CONNECTION TECHNOLOGY SYSTEMS

HES-5106SFP+

4-port 10/100/1000Base-T +
1-port NBase-T (1G/2.5G/5G/10G) +
1-port 1G/10GBase-R SFP+
L2 Managed Fiber CPE Switch

Network Management

User's Manual

Version 1.1

Revision History

Version	F/W	Date	Description
1.0	1.00.00	2020/05/22	First release
1.1	1.00.00	2020/06/24	Modify the pictures of HES-5106SFP+

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.

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

Trademarks:
All trade names and trademarks are the properties of their respective companies.

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 5 RJ-45 ports (4 10/100/1000Base-T & 1 NBase-T (1G/2.5G/5G/10G)) plus 1 1G/10GBase-R SFP+ uplink port Managed Ethernet CPE 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 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:

- Telnet Management
- SNMP Management
- WEB Management
- SSH 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. 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 10/100/1000Base-TX 8-pin or NBase-T RJ-45 ports located at the front panel of the Managed Switch. Direct RJ-45 LAN cable connection between a PC and the Managed Switch is required for Web Management. Or through the SFP+ port located on the rear panel of the Managed Switch, a converter and direct RJ-45 LAN cable connection between a PC and the Managed Switch are required for this 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

Command Line Interface 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 use Telnet/SSH to login and access the CLI using the Terminal Emulation program (such as Putty or Tera Term) through network connection.

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..

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, 1000Bas-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.

10/100/1000Base-T / NBase-T RJ-45 Auto-MDI/MDIX Port

10/100/1000Base-T **/** NBase-T RJ-45 Auto-MDI/MDIX ports are located at the front of the Managed Switch. These RJ-45 ports allow user to connect their traditional copper-based Ethernet/Fast Ethernet devices to the network. All these ports support auto-negotiation and MDI/MDIX auto-crossover, i.e. either crossover or straight through CAT-5E UTP or STP cable may be used. As to NBase-T RJ-45 port can be plugged with CAT-5E/CAT.6/CAT-6A (22~24 AWG) or better cabling.

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:

- Telnet
- Configuring the system
- Resetting the system

2.1 Remote Management – Telnet/SSH

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

Follow steps described below to access the Managed Switch through Telnet/SSH session:

Step 1. Use any one of the RJ-45 ports on the front panel to login to the Managed Switch.

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

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

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

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

Step 6. Use new IP address to login to the Managed Switch via Telnet/SSH session again.

Only five active Telnet/SSH sessions can access the Managed Switch at the same time.

2.2 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.*

2.2.1 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

2.2.2 Quick Keys

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

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

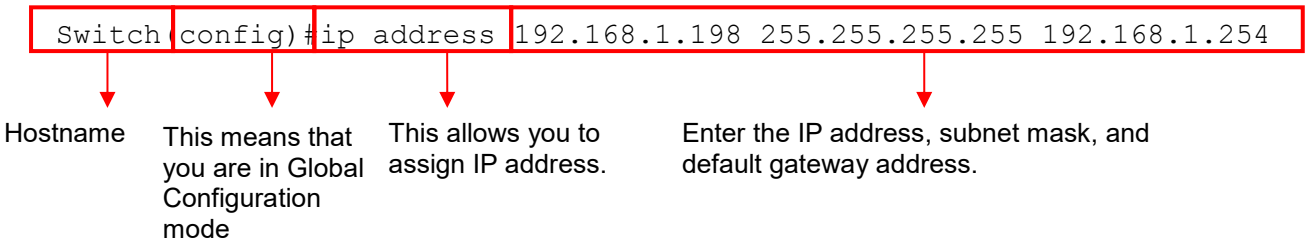
Unfinished command followed by ?	Enter an unfinished command or keyword and press “?” key to complete the command and get command syntax help.
	
	Example: List all available commands starting with the characters that you enter.
	
	`Switch#h?`
	`help` `Show available commands`
	`history` `Show history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

2.2.3 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 2.5.24 for detailed explanations.
[port_list]	Enter a range of port numbers or several discontinuous port numbers. See Section 2.5.24 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`

2.2.4 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.

2.3 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.
ping	Test whether a specified network device or host is reachable or not.
traceroute	Trace the route to HOST
enable	Enter the Privileged mode.

2.3.1 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		

2.3.2 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		

2.4 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.
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.

2.4.1 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

2.4.2 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		

2.4.3 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 2.5.6 for more details.** **Note 2: The command is just one-time command, and the setting will not be saved into the configuration file.**

2.4.4 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		

2.4.5 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

2.4.6 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		

2.4.7 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!

