
Console Login Fail Block Time: Specify the desired time that the Managed Switch will unblock the console for user's login if the accumulated retries times exceed the value you set up in **Console Login Fail Retry Times** parameter.

4.16.2 User Account

To prevent any unauthorized operations, only registered users are allowed to operate the Managed Switch. Users who would like to operate the Managed Switch need to create a user account first.

To view or change current registered users, select the option **User Account** from the **Management** menu and then the following screen page shows up.

.



Password Encryption: Pull down the menu of **Password Encryption** 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. Click **OK**, the new settings will be taken effect immediately. The default setting is disabled.

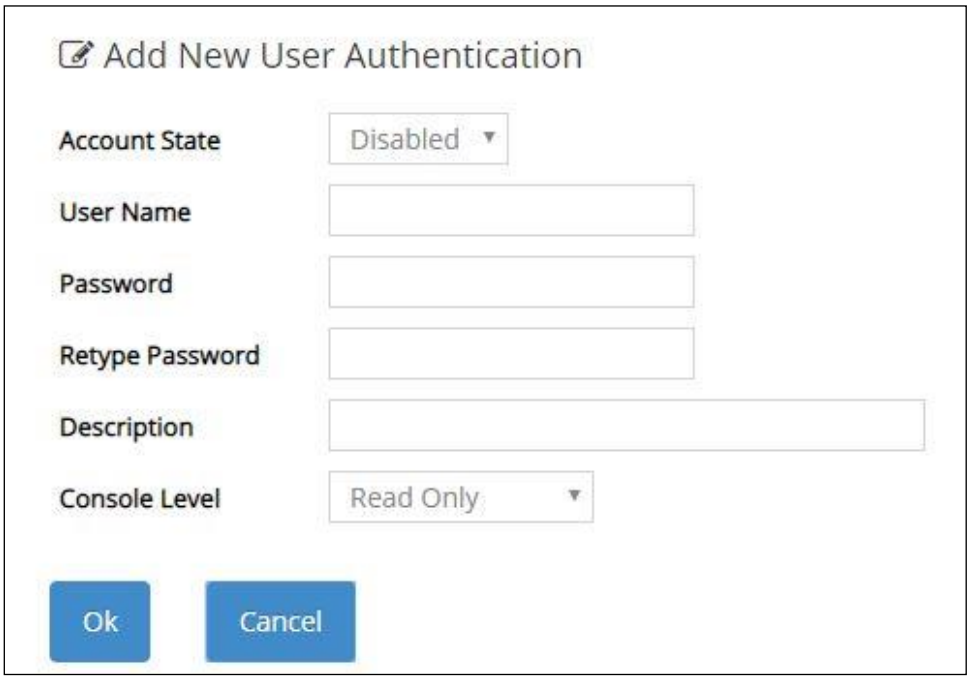
This user list will display the overview of each configured user account. Up to 10 users can be registered.

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total users who have already registered.

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

Click **Add User Account** to add a new user and then the following screen page appears for the further user registration settings.



Account State: Enable or disable this user account.

User Name: Specify the authorized user login name. Up to 20 alphanumeric characters can be accepted.

Password: Enter the desired user password. Up to 20 alphanumeric characters can be accepted.

Retype Password: Enter the password again for double-checking.

Description: Enter a unique description for this user. Up to 35 alphanumeric characters can be accepted. This is mainly used for reference only.

Console Level: Select the desired privilege level for the management operation from the pull-down menu. Three operation levels of privilege are available in Managed Switch:

> **Administrator:** Own the full-access right. The user can maintain user account as well as system information, load the factory default settings, and so on.
>
> **Read & Write:** Own the partial-access right. The user is unable to modify user account and system information, do the firmware upgrade, load the factory default settings, and set up auto-backup.
>
> **Read Only:** Allow to view only.

Click the  icon to modify the settings of a registered user you specify.

Click the  icon to remove the selected registered user account from the user list. Or click **Batch Delete** to remove a number of /all user accounts at a time by clicking on the checkbox belonging to the corresponding user in the **Action** field and then click **Delete Select Item**, the selected user(s) will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

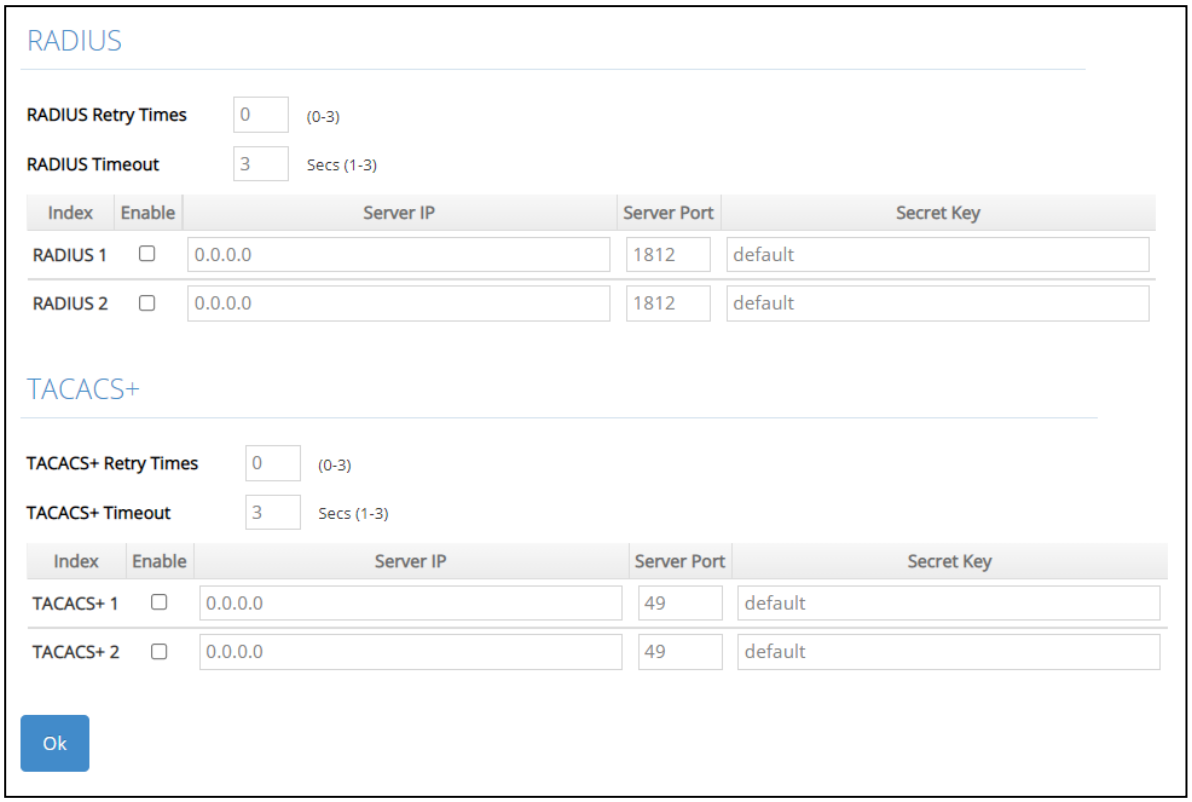
NOTE:

1. *To prevent incautious operations, users cannot delete their own account, modify their own user name and change their own account state.*
2. *The acquired hashed password from backup config file is not applicable for user login on CLI/Web interface.*
3. *We strongly recommend not to alter off-line Auth Method setting in backup configure file.*
4. *If Auth-Method is enabled and do firmware downgrade, users must reset default config.*

4.16.3 RADIUS/TACACS+

RADIUS and TACACS+ are namely two protocols used in the centralized management over the access into the network mainly for preventing the unauthorized connection, both working under the framework AAA (authentication, authorization, and accounting). The first “A” denotes that a RADIUS/TACACS+ client is required to transmit its username and its password for the authentication against the RADIUS/TACACS+ server. If the credentials are valid, the access-accept message will then be sent, and the client at this point will gain the approval of access into the Managed Switch, which in return delivers effective protection against unauthorized operation from malicious users.

To configure RADIUS/TACACS+, select the option **RADIUS/TACACS+** from the **Management** menu and then the following screen page shows up.



RADIUS: Configure the RADIUS server authentication method.

1. **RADIUS Retry Times:** The maximum number of attempts to reconnect if the RADIUS server is not reachable. Valid values are 0 through 3.

2. **RADIUS Timeout:** The amount of time (second) that the Managed Switch will wait if the RADIUS server is not responding. Valid values are 1 through 3.

3. **Index:** The entry of the RADIUS servers. Up to 2 servers can be configured as the RADIUS authentication server.

4. **Enable:** Click the checkbox of the intended RADIUS server to enable RADIUS authentication. Once it's enabled, the user login will be upon those settings on the RADIUS server.

5. **Server IP:** The IPv4/IPv6 address of the RADIUS server.

6. **Server Port:** The RADIUS service port on the RADIUS server. Valid values are 1025 through 65535.

7. **Secret Key:** The secret key for the RADIUS server; it is used to validate communications with the RADIUS server. Up to 32 alphanumeric characters can be set up.

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

TACACS+: Configure the TACACS+ server authentication method.

1. **TACACS+ Retry Times:** The maximum number of attempts to reconnect if the TACACS+ server is not reachable. Valid values are 0 through 3.

2. **TACACS+ Timeout:** The amount of time (second) that the Managed Switch will wait if the TACACS+ server is not responding. Valid values are 1 through 3.

3. **Index:** The entry of the TACACS+ servers. Up to 2 servers can be configured as the TACACS+ authentication server.

4. **Enable:** Click the checkbox of the intended TACACS+ server to enable TACACS+ authentication. Once it's enabled, the user login will be upon those settings on the RADIUS server.

5. **Server IP:** The IPv4/IPv6 address of the TACACS+ server.

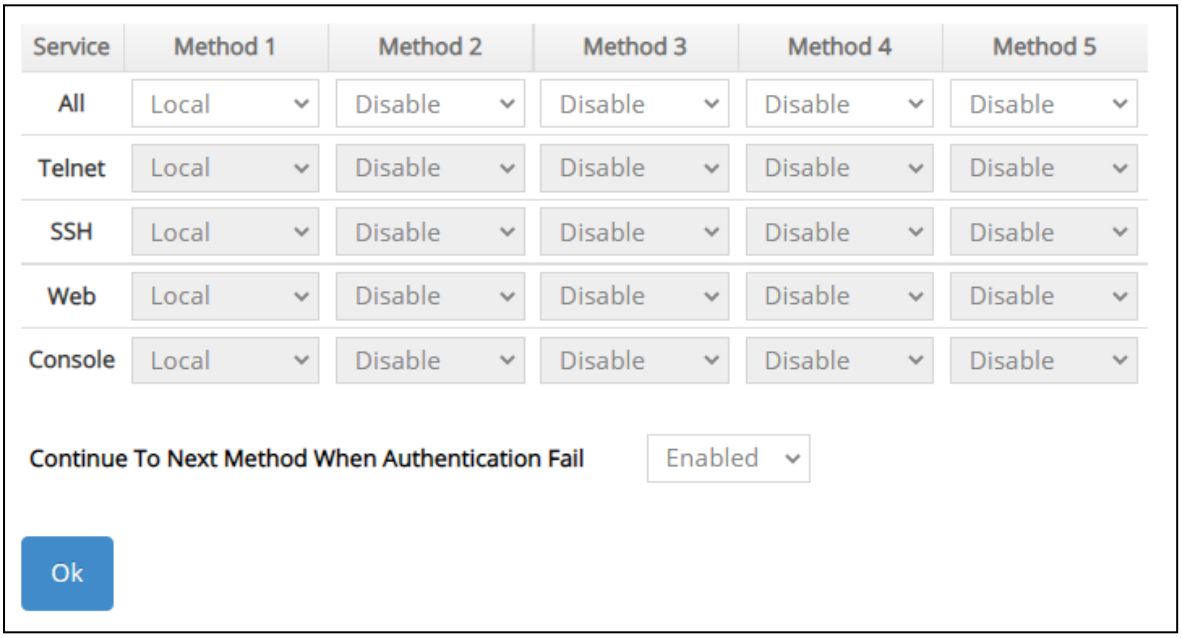
6. **Server Port:** The TACACS+ service port on the TACACS+ server. Valid values are 49, and 1025 through 65535.

7. **Secret Key:** The secret key for the TACACS+ server; it is used to validate communications with the TACACS+ server. Up to 32 alphanumeric characters can be set up.

4.16.4 Management Authentication

Management Authentication makes possible the versatile approaches to authentication on the Managed Switch. Network administrators can opt for multiple authentication methods and prioritize them in accordance with their most desired plan. This function brings not only enhanced flexibility to the authentication management, but also a smart countermeasure for an unexpected user authentication failure.

To configure the authentication method, select the option **Management Authentication** from the **Management** menu and then the following screen page shows up.



Service: The interfaces via which the user accesses the Managed Switch, including **All**, **Telnet**, **SSH**, **Web**, and **Console**.

All: Every user accessing the Managed Switch will be authenticated against the same

authentication method scheme, regardless of the interface adopted by the user.

Method 1-5: Select **Local**, **RADIUS 1**, **RADIUS 2**, **TACACS+ 1**, **TACACS+ 2,** or **Disable** from each Method's pull-down menu to form a chain of authentication methods. However, **Local** must be set after **RADIUS** and **TACACS+** servers throughout the specified method scheme, and the 1st method cannot be configured as **Disable**.

Local: The user information stored in the Managed Switch against which the user will be authenticated when accessing the Managed Switch.

RADIUS 1/2: The RADIUS server against which the user will be authenticated when accessing the Managed Switch.

TACACS+ 1/2: The TACACS+ server against which the user will be authenticated when accessing the Managed Switch.

Continue To Next Method When Authentication Fail: Select **Enabled** or **Disabled** from the pull-down menu to enable or disable the function.

Note:
1. *Once this function is enabled, the Managed Switch will continue to the next method if Method 1 fails, say, due to invalid client credentials. It indeed delivers extra flexibility for an ought-to-be-authenticated user, yet at the expense of network security. To fully protect against malicious users, it's recommended to set this function disabled.*

2. Disabling this function means the device will only apply Method 1. Access to the Managed Switch will be denied to those who fail the authentication with Method 1.

4.16.5 SNMP

Select the option **SNMP** from the **Management** menu and then four functions, including SNMPv3 USM User, Device Community, Trap Destination and Trap Setup will be displayed for your selection.

4.16.5.1 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. The following screen page appears if you choose **SNMPv3 USM User** function.

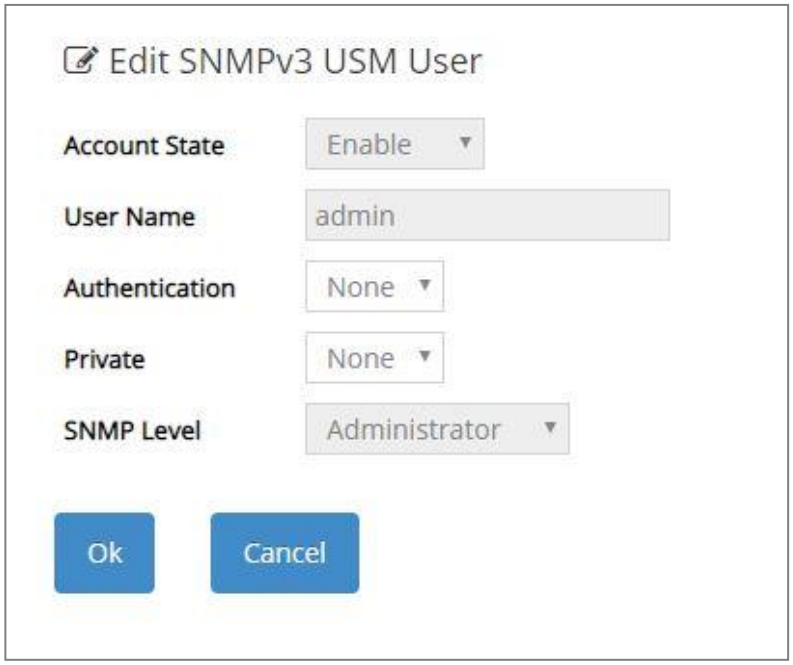
Note: *The SNMPv3 user account is generated from "User Authentication". (Refer to Section 4.15.2)*

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total registered communities.

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

Click the icon to modify the SNMPv3 USM User settings for a registered user.



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. Select “None” from the pull-down menu 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. Select “MD5” from the pull-down menu to enable this authentication.

SHA(Secure Hash Algorithm): A 160-bit hash function which resembles the said MD5 algorithm. Select “SHA” from the pull-down menu to enable this authentication.

Authentication-Password: Specify the passwords if “MD5” or “SHA” is chosen. Up to 20 characters can be accepted.

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. Select “None” from the pull-down menu to disable it.

DES (Data Encryption Standard): An algorithm to encrypt critical information such as message text message signatures, etc. Select “DES” from the pull-down menu to enable it.

Private-Password: Specify the passwords if “DES” is chosen. Up to 20 characters can be accepted.

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

Administrator: Own the full-access right, including maintaining user account & system information, load factory settings …etc.

Read & Write: Own the 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 shown 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	Enables authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms.
MD5 or SHA	Data Encryption Standard(DES)	Enables authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms. What’s more, enables DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES standard.

4.16.5.2 Device Community

The following screen page appears if you choose **Device Community** function.

This table will display the overview of each configured devcie community. Up to 10 devcie communities can be registered.

Occupied/Max Entry: View-only field.

Occupied: his shows the amount of total registered communities.

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

Click **Add Device Community** to add a new community and then the following screen page appears for the further devcie community settings.

Account State: Enable or disable this Community Account.

SNMP Level: Click the pull-down menu to select the desired privilege for the SNMP operation.

NOTE: *When the community browses the Managed Switch without proper access right, the Managed Switch will not respond. For example, if a community only has Read & Write privilege, then it cannot browse the Managed Switch's user table.*

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

Description: Enter a unique description for this community name. Up to 35 alphanumeric characters can be accepted. This is mainly for reference only.

Click ✔ when the settings are completed, this new community will be listed on the devcie community table, or click ✖ to cancel the settings.

Click the icon to modify the settings of a specified community.

Click the icon to remove a specified registered community entry and its settings from the devcie community table. Or click **Batch Delete** to remove a number of /all communities at a time by clicking on the checkbox belonging to the corresponding community in the **Action** field and then click **Delete Select Item**, the selected community/communities will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

4.16.5.3 Trap Destination

The following screen page appears if you choose **Trap Destination** function.

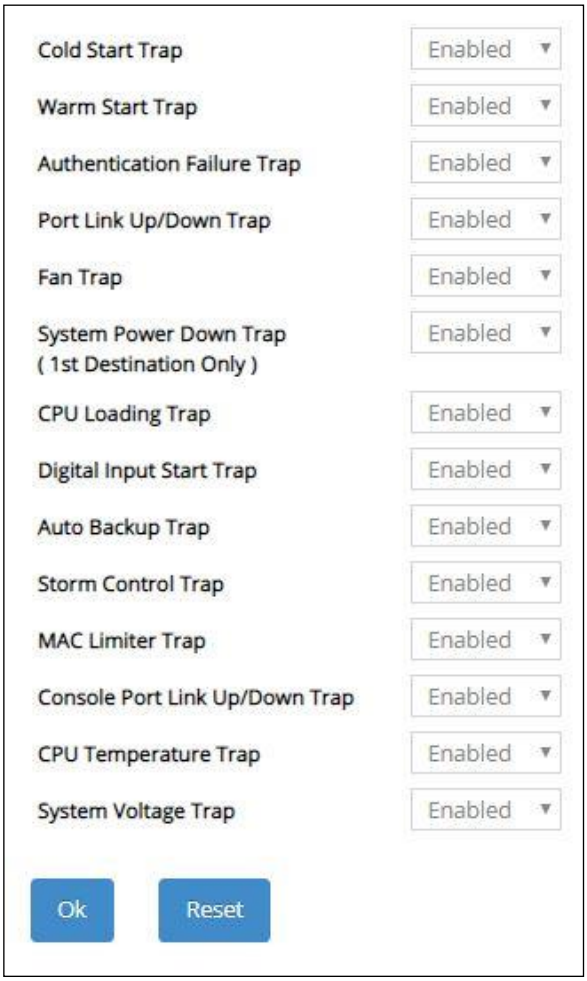
State: Enable or disable the function of sending trap to the specified destination.

Destination IP: Enter the specific IPv4/IPv6 address of the network management system that will receive the trap.

Community: Enter the description for the specified trap destination.

4.16.5.4 Trap Setup

The following screen page appears if you choose **Trap Setup** function.



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.

Fan Trap: Enable or disable the Managed Switch to send a trap either when the fan speed of FAN1/FAN2/FAN3 is zero or at/under the threshold (**≤** 5040 RPM).

System Power Down Trap (1st Destination Only): Enable or disable the Managed Switch to send a trap when the power failure occurs.

CPU Loading Trap: Enable or disable the Managed Switch to send a trap when the CPU is overloaded.

Digital Input Start Trap: Enable or disable the Managed Switch to send a trap when the alarm occurs.

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

Storm Control Trap: Enable or disable the Managed Switch to send a trap when broadcast/ unknown multicast/unknown unicast packets flood. And it will keep sending this trap upon the notification threshold interval setup of Storm Control function once these packets flood continuously.

MAC Limiter Trap: Enable or disable the Managed Switch to send a trap when any port in which the Mac Limit function is enabled exceeds the specified source MAC address limit. And it will keep sending this trap upon the notification threshold interval setup of MAC Limiters function once any port exceeds the specified source MAC address limit continuously.

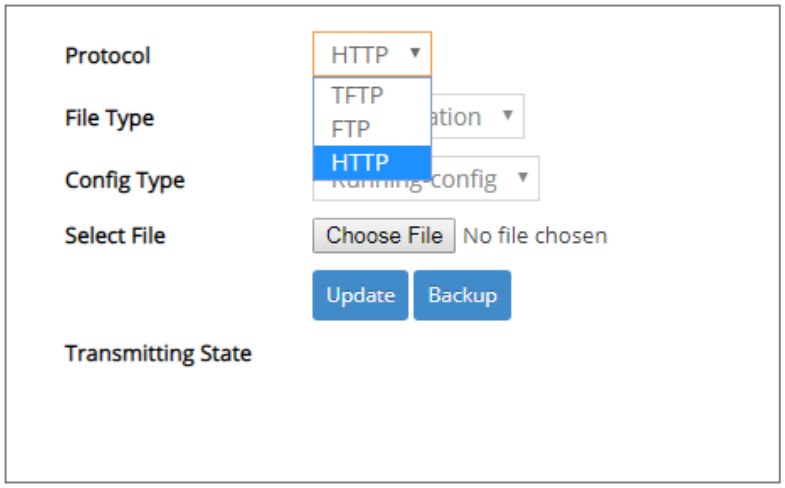
Console Port Link Up/Down Trap: Enable or disable the Managed Switch to send a trap when console port link up/link down occurs.

CPU Temperature Trap: Enable or disable the Managed Switch to send a trap when CPU temperature is over the parameter of **High Temperature Threshold** value, CPU temperature returns to the normal status (at or under the parameter of **High Temperature Threshold** value), CPU temperature exceeds the range of threshold (0~95 degrees centigrade), or the temperature sensor fails to detect CPU temperature.

System Voltage Trap: Enable or disable the Managed Switch to send a trap either when the voltage of ASIC system power/ASIC core power/Power A/Power B is at/over the High threshold or at/under the Low threshold.

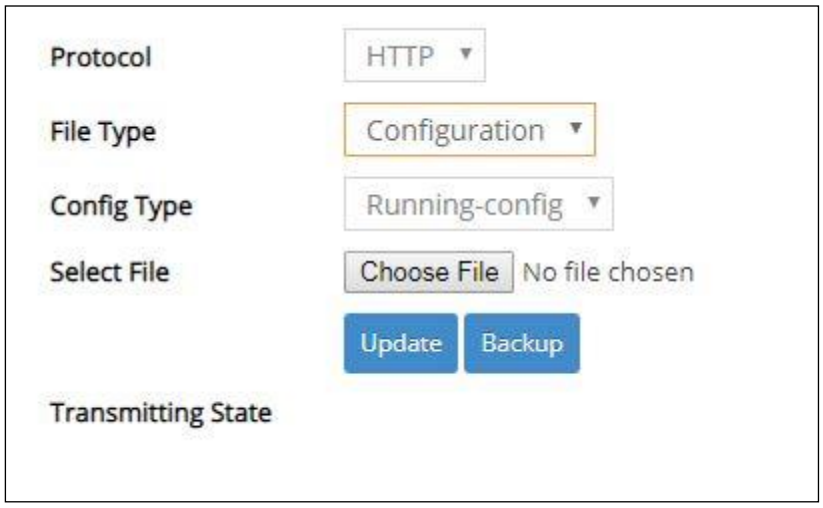
4.16.6 Firmware Upgrade

The Managed Switch offers three methods, including HTTP, FTP and TFTP to back up/restore the configuration and update the firmware. To do this, please select the option **Firmware Upgrade** from the **Management** menu and then the following screen page appears.



4.16.6.1 Configuration Backup/Restore via HTTP

To back up or restore the configuration via HTTP, just pull down the **Protocol** menu and select **HTTP**. Also configure the type of file as **"Configuration"** to process. The related parameter description is as below.



Config Type: There are three types of the configuration file: Running-config, Default-config and Start-up-config.

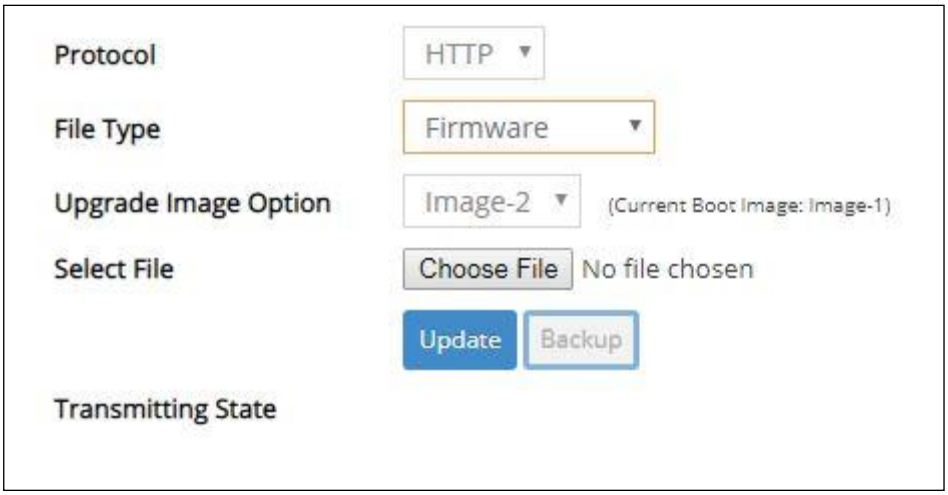
- **Running-config:** Back up the data you're processing.
- **Default-config:** Back up the data same as the factory default settings.
- **Start-up-config:** Back up the data same as last saved data.

Backup: Click **Backup** to begin download the configuration file to your PC.

Select File: Click **Choose File** to select the designated data and then click **Update** to restore the configuration.

4.16.6.2 Firmware Upgrade via HTTP

To update the firmware via HTTP, just pull down the **Protocol** menu and select **HTTP**. Also configure the type of file as **"Firmware"** to process. The related parameter description is as below.

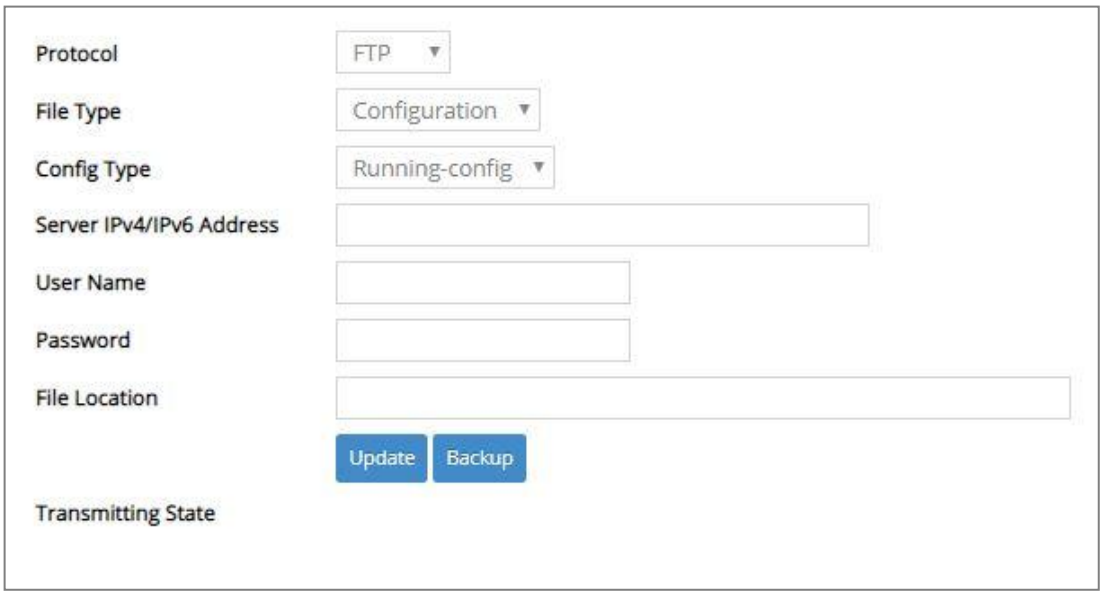


Upgrade Image Option: Pull down the list to choose the image you would like to upgrade.

Select File: Click **Choose File** to select the desired file and then click **Update** to begin the firmware upgrade.

4.16.6.3 Configuration Backup/Restore via FTP/TFTP

The Managed Switch has both built-in TFTP and FTP clients. Users may back up or restore the configuration via FTP/TFTP. Just pull down the **Protocol** menu and select **FTP** or **TFTP**, also configure the type of file as **"Configuration"** to process. The related parameter description is as below.



Protocol: Select the preferred protocol, either FTP or TFTP.

Config Type: Choose the type of the configuration file that will be saved or restored among “Running-config”, “Default-config” or “Start-up-config”.

Server IPv4/IPv6 Address: Enter the specific IPv4/IPv6 address of the FTP/TFTP file server.

User Name (for FTP only): Enter the specific username to access the FTP file server.

Password (for FTP only): Enter the specific password to access the FTP file server.

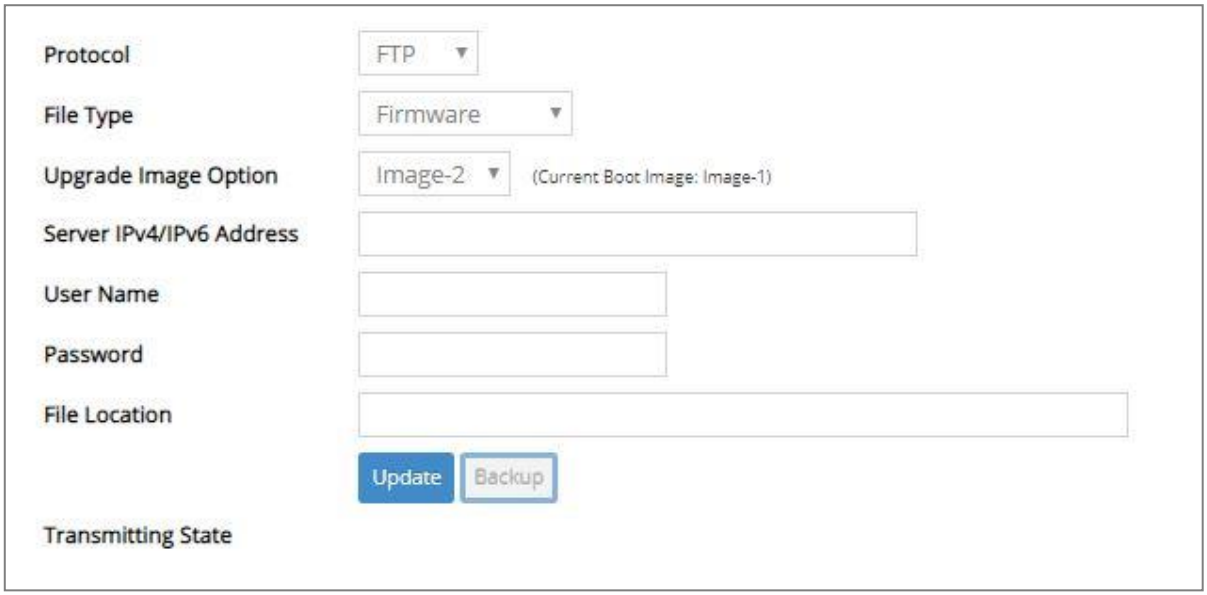
File Location: Enter the specific path and filename within the FTP/TFTP file server.

Click **Backup** to start the download process and receive files from the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind the user.

Click **Update** to start the upload process and transmit files to the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind users.

4.16.6.4 Firmware Upgrade via FTP/TFTP

The Managed Switch has both built-in TFTP and FTP clients. Users may update the firmware via FTP/TFTP. Just pull down the **Protocol** menu and select **FTP** or **TFTP**, also configure the type of file as **“Firmware”** to process. The related parameter description is as below.



Protocol: Select the preferred protocol, either FTP or TFTP.

Upgrade Image Option: Pull down the list to choose the image you would like to upgrade.

Server IPv4/IPv6 Address: Enter the specific IPv4/IPv6 address of the FTP/TFTP file server.

User Name (for FTP only): Enter the specific username to access the FTP file server.

Password (for FTP only): Enter the specific password to access the FTP file server.

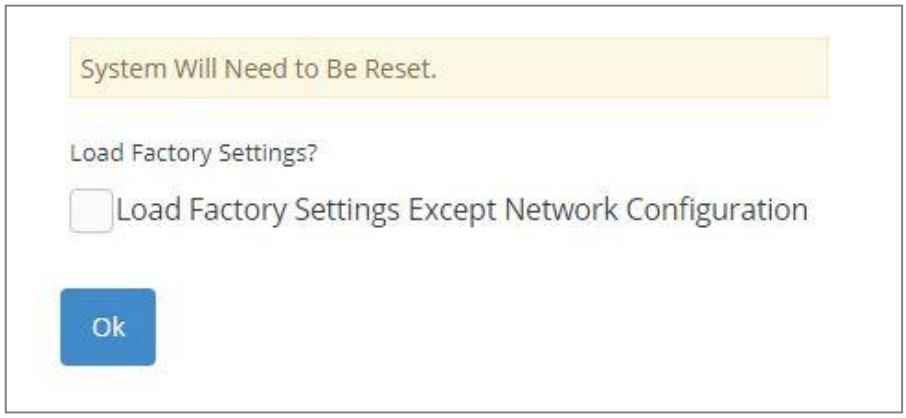
File Location: Enter the specific path and filename within the FTP/TFTP file server.

Click **Update** to start the upload process and transmit files to the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind users.

4.16.7 Load Factory Settings

Load Factory Settings will set all the configurations of the Managed Switch back to the factory default settings, including the IP and Gateway address. **Load Factory Setting** 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 Setting.

Select the option **Load Factory Settings** from the **Management** menu and then the following screen page appears.



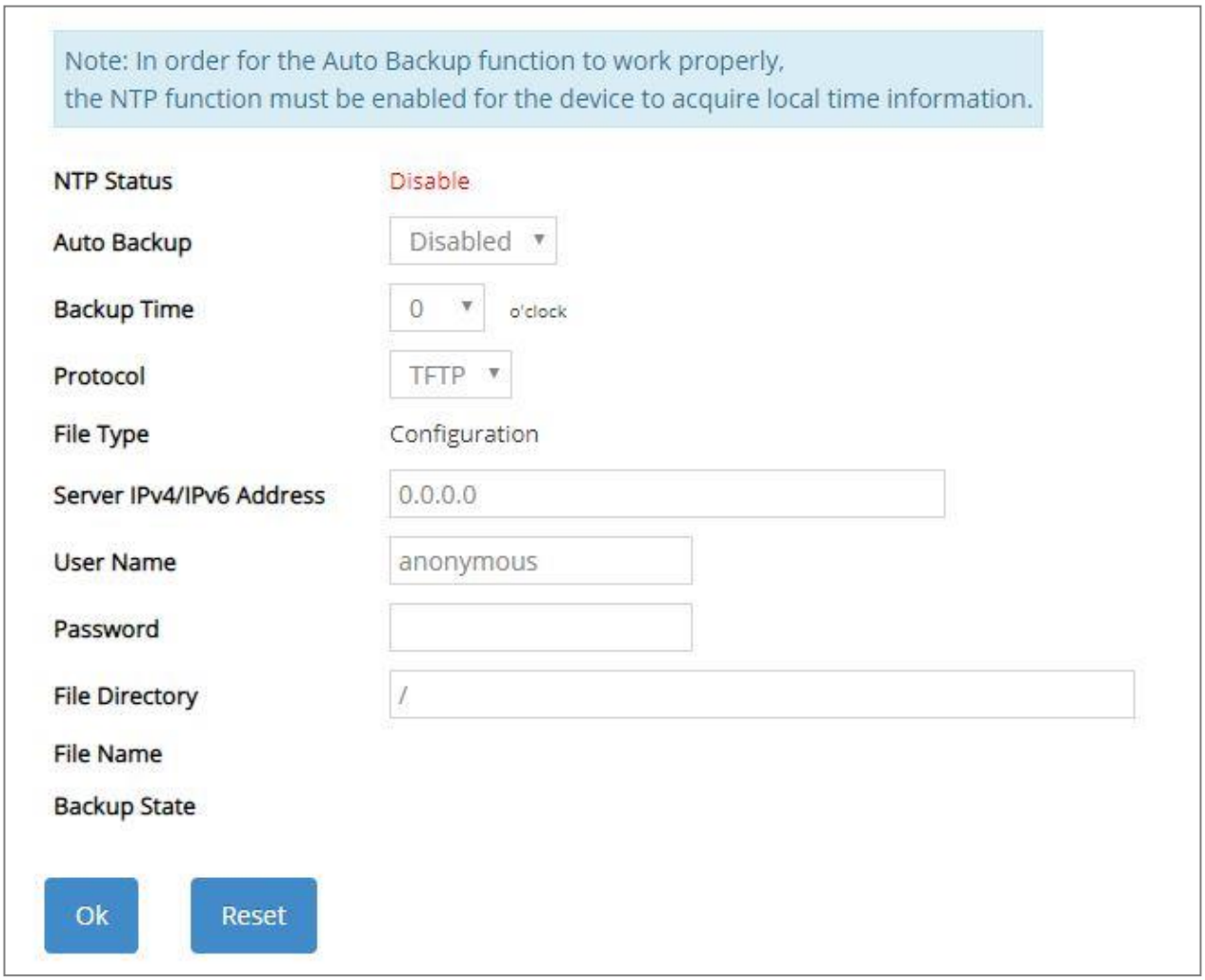
Load Factory Settings Except Network Configuration: It will set all the configurations of the Managed Switch back to the factory default settings. However, IP and Gateway addresses will not restore to the factory default. It is very useful when network administrators need to re-configure the system “REMOTELY” because conventional Factory Reset will bring network settings back to default and lose all network connections.

Click **OK** to start loading factory settings. Or click the checkbox in front of **Load Factory Settings Except Network Configuration** and then click **OK** to start loading factory settings except network configuration.