2.4.8 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)#

2.4.9 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.

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 Event Log

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

7. Show Port Link Flap Log

Show the log of Port Link Flap information. Refer to “Show log link-flap command” section.

2.5 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.
exit	Exit the global configuration mode.
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.
lan-follow-wan	Set up LAN port(s) to follow WAN port’s linkup/linkdown commands
loop-detection	Configure loop-detection to prevent loop between switch ports by locking them.
led	All LEDs intensity configuration commands
mac	Set up MAC learning function of each port.
management	Set up console/telnet/web/SSH access control and timeout value.
mirror	Set up target port for mirroring.
ntp	Set up required configurations for Network Time Protocol.
qos	Set up the priority of packets within the Managed 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.
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.

2.5.1 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.

2.5.2 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.

2.5.3 Show Command

The “show” command is very important for network administrators to get information about the device, receive outputs to verify a command’s configurations or troubleshoot a network configuration error. 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.

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 Event Log

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

7. Show Port Link Flap Log

Show the log of Port Link Flap information. Refer to “Show log link-flap command” section.

2.5.4 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 (1~6).
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 any		Specify destination MAC as “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.

2.5.5 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.

2.5.6 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		Enable IPv4 DHCP Auto Recycle function on the specified ports. Only

auto-recycle		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 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 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 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 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 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 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.
Switch(config)# show ip igmp snooping groups		Show IGMP snooping groups table.
Switch(config)# show ip igmp snooping status		Show IGMP Snooping status.
Switch(config)# show ip mld snooping groups		Show MLD snooping groups table.
Switch(config)# show ip mld snooping status		Show MLD Snooping status.

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)#		Remove the selected port(s) from the

no ip igmp snooping mcast-router		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.

2.5.7 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]	Specify IPv6 global address and prefix-length of the Managed Switch.
[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]	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.

2.5.8 lan-follow-wan Command

With the lan-follow-wan function, the device(s) connected with the LAN port(s) of the Managed Switch can be immediately triggered by its link-up WAN port (SFP+ port that is located at the rear panel of the Managed Switch) switched from link-down into link-up status in order to obtain the new DHCP IP address and the related update information, such as the firmware or the configuration file, from the DHCP server.

1. Set up LAN ports.

lan-follow-wan Command	Parameter	Description
Switch(config)# lan-follow-wan		Enable the lan-follow-wan function.
Switch(config)# lan-follow-wan wan-down-timer [0-255]	[0-255]	Specify the timer to count down in order to trigger the specific LAN port(s) to do the link down when WAN port's link is down. "0" stands for "immediate".
Switch(config)# lan-follow-wan wan-up-timer [0-255]	[0-255]	Specify the timer to count down in order to trigger the specific LAN port(s) to do the link up when WAN port's link is up. "0" stands for "immediate".
No command		
Switch(config)# no lan-follow-wan		Disable the lan-follow-wan function.
Switch(config)# no lan-follow-wan wan-down-timer		Reset the timer to count down for LAN ports to follow WAN port's linkdown back to the default.(15 seconds)
Switch(config)# no lan-follow-wan wan-up-timer		Reset the timer to count down for LAN ports to follow WAN port's linkdup back to the default. (15 seconds)
Show command		
Switch(config)# show lan-follow-wan		Show the current lan-follow-wan configuration.
Examples of lan-follow-wan command		
Switch(config)# lan-follow-wan wan-down-timer 30		The specified LAN port(s) will link down after 30 seconds when WAN port link is down.
Switch(config)# lan-follow-wan wan-up-timer 0		The specified LAN port(s) will link up immediately when WAN port link is up.

2. Use "Interface" command to configure a group of ports' lan-follow-wan settings.

lan-follow-wan & 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)# lan-follow-wan		Enable the lan-follow-wan function on the selected port(s).
No command		
Switch(config-if-PORT-PORT)# no lan-follow-wan		Disable the lan-follow-wan function on the selected port(s).

2.5.9 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 packets received on the looped port.
2. It slowly blinks the LED of looped port in orange (Ports 1~4) or in blue (Ports 5~6).
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 (Ports 1~4) or in blue (Ports 5~6).
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* (Ports 1~4) or in blue (Ports 5~6) *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 2.5.23). **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).

2.5.10 led Command

LED commands allows the user to control the light intensity of all LEDs at will on the Managed Switch in order to decrease the possibility of the light pollution damage.