4.16.8 Auto-Backup Setup

In the Managed Switch, the forementioned **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 Setup** function to do this backup automatically and periodically. It is useful to prevent the loss of users’ 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 Setup** from the **Management** menu, the following screen page shows up.



NTP Status: Display the current state of NTP server. Include Disable, Inactive and active 3 states.

Disable: NTP server is disabled.

Inactive: NTP server is enabled, but the Managed Switch does not obtain the local time from NTP server.

Active: NTP server is enabled, and the Managed Switch obtains the local time from NTP server.

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

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 backup the start-up configuration files.

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

Server IPv4/IPv6 Address: Set up the IPv4/IPv6 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.

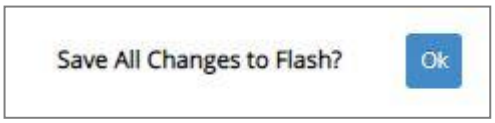
File Name: The filename assigned to the auto- backup configuration files. The format of filename generated automatically is as follows:

> **ip address_Device Name_yyyyMMdd-HHmm.txt** , for example, 192.168.0.3_FOS-5152_20190606-1600.txt

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

4.16.9 Save Configuration

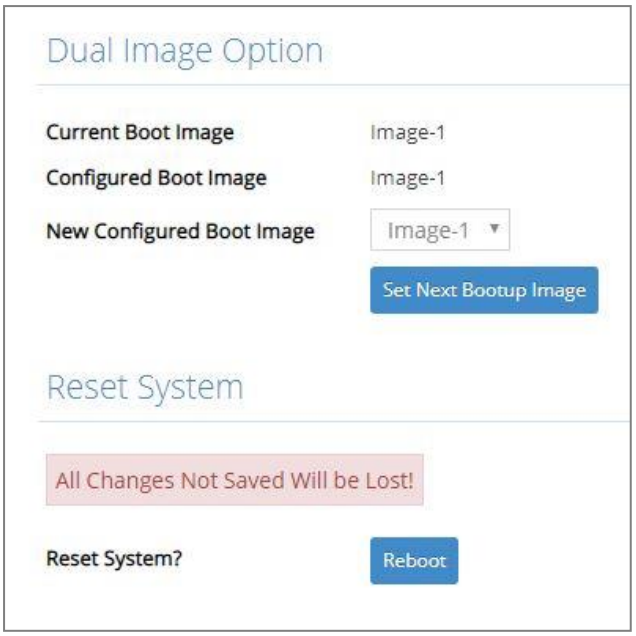
In order to save the configuration permanently, users need to save configuration first before resetting the Managed Switch. Select the option **Save Configuration** from the **Management** menu and then the following screen page appears.



Click **OK** to save the configuration. Alternatively, you can also press the **Save** quick button located on the top-right side of the webpage, which has the same function as Save Configuration.

4.16.10 Reset System

To reboot the system, please select the option **Reset System** from the **Management** menu and then the following screen page appears. From the pull-down menu of **New Configured Boot Image**, you can choose the desired image for the next system reboot if necessary.



Click **Set Next Bootup Image** to change the image into the new boot-up image you select.
Click **Reboot** to restart the Managed Switch.

APPENDIX A: Free RADIUS readme

The advanced RADIUS Server Set up for **RADIUS Authentication** is described as below.

When free RADIUS client is enabled on the device,

On the server side, it needs to put this file "**dictionary.sample**" under the directory **/raddb**, and modify these three files - "**users**", "**clients.conf**" and "**dictionary**", which are on the disc shipped with this product.

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

In the file "**users**",

Set up user name, password, and other attributes.

In the file "**clients.conf**",

Set the valid range of RADIUS client IP address.

In the file "**dictionary**",
Add this following line -

$INCLUDE dictionary.sample

APPENDIX B: Set Up DHCP Auto-Provisioning

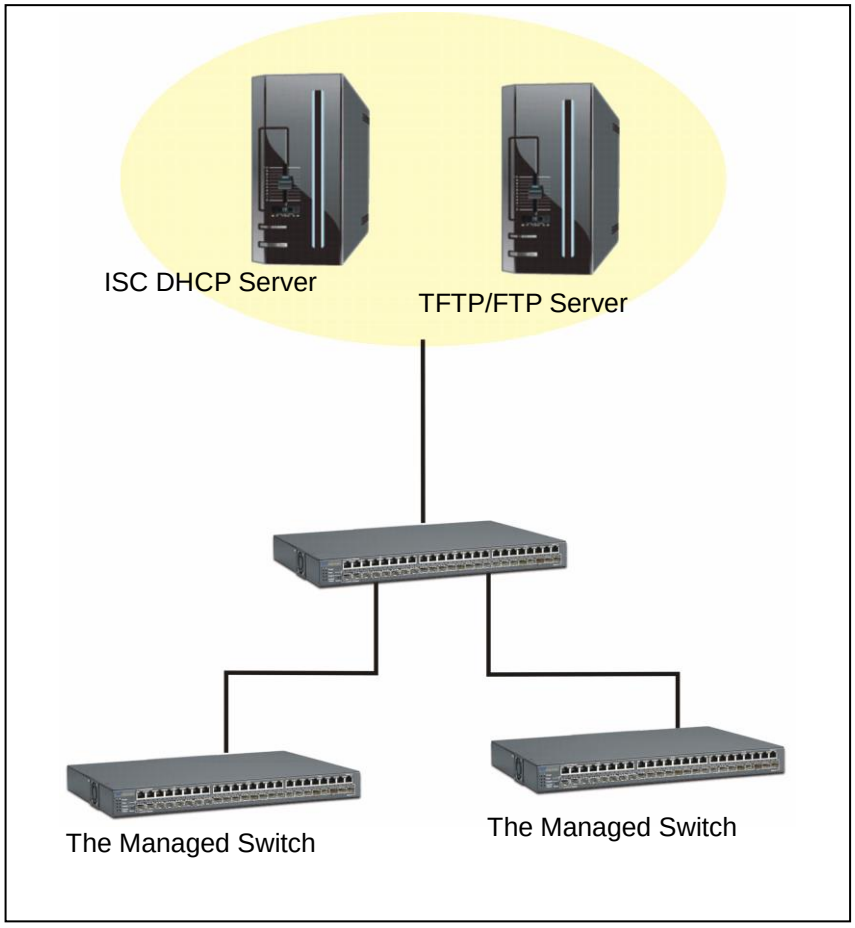
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the Managed Switch that you purchased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

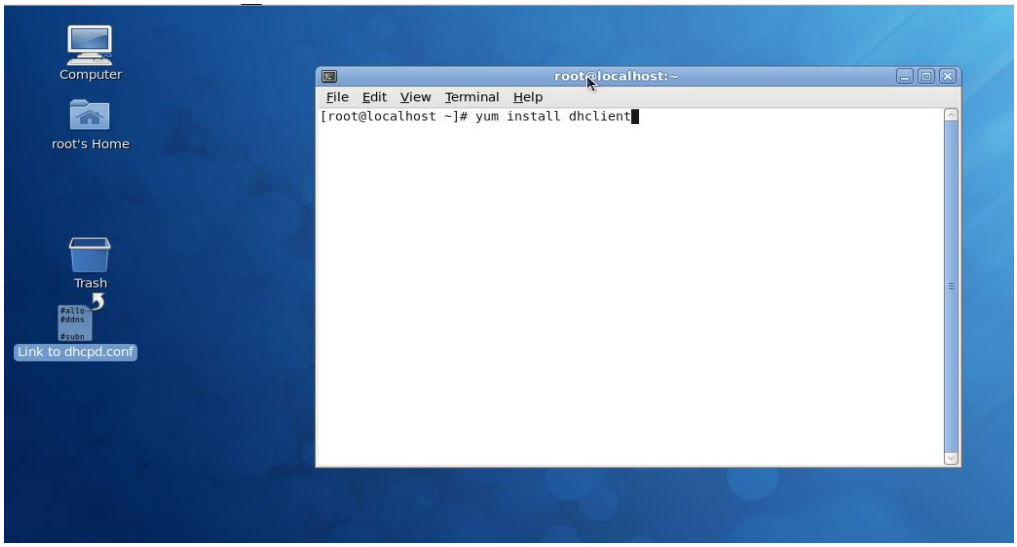
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Topology Example

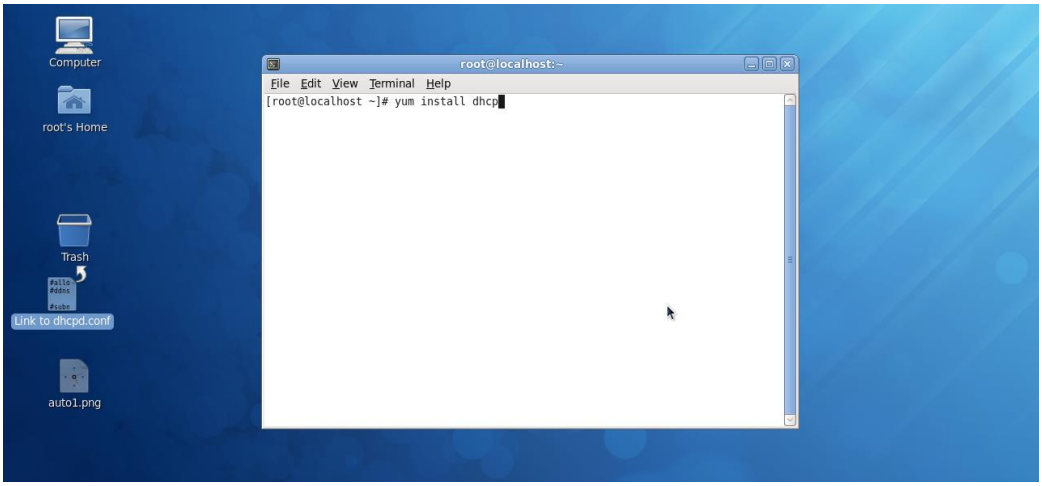
Step 2. Set up Auto Provision Server

- **Update DHCP Client**



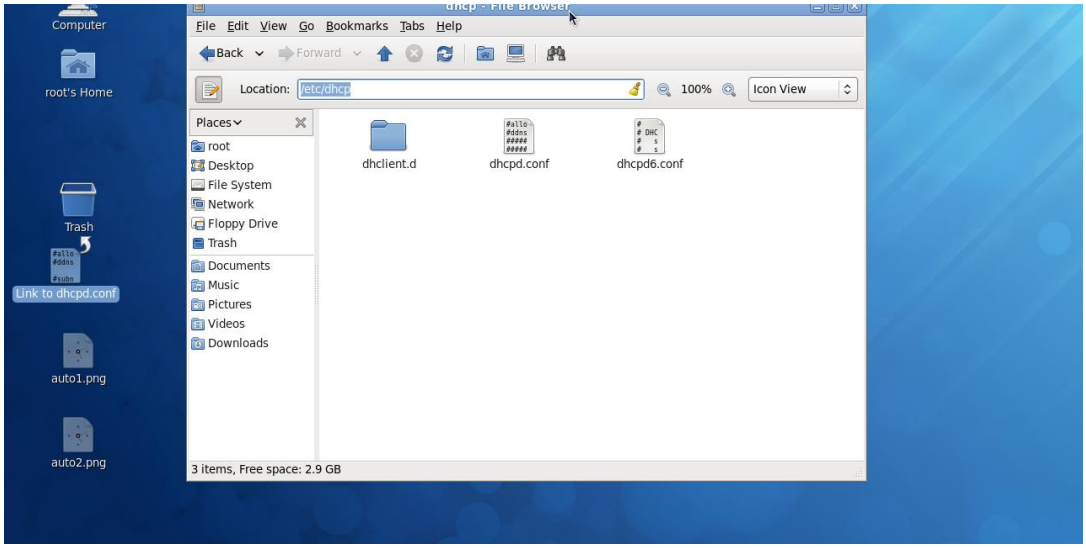
Linux Fedora 12 supports “yum” function by default. First of all, update DHCP client function by issuing “yum install dhclient” command.

- **Install DHCP Server**



Issue “yum install dhcp” command to install DHCP server.

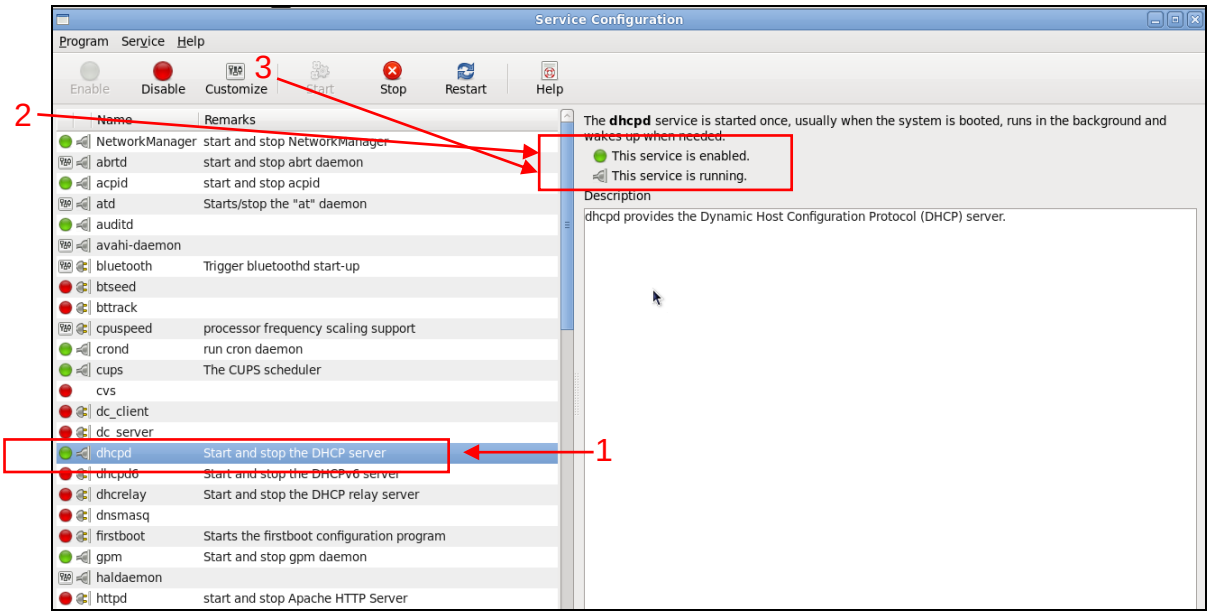
- **Copy dhcpd.conf to /etc/dhcp/ directory**



Copy dhcpd.conf file provided by the vendor to /etc/dhcp/ directory.

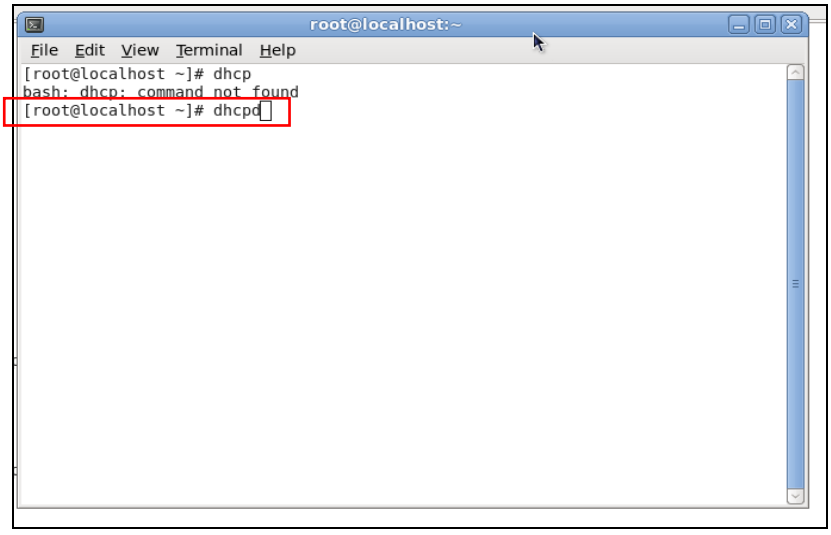
Please note that each vendor has their own way to define auto provisioning. Make sure to use the file provided by the vendor.

- **Enable and run DHCP service**



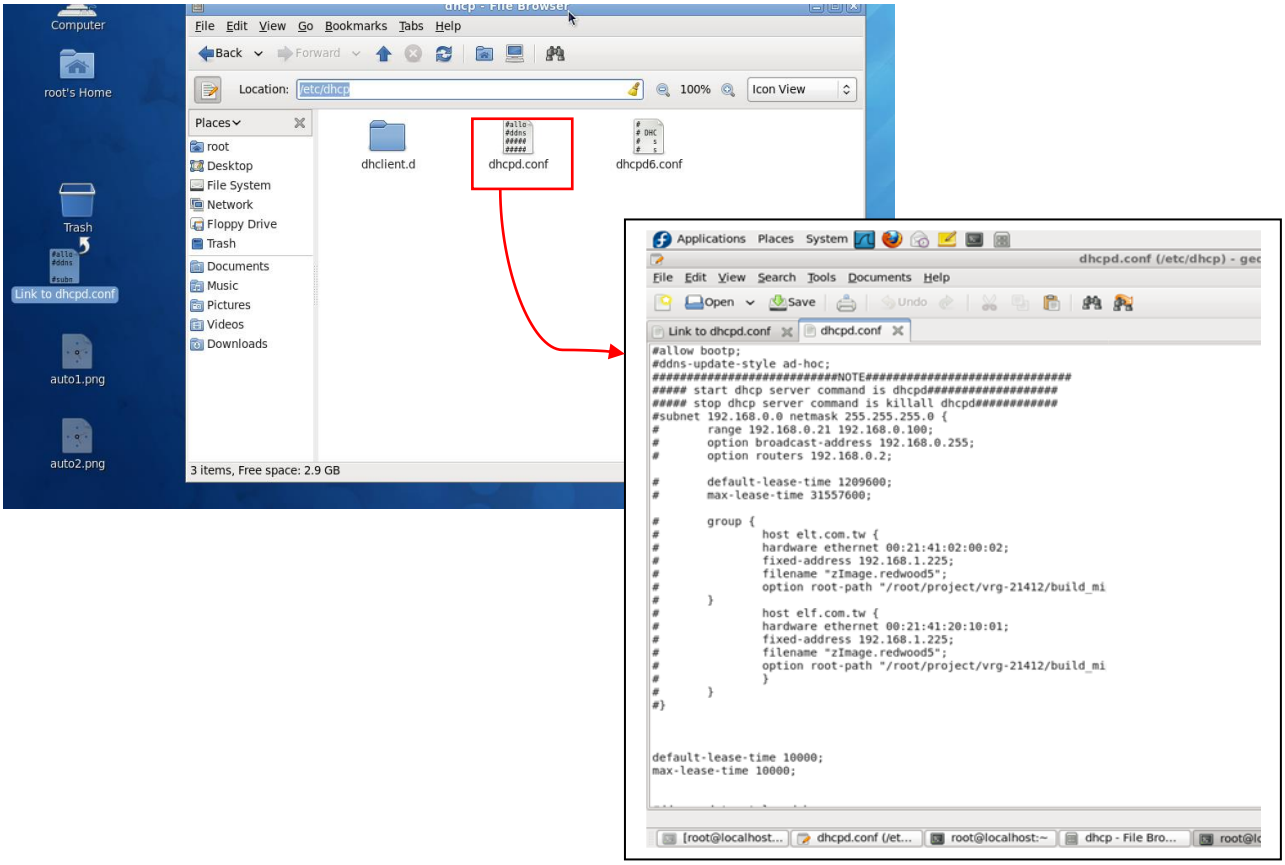
1. Choose dhcpd.
2. Enable DHCP service.
3. Start running DHCP service.

NOTE: *DHCP service can also be enabled by CLI. Issue "dhcpd" command to enable DHCP service.*



Step 3. Modify dhcpd.conf file

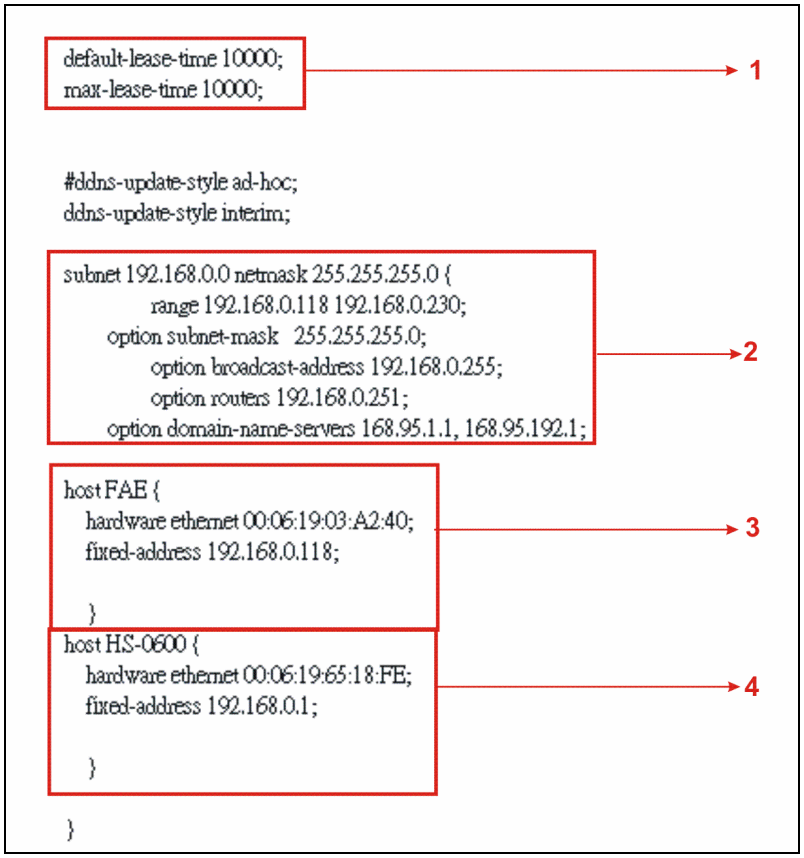
- **Open dhcpd.conf file in /etc/dhcp/ directory**



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.



1. Define DHCP default and maximum lease time in seconds.

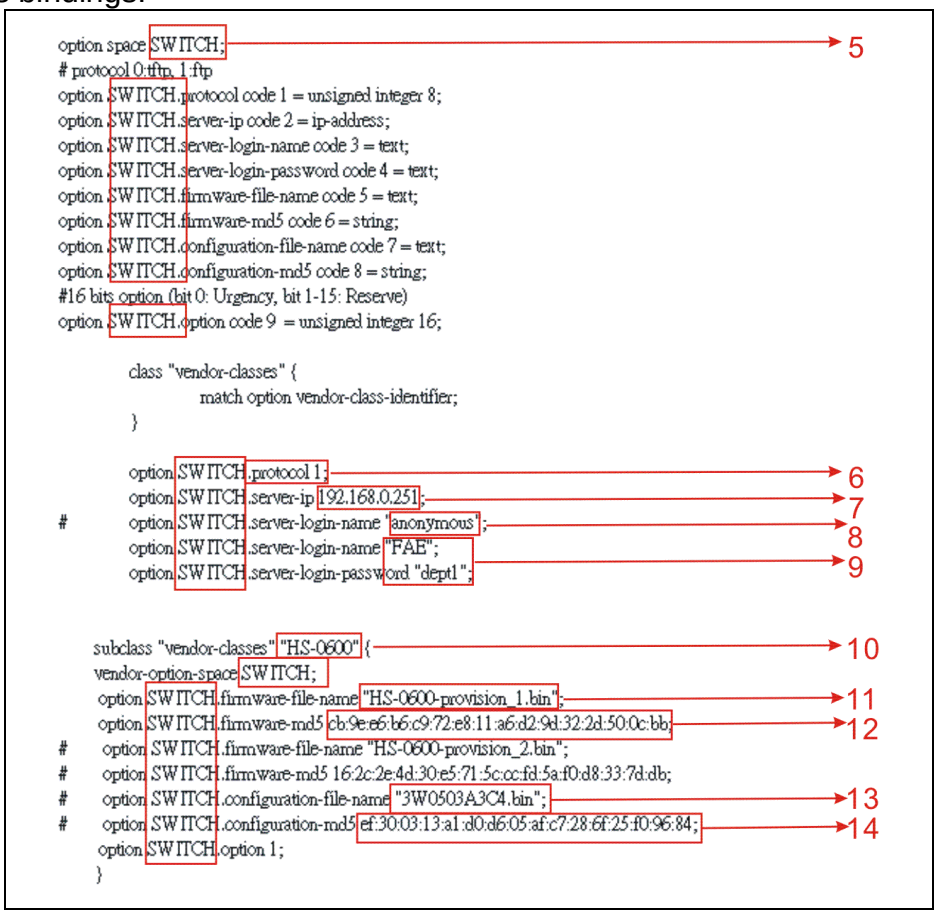
   Default lease time: If a client does not request a specific IP lease time, the server will assign a default lease time value.

   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.

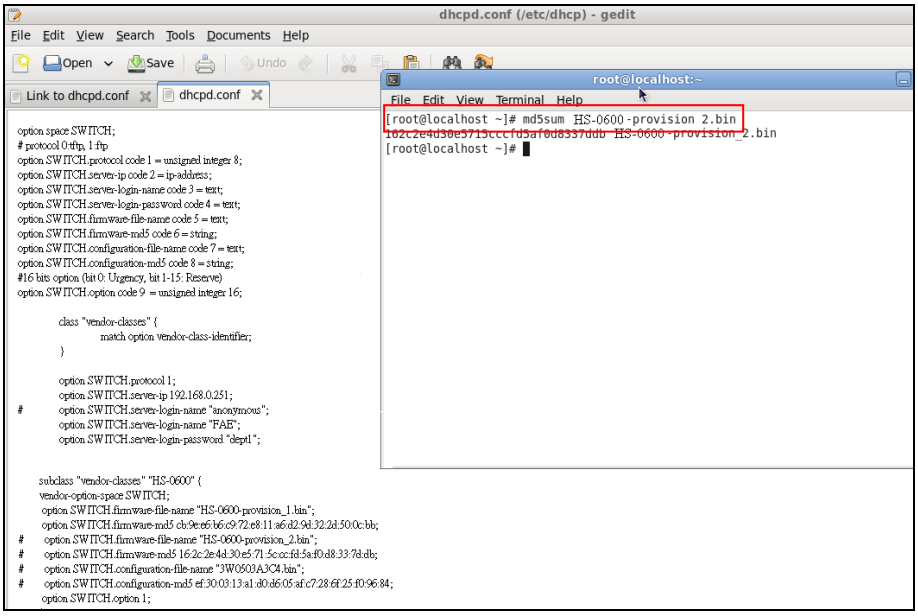
4. Map a host's MAC address to a fixed IP address. Use the same format to create multiple MAC-to-IP address bindings.



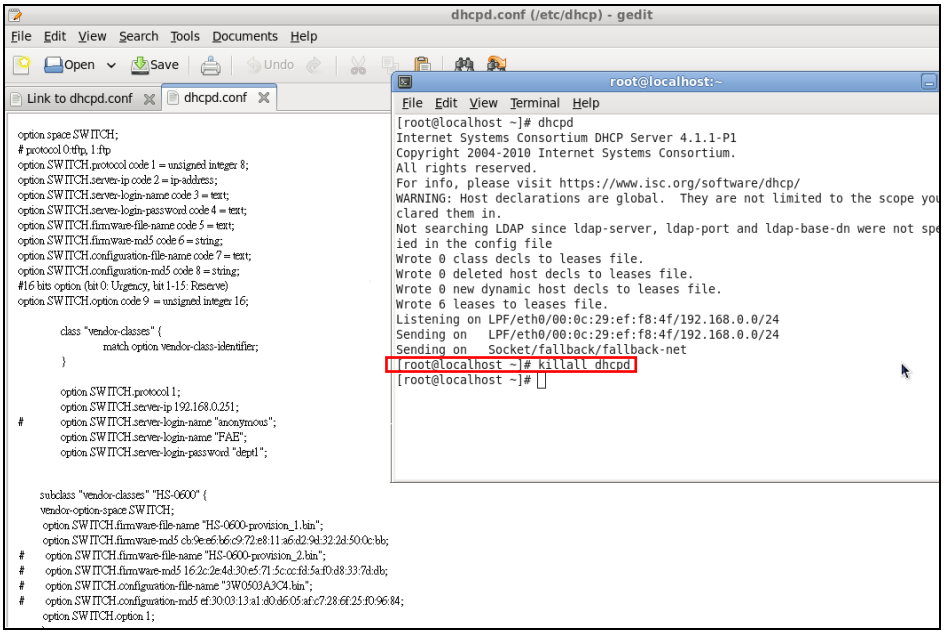
5. This value is configurable and can be defined by users.
6. Specify the protocol used (Protocol 1: FTP; Protocol 0: TFTP).
7. Specify the FTP or TFTP IP address.
8. Login TFTP server anonymously (TFTP does not require a login name and password).
9. Specify FTP Server login name and password.
10. Specify 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.

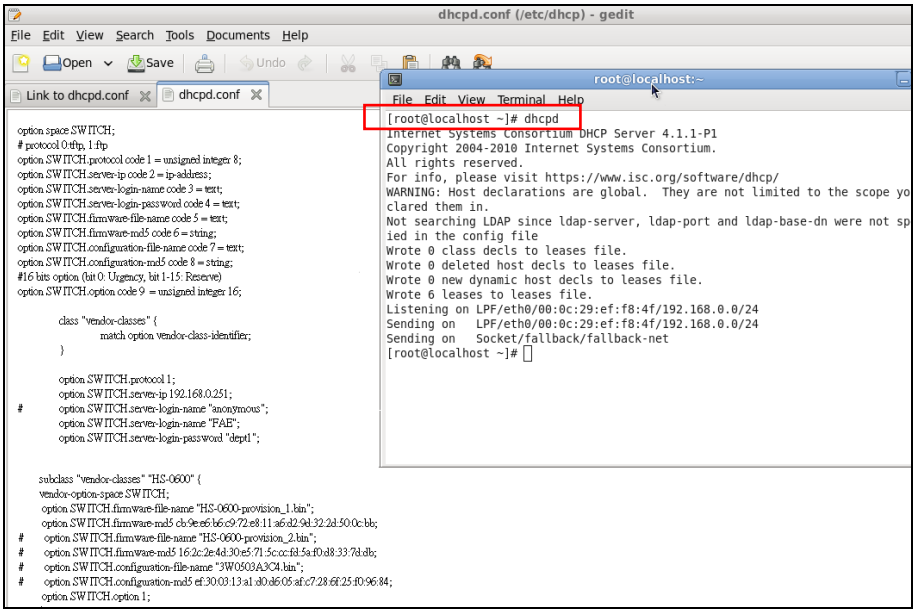
NOTE 1: *The text beginning with a pound sign (#) will be ignored by the DHCP server. For example, in the figure shown above, firmware-file-name "HS-0600-provision_2.bin" and firmware-md5 (line 5 & 6 from the bottom) will be ignored. If you want DHCP server to process these two lines, remove pound signs 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.*



- **Restart DHCP service**





Every time when 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. This is because that 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 causing the device to reboot endless.

In order for your Managed Switch to 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 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

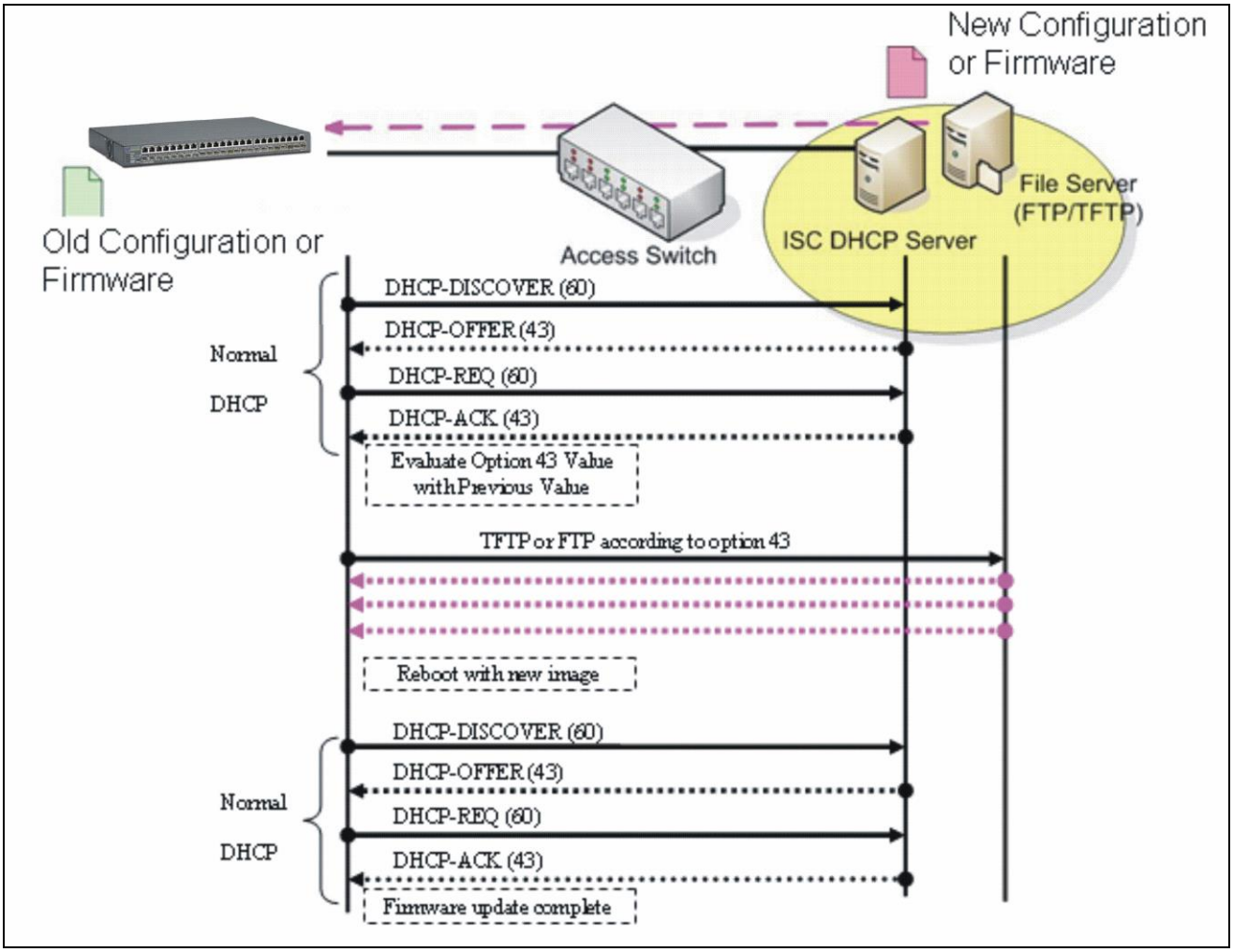
The TFTP/FTP File server should include the following items:

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. The ISC DHCP server will recognize the device whenever it sends an IP address request to it, 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 when 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 right after.
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 C: VLAN Application Note

(Take FOS-5128 as example: 24-port 100/1000Base-X SFP + 4-port 1/10GBase-R SFP+ Managed Fiber Access Switch)

Overview

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme instead of the physical layout. It can be used to combine any collection of LAN segments into a group that appears as a single LAN so as to logically segment 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.

Generally, end nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. In this way, the use of VLANs can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another VLAN. This allows VLAN to accommodate network moves, changes and additions with the utmost flexibility.

The Managed Switch supports Port-based VLAN implementation and IEEE 802.1Q standard tagging mechanism that enables the switch to differentiate frames based on a 12-bit VLAN ID (VID) field. Besides, the Managed Switch also provides double tagging function. The IEEE 802.1Q double tagging VLAN is also referred to Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1Q VLAN space by tagging the inner tagged packets. In this way, a "double-tagged" frame is created so as to separate customer traffic within a service provider network. Moreover, the addition of double-tagged space increases the number of available VLAN tags which allow service providers to use a single SP-VLAN (Service Provider VLAN) tag per customer over the Metro Ethernet network.

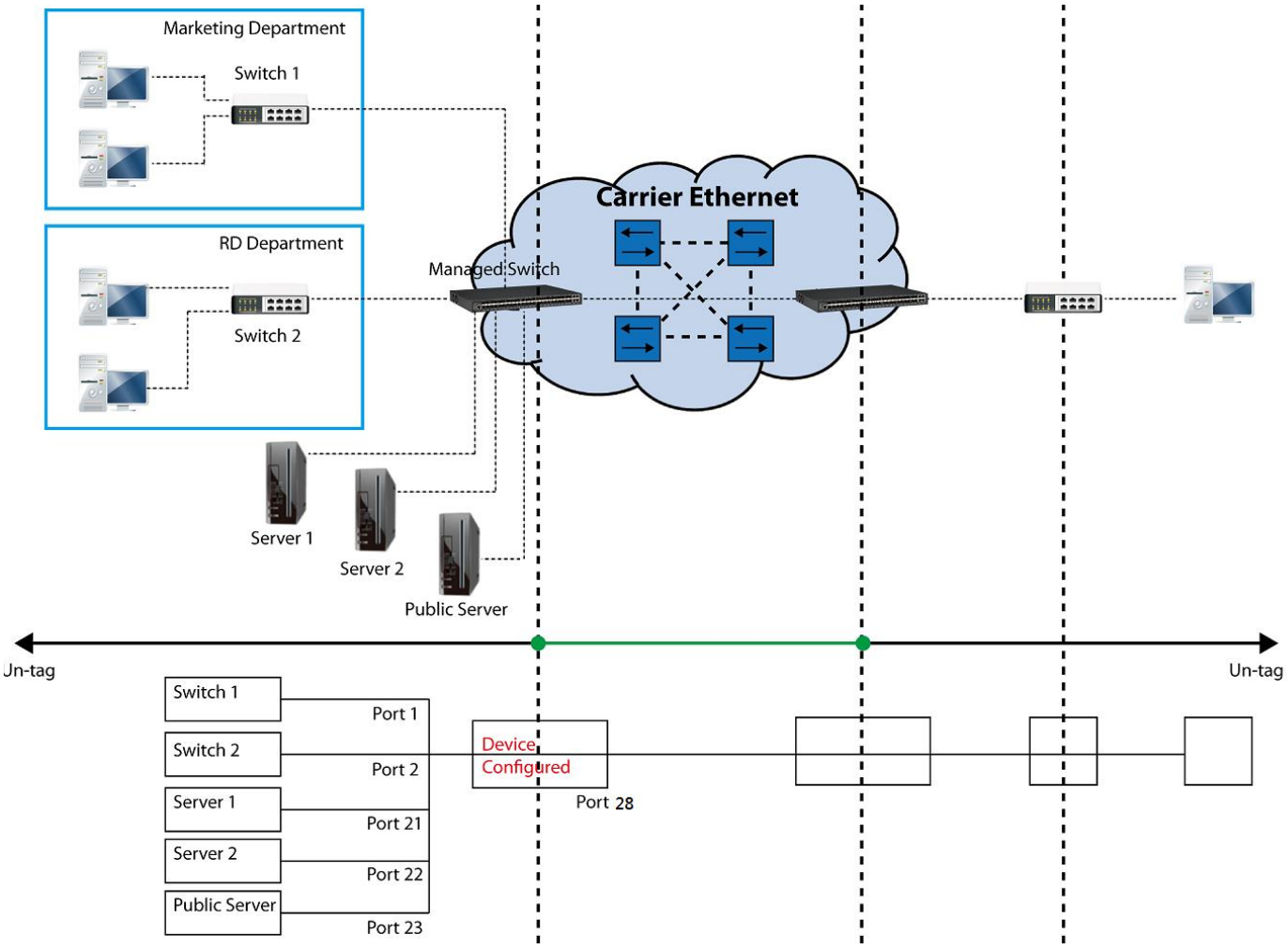
While this application note can not cover all of the real-life applications that are possible on this Managed Switch, it does provide the most common applications largely deployed in most situations. In particular, this application note provides a couple of network examples to help users implement Port-Based VLAN, Data VLAN, Management VLAN and Double-Tagged VLAN. Step-by-step configuration instructions using CLI and Web Management on setting up these examples are also explained. Examples described below include:

Examples	Configuration Procedures	
I. Port-Based VLAN	CLI	WEB
II. Data VLAN	CLI	WEB
III. Management VLAN	CLI	WEB
IV. Q-in-Q	CLI	WEB

I. Port-Based VLAN

Port-Based VLAN is uncomplicated in implementation and is useful for network administrators who wish to quickly and easily set up VLANs to isolate the effect of broadcast packets on their network. In the network diagram provided below, the network administrator is required to set up VLANs to separate traffic based on the following design conditions:

- Switch 1 is used in the Marketing Department to provide network connectivity to client PCs or other workstations. Switch 1 also connects to Port 1 in Managed Switch.
- Client PCs in the Marketing Department can access the Server 1 and Public Server.
- Switch 2 is used in the RD Department to provide network connectivity to Client PCs or other workstations. Switch 2 also connects to Port 2 in Managed Switch.
- Client PCs in the RD Department can access the Server 2 and Public Server.
- Client PCs in the Marketing and RD Department can access the Internet.