1. Set up the intensity of the light for all LEDs on the Managed Switch.

led Command	Parameter	Description
Switch(config)# led control intensity [high|medium|low|off]	[high|medium|low|off]	Specify the light intensity of device LEDs. **High:** It indicates LEDs of Ports 1~6, Status LED and Power LED on the Managed Switch will light with the highest level. **Medium:** It indicates LEDs of Ports 1~6, Status LED and Power LED on the Managed Switch will light with the medium level. **Low:** It indicates LEDs of Ports 1~6, Status LED and Power LED on the Managed Switch will light with the lowest level. **Off:** It indicates all LEDs except Power LED on the Managed Switch will be off. Power LED will light with the lowest level.
No command		
Switch(config)# no led control intensity		Reset the light intensity of device LEDs back to the default.(High)
Show command		
Switch(config)# show led control		Show the current LED control configuration.
Examples of led command		
Switch(config)# led control intensity low		Configure the light intensity of all LEDs on Managed Switch as “Low” level.

2.5.11 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).

2.5.12 Management Command

Management Command	Parameter	Description
Switch(config)# management console timeout [1-1440]	[1-1440]	To disconnect the Managed Switch when console management is inactive for a certain period of time. The allowable value is from 1 to 1440 (seconds).
Switch(config)# management console timeout [1-1440] min	[1-1440]	To disconnect the Managed Switch when console management is inactive for a certain period of time. The allowable value is from 1 to 1440 (minutes).
Switch(config)# management ssh		Enable SSH management. To manage the Managed Switch via SSH.
Switch(config)# management telnet		Enable Telnet Management. To manage the Managed Switch via Telnet.
Switch(config)# management telnet port [1-65535]	[1-65535]	When telnet is enabled, you can set up the port number that allows telnet access. The default port number is set to 23. However, you can also identify a port number between 1 and 65535.
Switch(config)# management web		Enable Web management by the http method.
Switch(config)# management web [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 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.

2.5.13 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 (1~6) 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 1-4 direction tx		Port 1 to 4's transmitting packets will mirror to the destination port in the port mirroring of Index No. 3.

2.5.14 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-Days,hh:mm]	[Days,hh:mm-Days,hh:mm]	Specify the offset of daylight saving in date mode. **Mm=1-12, w=1-5, d=0-6(0=Sun, 6=Sat) Hh=0-23, mm=0-59, Days=1-365**
Switch(config)# ntp server1 [A.B.C.D | A:B:C:D: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.

2.5.15 QoS Command

1. Set up QoS

QoS Command	Parameter	Description
Switch(config)# qos [802.1p | dscp]	[802.1p | dscp]	Specify QoS mode.
Switch(config)# qos dscp-map [0-63] [0-7]	[0-63]	Specify a DSCP bit value.
	[0-7]	Specify a queue value.
Switch(config)# qos management-priority [0-7]	[0-7]	Specify management default 802.1p bit.
Switch(config)# qos queuing-mode [weight | 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 dscp		Globally disable DSCP remarking.
Switch(config)# no qos remarking dscp-map [1-8]	[1-8]	Reset the DSCP remaking for the specified priority mapping ID back to the default.
Switch (config-dscp-map-ID)# no new-dscp		Reset the new DSCP bit value for the selected priority mapping ID back to the default.

Switch (config-dscp-map-ID)# no rx-dscp		Reset the received DSCP bit value for the selected priority mapping ID back to the default.
Switch(config)# no qos remarking 802.1p		Globally disable 802.1p 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.

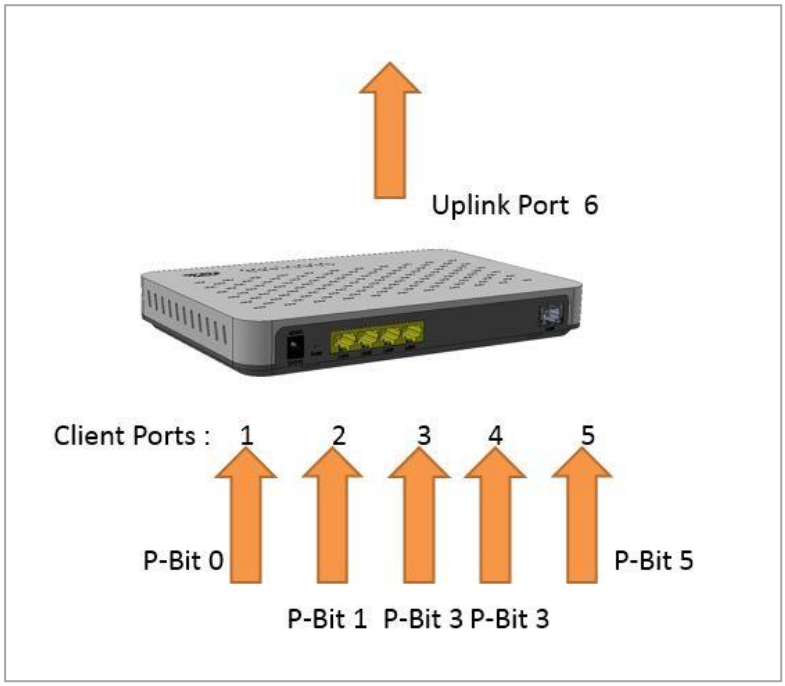
2. Use “interface” command to configure a group of ports’ QoS settings.