Port-Based VLAN Network Diagram

Based on design conditions described above, port-based VLAN assignments can be summarized in the table below.

VLAN Name	Member ports
Marketing	1, 21, 23, 28
RD	2, 22, 23, 28

CLI Configuration:

Steps…	Commands…

1. Enter Global Configuration mode.	`Switch> enable`
	`Password:`
	`Switch#config`
	`Switch(config)#`

2. Create port-based VLANs “Marketing” and “RD”	`Switch(config)# vlan port-based Marketing`
	`OK !`
	`Switch(config)# vlan port-based RD`
	`OK !`

3. Select port 1, 21, 23 and 28 to configure.	`Switch(config)# interface 1,21,23,28` `Switch(config-if-1,21,23,28)#`
4. Assign the ports to the port-based VLAN “Marketing”.	`Switch(config-if-1,21,23,28)# vlan port-based Marketing` `OK !`

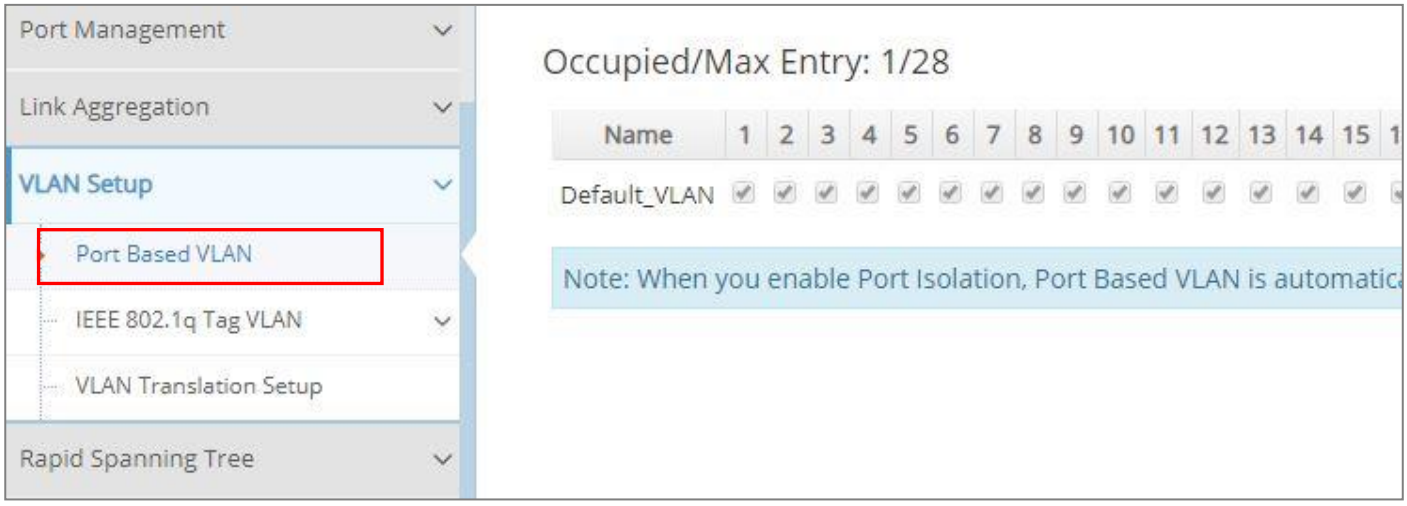
5. Return to Global Configuration mode, and select port 2, 22, 23 and 28 to configure.	`Switch(config-if-1,21,23,28)# exit`
	`Switch(config)# interface 2,22,23,28`
	`Switch(config-if-2,22,23,28)#`

6. Assign the ports to the port-based VLAN “RD”.	`Switch(config-if-2,22,23,28)# vlan port-based RD` `OK !`

7. Return to Global Configuration mode, and show currently configured port-based VLAN membership.	`Switch(config-if-2,22,23,28)# exit`
	`Switch(config)# show vlan port-based`
	`When you enable Port Isolation, Port Based VLAN is automatically invalid.`
	`==========`
	`Port Based VLAN :`
	`==========`
	`Name  Port Member`
	`----------  ----------`
	`Default_VLAN  1-28,CPU`
	`Marketing  1,21,23,28`
	`RD  2,22,23,28`
	
	Note: By default, all ports are member ports of the Default_VLAN. Before removing the Deafult_VLAN from the VLAN table, make sure you have correct management VLAN and VLAN mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.

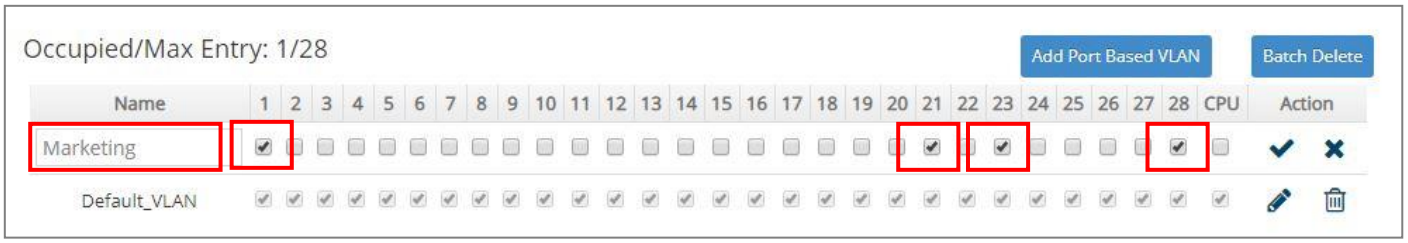
Web Management Configuration:

1. **Select “Port Based VLAN” option in VLAN Setup menu.**
   VLAN Setup > Port Based VLAN



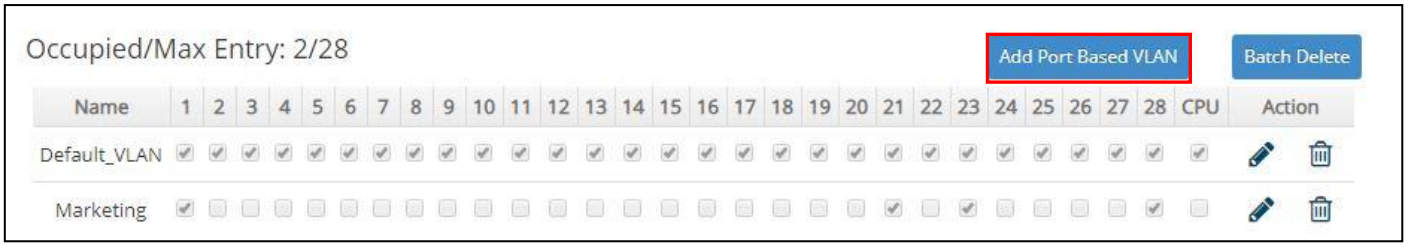
2. **Click “Add Port Based VLAN” to add a new Port-Based VLAN**
   VLAN Setup>Port Based VLAN>Add Port Based VLAN

3. **Add Port 1, 21, 23 and 28 in a group and name it to “Marketing”.**
   VLAN Setup>Port Based VLAN>Add Port Based VLAN

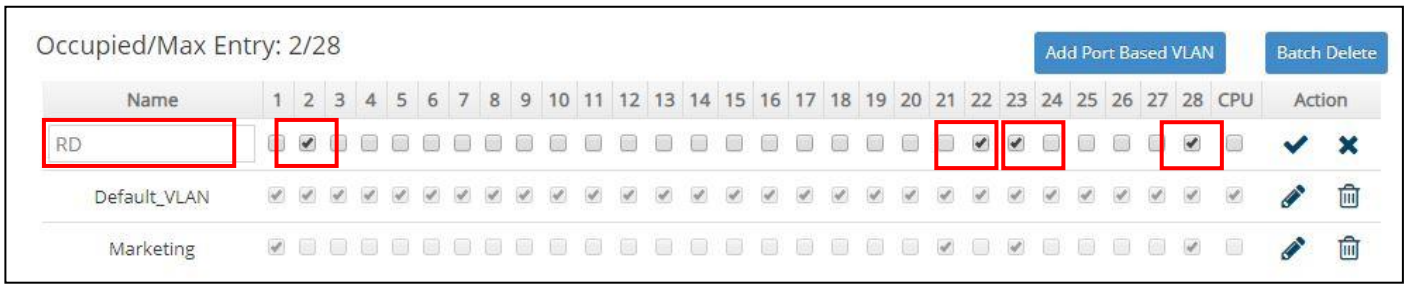


Click ✔ to apply the new settings when completing.

4. **Click “Add Port Based VLAN” again to add a new Port-Based VLAN.**
   VLAN Setup>Port Based VLAN> Add Port Based VLAN

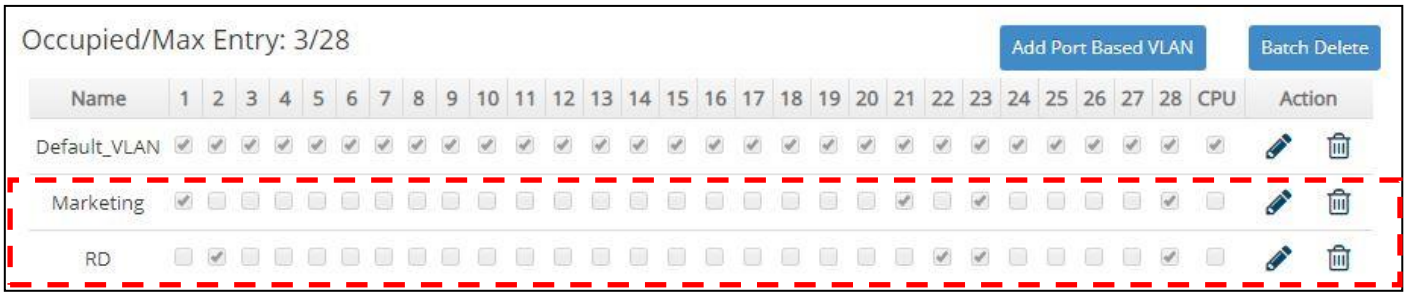


5. **Add Port 2, 22, 23 and 28 in a group and name it to "RD".**
   VLAN Setup>Port Based VLAN>Add Port Based VLAN



Click ✔ to apply the new settings when completing.

6. **Check Port-Based VLAN settings.**
   VLAN Setup>Port Based VLAN



NOTE: *By default, all ports are member ports of the Default_VLAN. Before removing the Deafult_VLAN from the VLAN table, make sure you have correct management VLAN and VLAN mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.*

Treatments of packets:

1. A untagged packet arrives at Port 1
Untagged packets received on the Managed Switch will be forwarded out untagged. Therefore, in this example, the Managed Switch will look at the Port-Based forwarding table for Port 1 and forward untagged packets to member port 21, 23, and 28.

2. A untagged packet arrives at Port 2
Untagged packets received on the Managed Switch will be forwarded out untagged. Therefore, in this example, the Managed Switch will look at the Port-Based forwarding table for Port 2 and forward untagged packets to member port 22, 23, and 28.

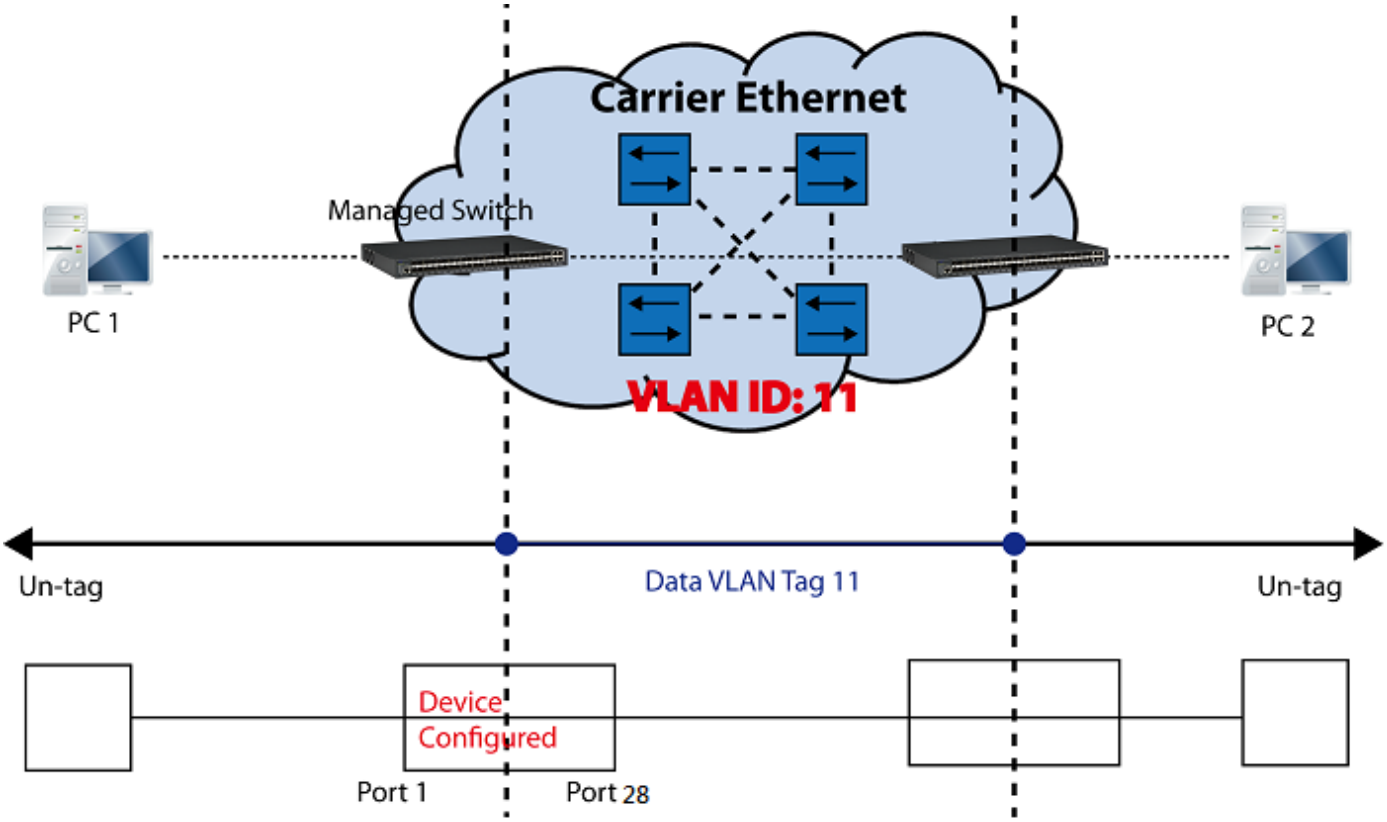
3. A tagged packet with any permissible VID arrives at Port 1
Tagged packets received on the Managed Switch will be forwarded out tagged. Therefore, in this example, the Managed Switch will look at the Port-Based forwarding table for Port 1 and forward tagged packets to member port 21, 23, and 28.

4. A tagged packet with any permissible VID arrives at Port 2
Tagged packets received on the Managed Switch will be forwarded out tagged. Therefore, in this example, the Managed Switch will look at the Port-Based forwarding table for Port 2 and forward tagged packets to member port 22, 23, and 28.

II. Data VLAN

In networking environment, VLANs can carry various types of network traffic. The most common network traffic carried in a VLAN could be voice-based traffic, management traffic and data traffic. In practice, it is common to separate voice and management traffic from data traffic such as files, emails. Data traffic only carries user-generated traffic which is sometimes referred to a user VLAN and usually untagged when received on the Managed Switch.

In the network diagram provided, it depicts a data VLAN network where PC1 wants to ping PC2 in a remote network. Thus, it sends out untagged packets to the Managed Switch to be routed in Carrier Ethernet. For this example, IEEE 802.1Q tagging mechanism can be used to forward data from the Managed Switch to the destination PC.



Data VLAN Network Diagram

CLI Configuration:

Steps…	Commands…

1. Enter Global Configuration mode.	`Switch> enable`
	`Password:`
	`Switch#config`
	`Switch(config)#`

2. Create VLAN 11 and assign Port 1 and Port 28 to VLAN 11.	`Switch(config)# interface 1,28`
	`Switch(config-if-1,28)# vlan dot1q-vlan trunk-vlan 11`
	`OK !`
	`Switch(config-if-1,28)# exit`

3. Name VLAN 11 as “DataVLAN”.	`Switch(config)# vlan dot1q-vlan 11`
	`Switch(config-vlan-11)# name DataVLAN`
	`OK !`
	`Switch(config-vlan-11)# exit`

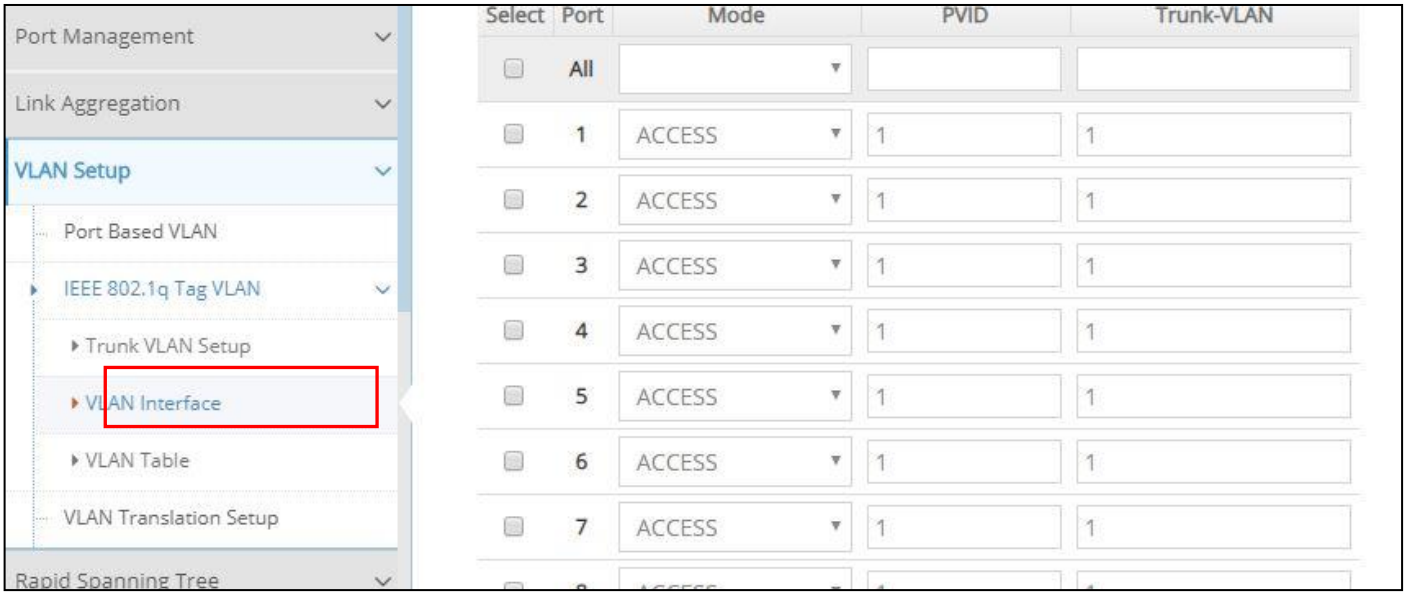
4. Set Port 28 to trunk mode.	`Switch(config)# interface 28`
	`Switch(config-if-28)# vlan dot1q-vlan mode trunk`
	`OK !`
	`Switch(config-if-28)# exit`

5. Change Port 1's Access VLAN ID into "11".	`Switch(config)# interface 1`
	`Switch(config-if-1)# vlan dot1q-vlan pvid 11`
	`OK !`
	`Switch(config-if-1)# exit`

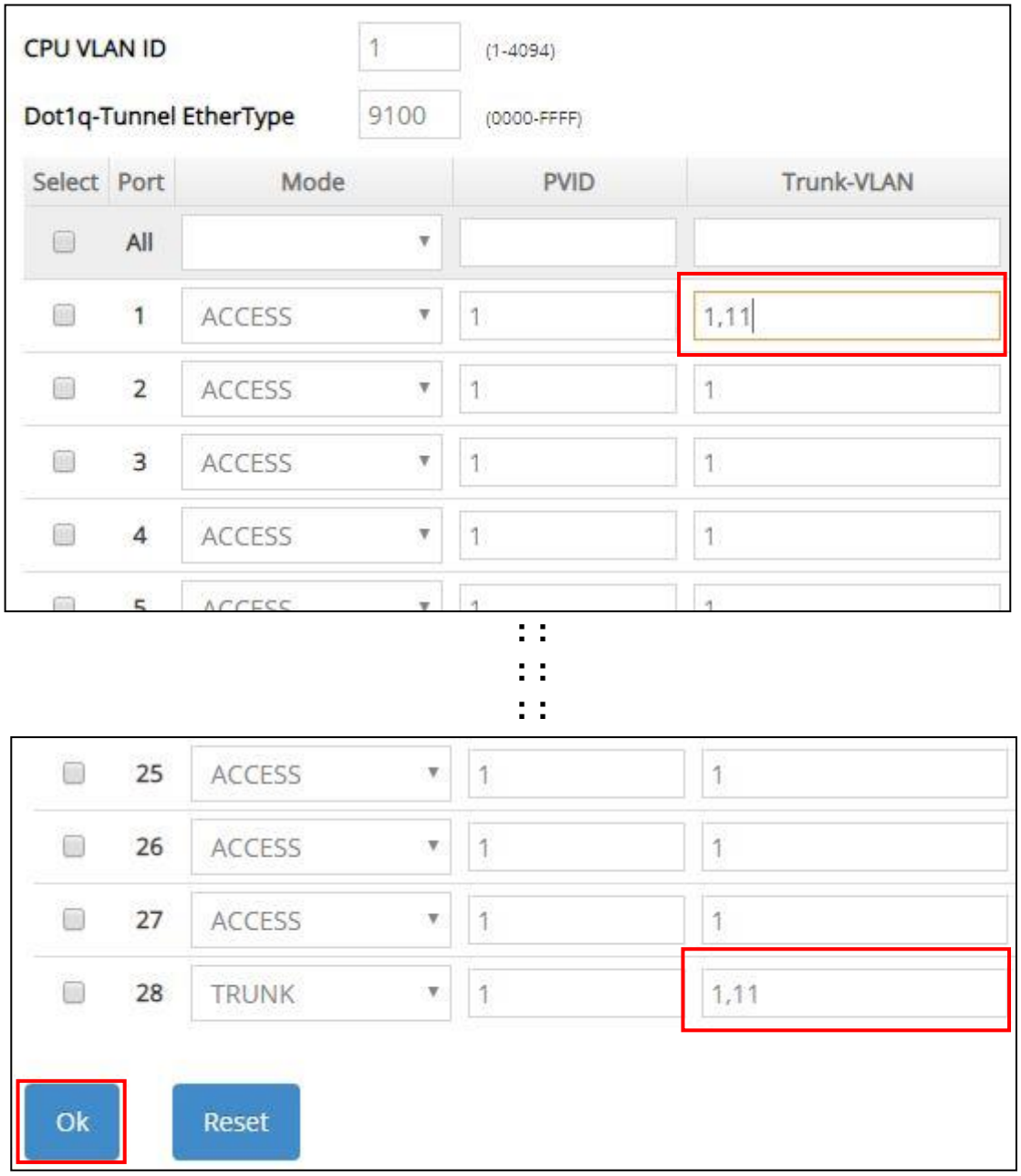
6. Show currently configured VLAN tag settings.	`Switch(config)# show vlan interface`
	
	`==========`
	`IEEE 802.1q Tag VLAN Interface`
	`==========`
	`CPU VLAN ID : 1`
	`Dot1q-Tunnel EtherType : 0x9100`
	
	`Port P-Bit Port VLAN Mode PVID Trunk-vlan`
	`---- ----- ---------- ---- ----------`
	`1 0 access 11 1,11`
	`2 0 access 1 1`
	`3 0 access 1 1.`
	`.`
	`.`
	`26 0 access 1 1`
	`27 0 access 1 1`
	`28 0 trunk 1 1,11`

Web Management Configuration:

1. **Select "VLAN Interface" option in IEEE 802.1q Tag VLAN menu.**
   VLAN Setup>IEEE 802.1q Tag VLAN>VLAN Interface

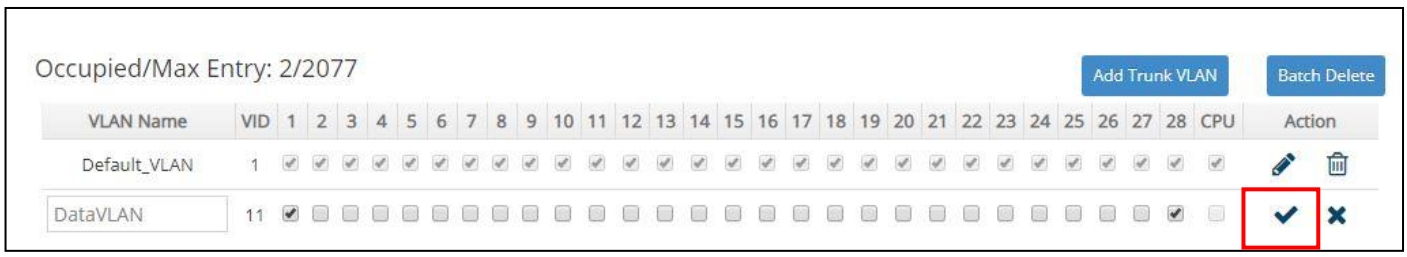


2. **Create a new Data VLAN 11 that includes Port 1 and Port 28 as members.**
   VLAN Setup>IEEE 802.1q Tag VLAN>VLAN Interface



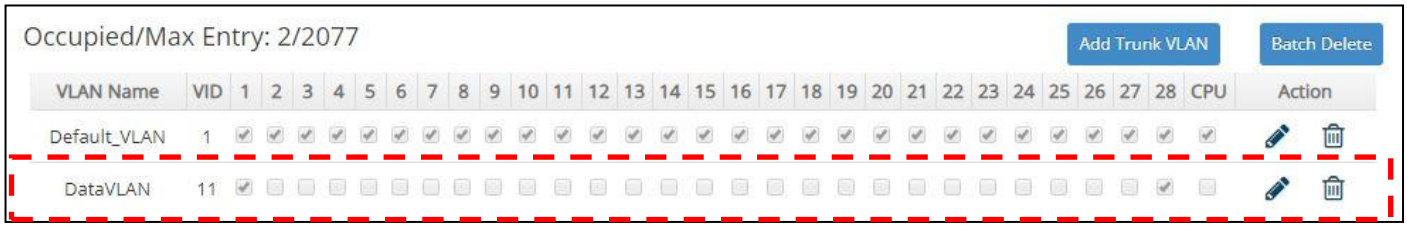
   Click **OK** to apply the new settings when completing..

3. **Click icon belonging to the new Trunk VLAN 11 named VLAN0011, and the following screen shows up. Rename this new Trunk VLAN 11 as "DataVLAN" that includes Port 1 and 28 as member ports.**
   VLAN Setup>IEEE 802.1q Tag VLAN>Trunk VLAN Setup

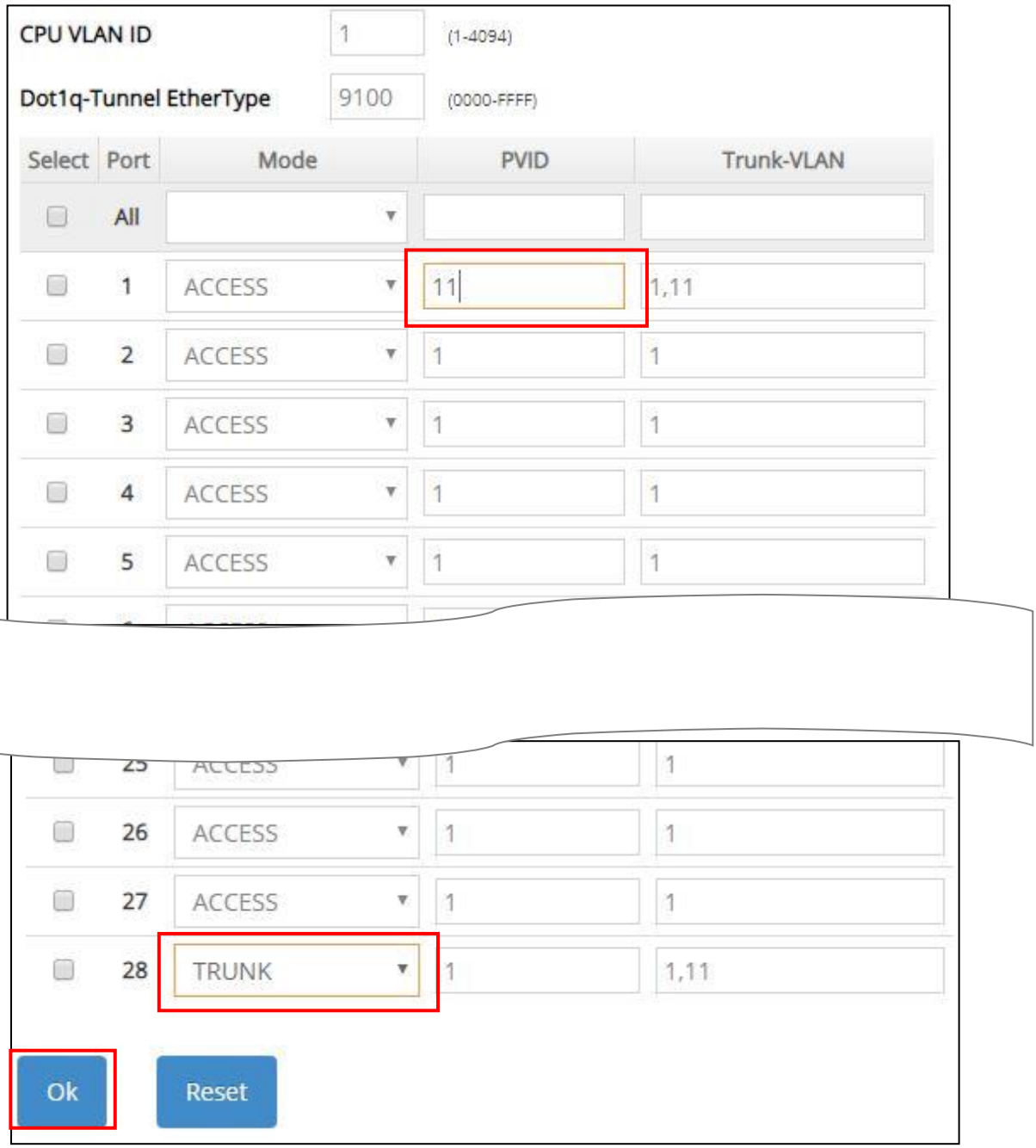


   Click to apply the new settings when completing.

4. **Check Trunk VLAN 11 settings.**
   VLAN Setup>IEEE 802.1q Tag VLAN>Trunk VLAN Setup



5. **Change Port 1's Access VLAN ID into 11, and set Port 28 to trunk mode.**
   VLAN Setup>IEEE 802.1q Tag VLAN>VLAN Interface



Click **OK** to apply the new settings when completing.

Treatments of Packets:

1. A untagged packet arrives at Port 1
When an untagged packet arrives at Port 1, Port 1's Port VLAN ID (11) will be added to the original port. Because Port 28 is configured as a trunk port, it will forward the packet with tag 11 out to the Carrier Ethernet.

2. A tagged packet arrives at Port 1
In most situations, data VLAN will receive untagged packets sent from the client PC or workstation. If tagged packets are received (possibly sent by malicious attackers), they will be dropped.

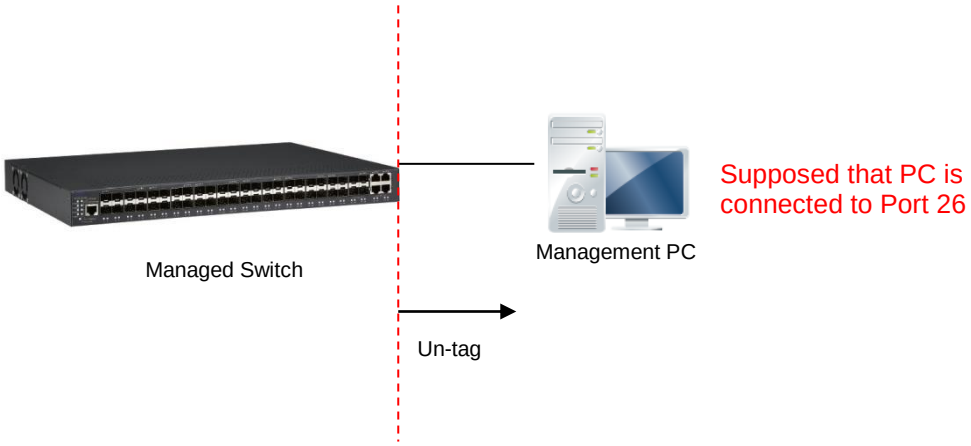
III. Management VLAN

For security and performance reasons, it is best to separate user traffic and management traffic. When Management VLAN is set up, only a host or hosts that is/are in this Management VLAN can manage the device; thus, broadcasts that the device receives or traffic (e.g. multicast) directed to the management port will be minimized.

Web Management Configuration (Access Mode):

Supposed that we have the default Management VLAN whose VLAN ID is 1 for all ports, we can create new Management VLANs as required. This example is to demonstrate how to set up Management VLAN from 15 to 20 on specified ports under Access mode.

In **Management VLAN Network Diagram**, the management PC on the right would like to manage the Managed Switch on the left directly. You can follow the steps described below to set up the Management VLAN.



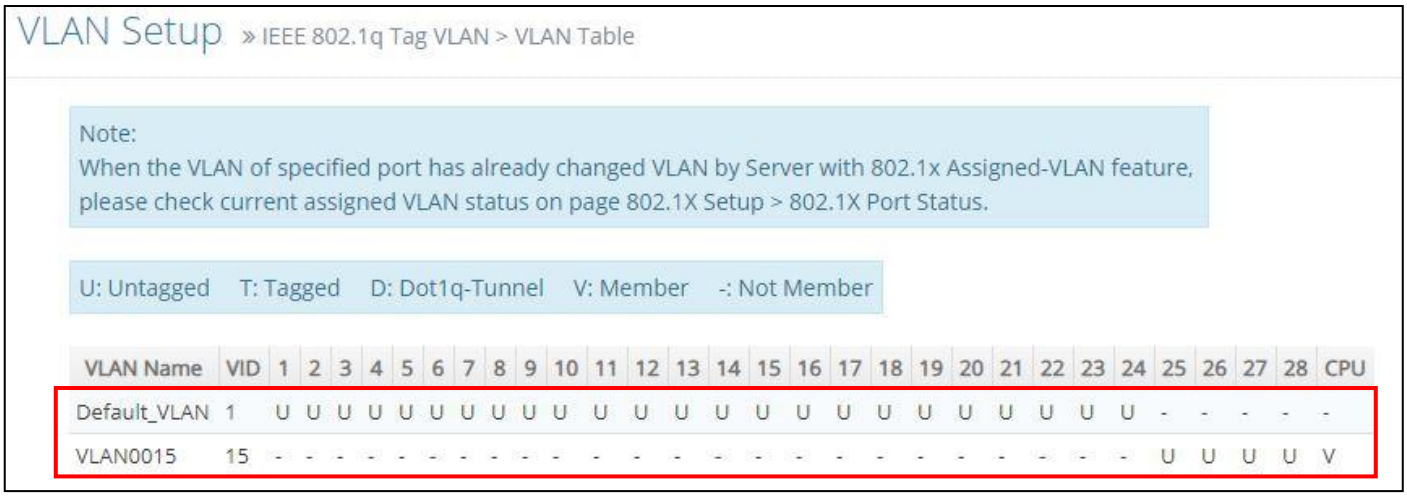
Management VLAN Network Diagram

1. **Change the Management default VLAN 1 into VLAN 15 that includes Port 25, 26, 27 and 28 under the Access mode.**
   VLAN Setup>IEEE 802.1q Tag VLAN>VLAN Interface

Click **OK** to apply the new settings when completing.

Note1: *Make sure you have correct management VLAN and VLAN Mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you click **OK** to apply.*

Note2: *To check the current status of Management VLAN, please refer to* ***VLAN Table****.*

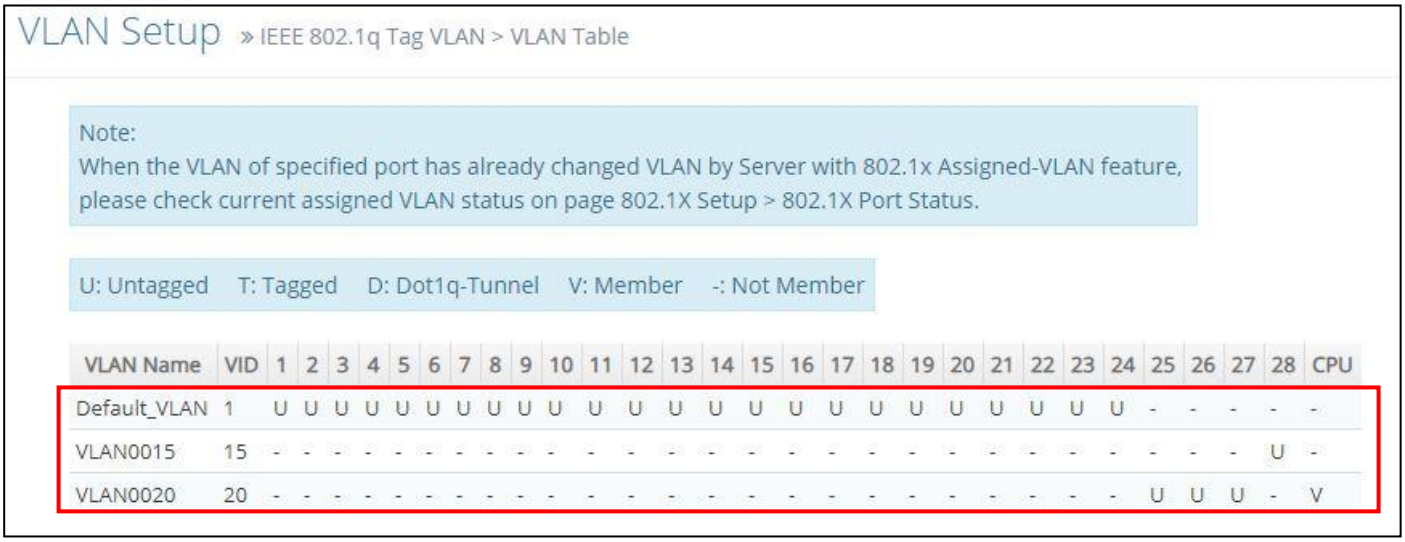


2. Now, change the Management VLAN 15 into VLAN 20 and includes Port 25, 26 and 27 under Access mode (It's necessary to include Port 26 to prevent the disconnection.)

VLAN Setup>IEEE 802.1q Tag VLAN>VLAN Interface

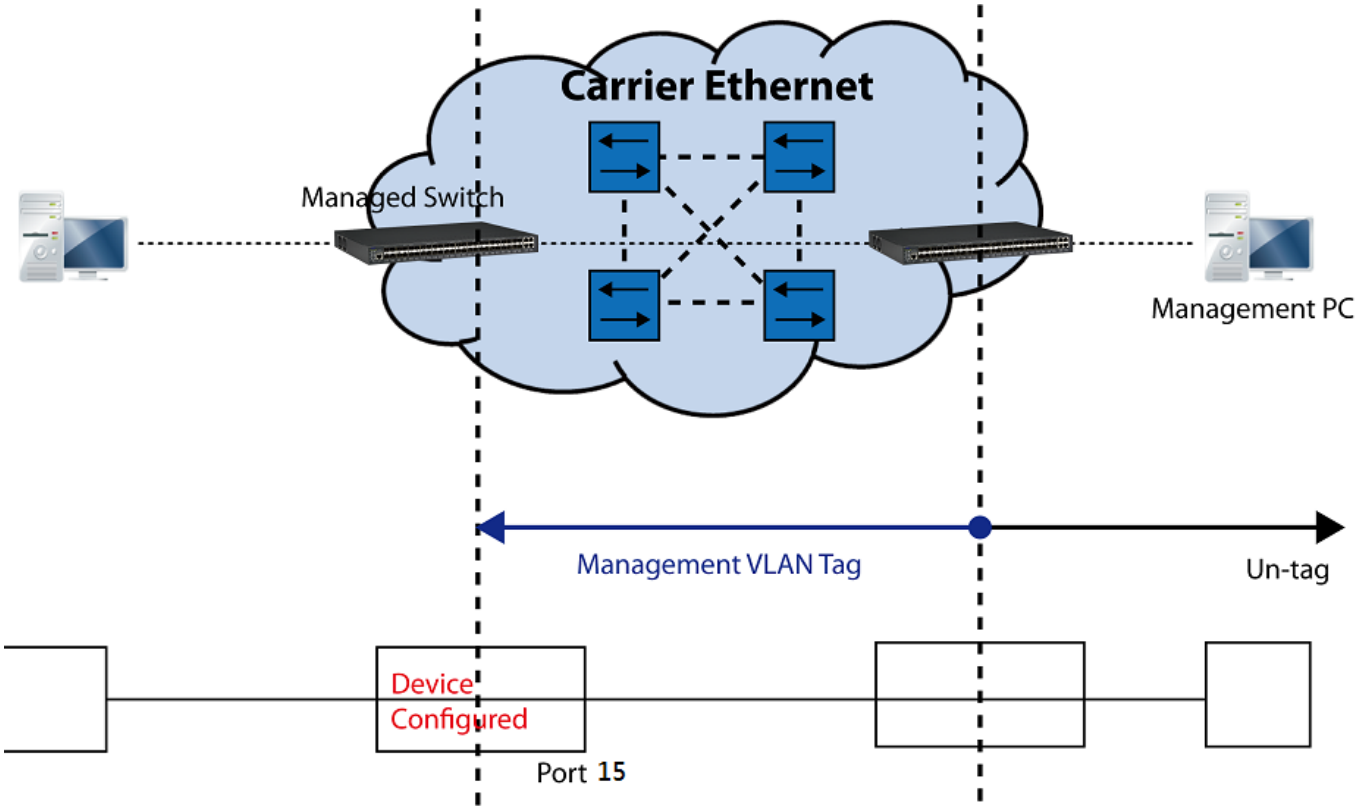
Click **OK** to apply the new settings when completing..

Note: *To check the current status of Management VLAN, please refer to* ***VLAN Table****.*



Web Management Configuration (Trunk Mode):

In **Management VLAN Network Diagram** shown below, the management PC on the right would like to manage the Managed Switch on the left remotely. You can follow the steps described below to set up the Management VLAN.



Management VLAN Network Diagram

Supposed that the Management PC is remotely connected to Managed Switch Port 15 as shown above while we have a variety of existing trunk vlan and the Management VLAN 15 is set on Port 25,26,27,28 and CPU as shown below. We can create new Management VLAN 20 as required.

This part is to demonstrate how to set up from Management VLAN 15 to VLAN 20 on specified ports under Trunk mode.

VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	CPU
Default_VLAN	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	-	U	U	U	U	U	U	U	U	U	-	-	-	-	-
VLAN0015	15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	U	-	-	-	-	-	-	-	-	-	T	T	T	T	V

IEEE 802.1q Tag VLAN Table

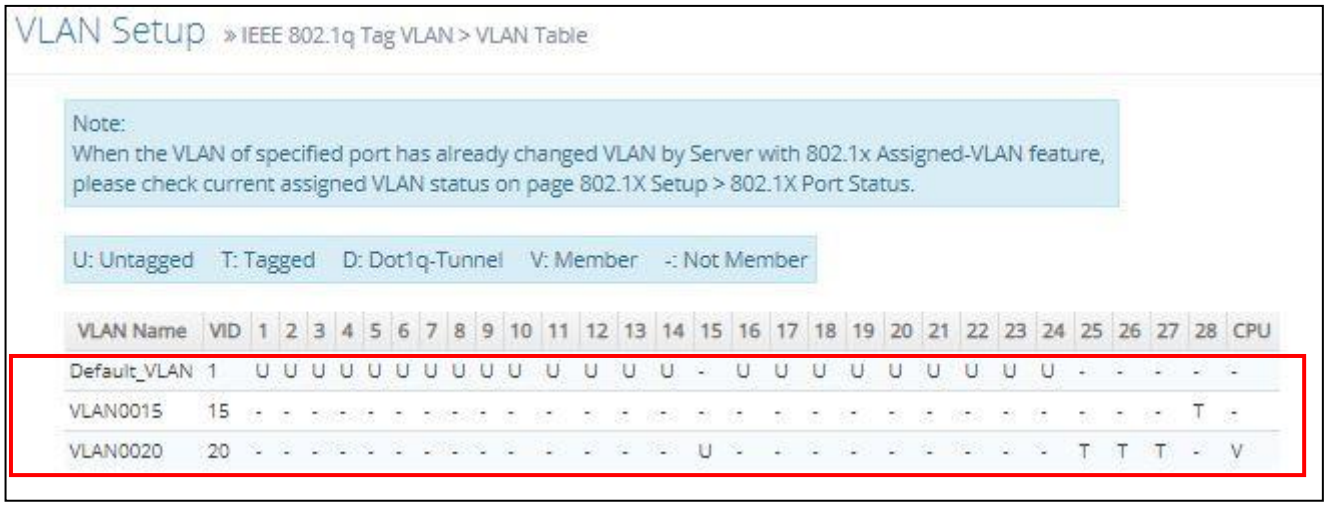
1. Change the Management VLAN 15 into VLAN 20 that includes Port 25, 26, 27 under Trunk mode.

Click **OK** to apply the new settings when completing.

Note1: *Make sure you have correct management VLAN and VLAN Mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you click* ***OK*** *to apply.*

Note2: *To check the current status of Management VLAN, please refer to* ***VLAN Table****.*

Then, Management VLAN has been changed into VLAN 20.



CLI Configuration (Access Mode):

Supposed that we have the default Management VLAN whose VLAN ID is 1 for all ports, we can create new Management VLANs as required. This example is to demonstrate how to set up Management VLAN 15 and then change VLAN 15 into VLAN 20 on specified ports under Access mode. Here, we supposed that the Management PC is remotely connected to Managed Switch Port 26.

1. Change the Management default VLAN 1 into VLAN 15 that includes Port 25, 26, 27 and 28 under Access mode.

Steps…	Commands…

1. Enter Global Configuration mode.	`Switch> enable`
	`Password:`
	`Switch# configure`
	`Switch(config)#`

2. Assign VLAN 15 to Management VLAN and Port 25-28 to Management port.	`Switch(config)# vlan management-vlan 15 management-port 25-28 mode access`
	`OK !`
	
	NOTE: Make sure you have correct management VLAN and VLAN mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.

3. Show currently configured dot1q settings and check CPU has been a member port in Management VLAN 15.	Switch(config)# show vlan ========== IEEE 802.1q VLAN Table ========== CPU VLAN ID : 15 Management Priority : 0 U: untagged port, T: tagged port, D: dot1q-tunnel port, V: member port ---------- VLAN Name VLAN 1 8 9 16 17 24 2528 CPU --- --- --- --- --- --- --- Default_VLAN 1 UUUUUUUU UUUUUUUU UUUUUUUU ---- - VLAN0015 15 -------- -------- -------- UUUU V

2. Now, change the Management VLAN 15 into VLAN 20 and includes Port 25, 26 and 27 to Access mode (It's necessary to include Port 26 to prevent the disconnection.)

Steps…	Commands…
1. Enter Global Configuration mode.	Switch> enable Password: Switch# configure Switch(config)#
2. Assign VLAN 20 to Management VLAN and Port 25-27 to Management port.	Switch(config)# vlan management-vlan 20 management-port 25-27 mode access OK ! **NOTE:** Make sure you have correct management VLAN and VLAN mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.
3. Show currently configured dot1q settings and check CPU has been a member port in Management VLAN 20.	Switch(config)# show vlan ========== IEEE 802.1q VLAN Table ========== CPU VLAN ID : 20 Management Priority : 0 U: untagged port, T: tagged port, D: dot1q-tunnel port, V: member port ---------- VLAN Name VLAN 1 8 9 16 17 24 2528 CPU --- --- --- --- --- --- --- Default_VLAN 1 UUUUUUUU UUUUUUUU UUUUUUUU ---- - VLAN0015 15 -------- -------- -------- ---U - VLAN0020 20 -------- -------- -------- UUU- V

CLI Configuration(Trunk Mode):

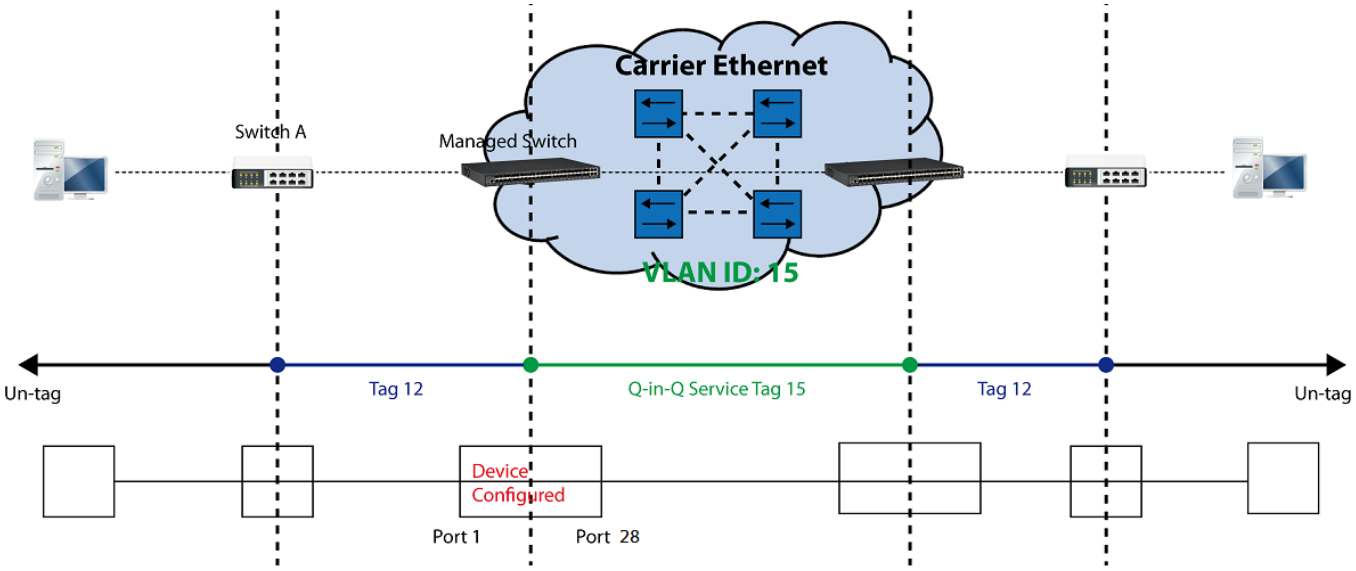
This part is to demonstrate how to change Management VLAN 15 into VLAN 20 on specified ports under Trunk mode. Supposed that we have the existing Management VLAN 15 on Port 25,26,27,28 and CPU, we can create new Management VLAN 20 as required. Here, we supposed that the Management PC is remotely connected to Managed Switch Port 15.

1. Change the Management VLAN 15 into VLAN 20 that includes Port 25, 26, 27 under Trunk mode.

Steps…	Commands…
1. Enter Global Configuration mode.	Switch> enable Password: Switch# configure Switch(config)#
2. Assign VLAN 20 to Management VLAN and Port 15 to Management port for the access of the Managed Switch.	Switch(config)# vlan management-vlan 20 management-port 15 mode access OK ! **NOTE:** Make sure you have correct management VLAN and VLAN mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.
3. Assign VLAN 20 to Management VLAN and Port 25-27 to Management port.	Switch(config)# vlan management-vlan 20 management-port 25-27 mode trunk OK ! **NOTE:** Make sure you have correct management VLAN and VLAN mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.
4. Show currently configured dot1q settings and check CPU has been a member port in Management VLAN 20.	Switch(config)# show vlan ========== IEEE 802.1q VLAN Table ========== CPU VLAN ID : 20 Management Priority : 0 U: untagged port, T: tagged port, D: dot1q-tunnel port, V: member port VLAN Name VLAN 1 8 9 16 17 24 2528 CPU ---------- ---- -------- -------- -------- ---- --- Default_VLAN 1 UUUUUUUU UUUUUU-U UUUUUUUU ---- - VLAN0015 15 -------- -------- -------- ---T - VLAN0020 20 -------- ------U- -------- TTT- V

IV. Q-in-Q

The IEEE 802.1Q double tagging VLAN is also referred to Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1q VLAN space by tagging the inner tagged packets. In this way, a “double-tagged” frame is created so as to separate customer traffic within a service provider network. As shown below, the network diagram depicts the Switch A (on the left) carries a Customer tag 12. When tagged packets are received on the Managed Switch, they should be tagged with an outer Service Provider tag 15. To set up the network as provided, you can follow the steps described below.



Q-in-Q VLAN Network Diagram

CLI Configuration:

Steps…	Commands…

1. Enter Global Configuration mode.	`Switch> enable`
	`Password:`
	`Switch#config`
	`Switch(config)#`

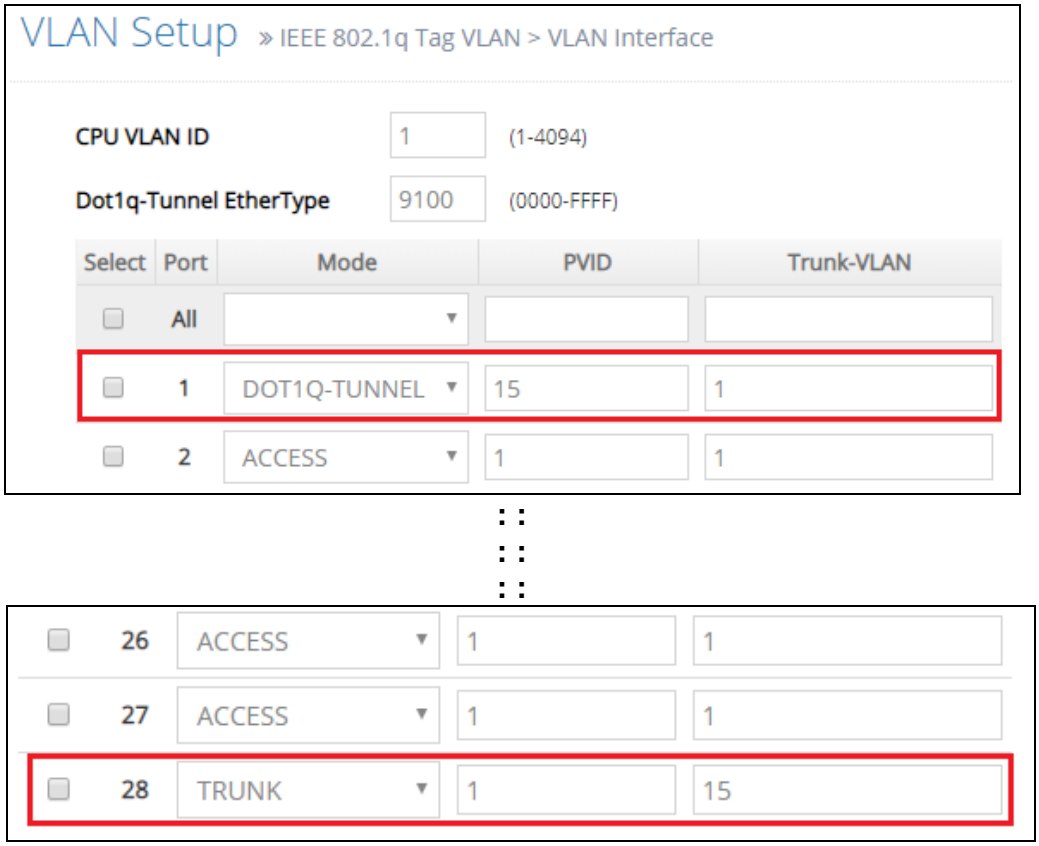
2. Create S-Tag 15 on Port 1.	`Switch(config)# interface 1`
	`Switch(config-if-1)# vlan dot1q-vlan mode dot1q-tunnel`
	`OK !`
	`Switch(config-if-1)# vlan dot1q-vlan pvid 15`
	`OK !`
	`Switch(config-if-1)# exit`

3. Create Port 28 to trunk port with 15 VLAN ID.	`Switch(config)# interface 28`
	`Switch(config-if-28)# vlan dot1q-vlan mode trunk`
	`OK !`
	`Switch(config-if-28)# vlan dot1q-vlan trunk-vlan 15`
	`OK !`
	`Switch(config-if-28)# no vlan dot1q-vlan trunk-vlan 1`
	`OK !`
	`Switch(config-if-28)# exit`

4. Show currently configured dot1q VLAN membership.	`Switch(config)# show vlan interface`
	`==========`
	`IEEE 802.1q Tag VLAN Interface`
	`==========`
	`CPU VLAN ID : 1`
	`Dot1q-Tunnel EtherType : 0x9100`
	
	`Port P-Bit Port VLAN Mode PVID Trunk-vlan`
	`---- ----- ---------- ---- ----------`
	`1 0 dot1q tunnel 15 1`
	`2 0 access 1 1`
	`. . .`
	`27 0 access 1 1`
	`28 0 trunk 1 15`
	
	NOTE: By default, all ports are member ports of the Default_VLAN. Before removing the Default_VLAN from the VLAN table, make sure you have correct management VLAN and VLAN mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.

Web Management Configuration:

1. **Select “VLAN Interface” option in IEEE 802.1Q Tag VLAN menu.**
   VLAN Setup>IEEE 802.1q Tag VLAN>VLAN Interface



   Check the VLAN status. Supposed that Port 1 carries dot1q-tunnel VLAN 15 while Port 28 trunk VLAN 15.

Treatments of Packets:

1. **A tagged packet arrives at Port 1**
   When a packet with a tag 12 arrives at Port 1, the original tag will be kept intact and then added an outer tag 15 by Port 1, which is set as a tunnel port. When this packet is forwarded to Port 28, two tags will be forwarded out because Port 28 is set as a trunk port.

2. **A untagged packet arrives at Port 1**
   If an untagged packet is received, it will also be added a tag 15. However, Q-in-Q function will not work.

APPENDIX D: SFP/SFP+ Port Threshold

Command & Configuration Guide

Version 1.0

Chapter 1. SFP/SFP+ Port Threshold
1.1 Introduction

CTS SFP/SFP+ ports of FOS-5-Series switch support alarm and warning thresholds for temperature (degrees C), voltage (V), current (mA), TX power (dBm) and RX power (dbm) commands that is easy troubleshooting for network manager when SFP/SFP+ transceiver has issue or prevent issue in advance.
It supports two alarm and warning threshold method:

1. Auto Detection: Switch will auto detect alarm & warning threshold value if the SFP/SFP+ transceiver supports and follow the full SFF-8472. The SFP/SFP+ transceiver has default alarm and warning thresholds, which are fixed and cannot be changed.
2. Manual: network manager can set alarm and warning threshold value manually when SFP/SFP+ transceiver doesn't support the full SFF-8472 or customer doesn't trust the threshold value from SFP/SFP+ transceiver (SFF-8472).

When the temperature (degrees C), voltage (V), current (mA), TX power (dBm) or RX power (dbm) of SFP/SFP+ transceiver exceeds the alarm/warning threshold, an alarm or warning is generated, indicating that the SFP/SFP+ transceiver may be faulty, and switch will auto send message for network manager if network manager already enable SFP/SFP+ port threshold function. When message of alarm and warning threshold is generated, check the SFP/SFP+ transceiver, operating temperature and connected fibers first.

Chapter 2. Configuration Command
2.1 Configuring SFP/SFP+ Port Threshold Global Parameters

To configure the SFP/SFP+ port threshold global parameters, perform this task:

	Command or Action	Purpose
Step 1	Switch# **configure**	Enters global configuration mode.
Step 2	Switch (config)# **sfp threshold**	Enables global SFP threshold on the switch. The "**no sfp threshold**" command disables the global SFP threshold function.
Step 3	Switch (config)# **sfp threshold notification continuous-alarm**	Enables global notification continuous alarm of SFP threshold on the switch. The "**no sfp threshold notification continuous-alarm**" command disables the global notification continuous alarm of SFP threshold function. Default value is enabled.
Step 4	Switch (config)# **sfp threshold notification continuous-alarm interval** *[60-86400]*	(Optional) Configures specifies continuous alarm interval for notification. The "**no sfp threshold notification continuous-alarm interval**" command reset alarm interval time in default parameter, the default alarm interval time is 120 seconds.
Step 5	Switch (config)# **sfp threshold notification interval** *[120-86400]*	(Optional) Configures specifies interval for notification. The "**no sfp threshold notification interval**" command reset interval time in default parameter, the default interval time is 600 seconds.
Step 6	Switch (config)# **exit**	Returns to privileged EXEC mode.
Step 7	Switch# **write**	(Optional) Save the configuration.

This example shows how to enable global SFP threshold; and set specify notification continuous alarm interval and notification interval time:

Switch (config)# **sfp threshold**
Switch (config)# **sfp threshold notification continuous-alarm**
Switch (config)# **sfp threshold notification continuous-alarm interval 100**
Switch (config)# **sfp threshold notification interval 180**
Switch (config)# **exit**
Switch# **write**

2.2 Configuring Auto Detection SFP/SFP+ Port Threshold Interface Parameters

To configure the auto detection SFP/SFP+ port threshold parameters, perform this task:

	Command or Action	Purpose
Step 1	Switch# **configure**	Enters global configuration mode.
Step 2	Switch(config)# **interface** *interface-id*	Specifies the Layer 2 port to configure, and enters interface configuration mode.
Step 3	Switch (config-if-interface-id)# **sfp threshold detect**	(Optional) Enable auto detect alarm and warning threshold for specific port. Default value is enabled.
Step 4	Switch (config-if-interface-id)# **sfp threshold current** *[high* | *low]*	Enable to check high/low **current** threshold for specific port. The "**no sfp threshold current** *[high* | *low]*" command reset high/low **current** threshold in default parameter.
Step 5	Switch (config-if-interface-id)# **sfp threshold rx-power** *[high* | *low]*	Enable to check high/low **RX power** threshold for specific port. The "**no sfp threshold rx-power** *[high* | *low]*" command reset high/low **RX power** threshold in default parameter.
Step 6	Switch (config-if-interface-id)# **sfp threshold temperature** *[high* | *low]*	Enable to check high/low **temperature** threshold for specific port. The "**no sfp threshold temperature** *[high* | *low]*" command reset high/low **temperature** threshold in default parameter.
Step 7	Switch (config-if-interface-id)# **sfp threshold tx-power** *[high* | *low]*	Enable to check high/low **TX power** threshold for specific port. The "**no sfp threshold tx-power** *[high* | *low]*" command reset high/low **TX power** threshold in default parameter.
Step 8	Switch (config-if-interface-id)# **sfp threshold voltage** *[high* | *low]*	Enable to check high/low **voltage** threshold for specific port. The "**no sfp threshold voltage** *[high* | *low]*" command reset high/low **voltage** threshold in default parameter.
Step 9	Switch (config-if-interface-id)# **exit**	Returns global configuration mode.
Step 10	Switch (config)# **exit**	Returns to privileged EXEC mode.
Step 11	Switch# **write**	(Optional) Save the configuration.

This example shows how to enable auto detection SFP threshold:
Switch (config)# **interface 1-52**
Switch (config-if-1-52)# **sfp threshold detect**
Switch (config-if-1-52)# **sfp threshold current high**
Switch (config-if-1-52)# **sfp threshold current low**
Switch (config-if-1-52)# **sfp threshold rx-power high**
Switch (config-if-1-52)# **sfp threshold rx-power low**
Switch (config-if-1-52)# **sfp threshold temperature high**
Switch (config-if-1-52)# **sfp threshold temperature low**
Switch (config-if-1-52)# **sfp threshold tx-power high**
Switch (config-if-1-52)# **sfp threshold tx-power low**
Switch (config-if-1-52)# **sfp threshold voltage high**
Switch (config-if-1-52)# **sfp threshold voltage low**
Switch (config-if-1-52)# **exit**
Switch (config)# **exit**
Switch# **write**

2.3 Configuring manual SFP/SFP+ Port Threshold Interface Parameters

To configure the manual SFP/SFP+ port threshold parameters, perform this task:

	Command or Action	Purpose
Step 1	Switch# **configure**	Enters global configuration mode.
Step 2	Switch(config)# **interface** *interface-id*	Specifies the Layer 2 port to configure, and enters interface configuration mode.
Step 3	Switch (config-if-interface-id)# **no sfp threshold detect**	Disable auto detect alarm and warning threshold for specific port.
Step 4	Switch (config-if-interface-id)# **sfp threshold current** *[high* | *low]*	Enable to check high/low **current** threshold for specific port. The "**no sfp threshold current** *[high* | *low]*" command reset high/low **current** threshold in default parameter.

Step 5	Switch (config-if-interface-id)# **sfp threshold current** *[high* | *low]* **value** *[0-1500]*	To set specific value for high/low alarm/warning **current** threshold for specific port. This command can set high/low alarm **and** warning **current** threshold at the same time; and use the same specific value, the value range is 0~1500 (Unit is 1/10mA). The "**no sfp threshold current** *[high* | *low]* **value**" command reset value for high/low alarm **and** warning **current** threshold in default parameter. Note: The value of low threshold cannot at or over high threshold.
Step 6	Switch (config-if-interface-id)# **sfp threshold current** *[high* | *low]* **value** *[alarm* | *warning] [0-1500]*	To set specific value for high/low alarm/warning **current** threshold for specific port. This command can set high/low alarm **or** warning **current** threshold, the value range is 0~1500 (Unit is 1/10mA). The "**no sfp threshold current** *[high* | *low]* **value** *[alarm* | *warning]*" command reset value for high/low alarm **or** warning **current** threshold in default parameter. Note: 1. The value of low alarm threshold cannot over low warning threshold; 2. The value of low warning threshold cannot at or over high warning threshold; 3. The value of high warning threshold cannot over high alarm threshold. Please don't use step 5 and 6 at the same time.
Step 7	Switch (config-if-interface-id)# **sfp threshold rx-power** *[high* | *low]*	Enable to check high/low **RX power** threshold for specific port. The "**no sfp threshold rx-power** *[high* | *low]*" command reset high/low **RX power** threshold in default parameter.
Step 8	Switch (config-if-interface-id)# **sfp threshold rx-power** *[high* | *low]* **value** *[-400~100]*	To set specific value for high/low alarm/warning **RX power** threshold for specific port. This command can set high/low alarm **and** warning **RX power** threshold at the same time; and use the same specific value, the value range is -400~100 (Unit is 1/10dBm). The "**no sfp threshold rx-power** *[high* | *low]* **value**" command reset value for high/low alarm **and** warning **RX power** threshold in default parameter. Note: The value of low threshold cannot at or over high threshold.
Step 9	Switch (config-if-interface-id)# **sfp threshold rx-power** *[high* | *low]* **value** *[alarm* | *warning] [-400~100]*	To set specific value for high/low alarm/warning **RX power** threshold for specific port. This command can set high/low alarm **or** warning **RX power** threshold, the value range is -400~100 (Unit is 1/10dBm). The "**no sfp threshold rx-power** *[high* | *low]* **value** *[alarm* | *warning]*" command reset value for high/low alarm **or** warning **RX power** threshold in default parameter. Note: 1. The value of low alarm threshold cannot over low warning threshold; 2. The value of low warning threshold cannot at or over high warning threshold; 3. The value of high warning threshold cannot over high alarm threshold. Please don't use step 8 and 9 at the same time.
Step 10	Switch (config-if-interface-id)# **sfp threshold temperature** *[high* | *low]*	Enable to check high/low **temperature** threshold for specific port. The "**no sfp threshold temperature** *[high* | *low]*" command reset high/low **temperature** threshold in default parameter.
Step 11	Switch (config-if-interface-id)# **sfp threshold temperature** *[high* | *low]* **value** *[-400~1200]*	To set specific value for high/low alarm/warning **temperature** threshold for specific port. This command can set high/low alarm **and** warning **temperature** threshold at the same time; and use the same specific value, the value range is -400~1200 (Unit is 1/10 degrees C). The "**no sfp threshold temperature** *[high* | *low]* **value**" command reset value for high/low alarm **and** warning **temperature** threshold in default parameter.

		Note: The value of low threshold cannot at or over high threshold.
Step 12	Switch (config-if-interface-id)# **sfp threshold temperature** *[high* | *low]* **value** *[alarm* | *warning] [-400~1200]*	To set specific value for high/low alarm/warning **temperature** threshold for specific port. This command can set high/low alarm **or** warning **temperature** threshold, the value range is -400~1200 (Unit is 1/10 degrees C). The "**no sfp threshold temperature** *[high* | *low]* **value** *[alarm* | *warning]*" command reset value for high/low alarm **or** warning **temperature** threshold in default parameter. Note: 1. The value of low alarm threshold cannot over low warning threshold; 2. The value of low warning threshold cannot at or over high warning threshold; 3. The value of high warning threshold cannot over high alarm threshold. Please don't use step 11 and 12 at the same time.
Step 13	Switch (config-if-interface-id)# **sfp threshold tx-power** *[high* | *low]*	Enable to check high/low **TX power** threshold for specific port. The "**no sfp threshold tx-power** *[high* | *low]*" command reset high/low **tx-power** threshold in default parameter.
Step 14	Switch (config-if-interface-id)# **sfp threshold tx-power** *[high* | *low]* **value** *[-300~100]*	To set specific value for high/low alarm/warning **TX power** threshold for specific port. This command can set high/low alarm **and** warning **TX power** threshold at the same time; and use the same specific value, the value range is -300~100 (Unit is 1/10dBm). The "**no sfp threshold tx-power** *[high* | *low]* **value**" command reset value for high/low alarm **and** warning **tx-power** threshold in default parameter. Note: The value of low threshold cannot at or over high threshold.
Step 15	Switch (config-if-interface-id)# **sfp threshold tx-power** *[high* | *low]* **value** *[alarm* | *warning] [-300~100]*	To set specific value for high/low alarm/warning **TX power** threshold for specific port. This command can set high/low alarm **or** warning **TX power** threshold, the value range is -300~100 (Unit is 1/10dBm). The "**no sfp threshold tx-power** *[high* | *low]* **value** *[alarm* | *warning]*" command reset value for high/low alarm **or** warning **tx-power** threshold in default parameter. Note: 1. The value of low alarm threshold cannot over low warning threshold; 2. The value of low warning threshold cannot at or over high warning threshold; 3. The value of high warning threshold cannot over high alarm threshold. Please don't use step 14 and 15 at the same time.
Step 16	Switch (config-if-interface-id)# **sfp threshold voltage** *[high* | *low]*	Enable to check high/low **voltage** threshold for specific port. The "**no sfp threshold voltage** *[high* | *low]*" command reset high/low **voltage** threshold in default parameter.
Step 17	Switch (config-if-interface-id)# **sfp threshold voltage** *[high* | *low]* **value** *[260~400]*	To set specific value for high/low alarm/warning **voltage** threshold for specific port. This command can set high/low alarm **and** warning **voltage** threshold at the same time; and use the same specific value, the value range is 260~400 (Unit is 1/100V). The "**no sfp threshold t voltage** *[high* | *low]* **value**" command reset value for high/low alarm **and** warning **voltage** threshold in default parameter. Note: The value of low threshold cannot at or over high threshold.
Step 18	Switch (config-if-interface-id)# **sfp threshold voltage** *[high* | *low]* **value** *[alarm* | *warning] [260~400]*	To set specific value for high/low alarm/warning **voltage** threshold for specific port. This command can set high/low alarm **or** warning **voltage** threshold, the value range is 260~400 (Unit is 1/100V). The "**no sfp threshold voltage** *[high* | *low]* **value** *[alarm* | *warning]*" command reset value for high/low alarm **or** warning **voltage** threshold in default parameter.

	Note: 1. The value of low alarm threshold cannot over low warning threshold; 2. The value of low warning threshold cannot at or over high warning threshold; 3. The value of high warning threshold cannot over high alarm threshold. Please don't use step 14 and 15 at the same time.
Switch (config-if-interface-id)# **exit**	Returns global configuration mode.
Switch (config)# **exit**	Returns to privileged EXEC mode.
Switch# **write**	(Optional) Save the configuration.

This example shows how to enable auto detection SFP threshold:
Switch (config)# **interface 1-48**
Switch (config-if-1-48)# **no sfp threshold detect**
Switch (config-if-1-48)# **sfp threshold current high**
Switch (config-if-1-48)# **sfp threshold current high value alarm 1100**
Switch (config-if-1-48)# **sfp threshold current high value warning 900**
Switch (config-if-1-48)# **sfp threshold current low**
Switch (config-if-1-48)# **sfp threshold current low value alarm 50**
Switch (config-if-1-48)# **sfp threshold current low value warning 100**
Switch (config-if-1-48)# **sfp threshold rx-power high**
Switch (config-if-1-48)# **sfp threshold rx-power high value alarm -10**
Switch (config-if-1-48)# **sfp threshold rx-power high value warning -20**
Switch (config-if-1-48)# **sfp threshold rx-power low**
Switch (config-if-1-48)# **sfp threshold rx-power low value alarm -220**
Switch (config-if-1-48)# **sfp threshold rx-power low value warning -210**
Switch (config-if-1-48)# **sfp threshold temperature high**
Switch (config-if-1-48)# **sfp threshold temperature high value alarm 800**
Switch (config-if-1-48)# **sfp threshold temperature high value warning 750**
Switch (config-if-1-48)# **sfp threshold temperature low**
Switch (config-if-1-48)# **sfp threshold temperature low value alarm -150**
Switch (config-if-1-48)# **sfp threshold temperature low value warning -100**
Switch (config-if-1-48)# **sfp threshold tx-power high**
Switch (config-if-1-48)# **sfp threshold tx-power high value alarm -20**
Switch (config-if-1-48)# **sfp threshold tx-power high value warning -30**
Switch (config-if-1-48)# **sfp threshold tx-power low**
Switch (config-if-1-48)# **sfp threshold tx-power low value alarm -110**
Switch (config-if-1-48)# **sfp threshold tx-power low value warning -100**
Switch (config-if-1-48)# **sfp threshold voltage high**
Switch (config-if-1-48)# **sfp threshold voltage high value alarm 365**
Switch (config-if-1-48)# **sfp threshold voltage high value warning 350**
Switch (config-if-1-48)# **sfp threshold voltage low**
Switch (config-if-1-48)# **sfp threshold voltage low value alarm 310**
Switch (config-if-1-48)# **sfp threshold voltage low value warning 320**
Switch (config-if-1-48)# **exit**
Switch (config)# **exit**
Switch# **write**

2.4 Configuring SNMP Trap for SFP/SFP+ Port Threshold Parameters

To configure the SNMP trap for SFP/SFP+ port threshold parameters, perform this task:

	Command or Action	**Purpose**
Step 1	Switch# **configure**	Enters global configuration mode.
Step 2	Switch(config)# **snmp-server trap-type sfp-threshold**	Enable SNMP trap for SFP threshold when SFP status changes from normal to abnormal or abnormal to normal. The "**no snmp-server trap-type sfp-threshold**" command disable SNMP trap for SFP threshold. Default value is enabled.
Step 10	Switch (config)# **exit**	Returns to privileged EXEC mode.
Step 11	Switch# **write**	(Optional) Save the configuration.

Chapter 3. Show Command

3.1 Display SFP/SFP+ Port Threshold Information

You can display selective QinQ information for the switch to perform this tasks:

Command	Purpose
Switch# **show sfp threshold** *interface-id*	Display all interface, single interface or interface range of temperature (degrees C), voltage (V), current (mA), TX power (dBm) and RX power (dBm) information that include SFP current status, high alarm, high warning, low warning and low alarm threshold.
Switch# **show sfp threshold current** *interface-id*	Display all interface, single interface or interface range of current (mA) information that include SFP current status, high alarm, high warning, low warning and low alarm threshold.
Switch# **show sfp threshold rx-power** *interface-id*	Display all interface, single interface or interface range of RX power (dBm) information that include SFP current status, high alarm, high warning, low warning and low alarm threshold.
Switch# **show sfp threshold temperature** *interface-id*	Display all interface, single interface or interface range of temperature (degrees C) information that include SFP current status, high alarm, high warning, low warning and low alarm threshold.
Switch# **show sfp threshold tx-power** *interface-id*	Display all interface, single interface or interface range of TX power (dBm) information that include SFP current status, high alarm, high warning, low warning and low alarm threshold.
Switch# **show sfp threshold voltage** *interface-id*	Display all interface, single interface or interface range of voltage (V) information that include SFP current status, high alarm, high warning, low warning and low alarm threshold.

This page is intentionally left blank.