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 [500-10000000 | 1-10000] Kbps/Mbps	[500-10000000 | 1-10000] 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 for Ports 1~4 and 500-10000000 in unit of Kbps or 1-10000 in unit of Mbps for Ports 5~6.).

Switch(config-if-PORT-PORT)# qos rate-limit ingress unit [Kbps | Mbps]	[Kbps | Mbps]	Specify the unit of the ingress rate limit between Kbps and 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 [500-10000000 | 1-10000] Kbps/Mbps	500-10000000 | 1-10000] 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 for Ports 1~4 and 500-10000000 in unit of Kbps or 1-10000 in unit of Mbps for Ports 5~6.).
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 HES-5106SFP+ Managed Switch for example to let the users have a clear understanding of these QoS commands.

Under this network environment, HES-5106SFP+ will be configured as Table 2-1. Ports 1-5 are client ports and Port 6 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 6: 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 HES-5106SFP+ Managed Switch.

	Command	**Purpose**
STEP1	configure **Example:** HES-5106SFP+# config HES-5106SFP+(config)#	**Enter the global configuration mode.**
STEP2	qos 802.1p **Example:** HES-5106SFP+(config)# qos 802.1p OK !	**In this example, it configures the QoS Mode to 802.1p.**

STEP3	qos queuing-mode weight **Example:** HES-5106SFP+(config)# qos queuing-mode weight **OK !**	**In this example, it configures Queue Mode as "Weight".**
STEP4	qos queue-weighted *weighted* **Example:** HES-5106SFP+(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:** HES-5106SFP+(config)# qos 802.1p-map 0 0 HES-5106SFP+(config)# qos 802.1p-map 1 1 HES-5106SFP+(config)# qos 802.1p-map 3 2 HES-5106SFP+(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:** HES-5106SFP+(config)# interface 1 HES-5106SFP+(config-if-1)#	**Specify the Port 1 that you would like to configure P-Bit.**
STEP7	qos user-priority *P-Bit* **Example:** HES-5106SFP+(config-if-1)# qos user-priority 0	**In this example, it configures P-Bit value as 0 for Port 1.**
STEP8	exit **Example:** HES-5106SFP+(config-if-1)# exit HES-5106SFP+(config)#	**Return to the global configuration mode.**
STEP9	interface *port_list* **Example:** HES-5106SFP+(config)# interface 2 HES-5106SFP+(config-if-2)#	**Specify the Port 2 that you would like to configure P-Bit.**
STEP10	qos user-priority *P-Bit* **Example:** HES-5106SFP+(config-if-2)# qos user-priority 1	**In this example, it configures P-Bit value as 1 for Port 2.**
STEP11	exit **Example:** HES-5106SFP+(config-if-2)# exit HES-5106SFP+(config)#	**Return to the global configuration mode.**
STEP12	interface *port_list* **Example:** HES-5106SFP+(config)# interface 3, 4 HES-5106SFP+(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:** HES-5106SFP+(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:** HES-5106SFP+(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:** HES-5106SFP+(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:** HES-5106SFP+(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:** HES-5106SFP+(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:** HES-5106SFP+(config-if-3,4)# exit HES-5106SFP+(config)#	**Return to the global configuration mode.**
STEP19	interface *port_list* **Example:** HES-5106SFP+(config)# interface 5 HES-5106SFP+(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:** HES-5106SFP+(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:** HES-5106SFP+(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:** HES-5106SFP+(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:** HES-5106SFP+(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:** HES-5106SFP+(config-if-5)# qos user-priority 5	**In this example, it configures P-Bit value as 5 for Port 5.**
STEP25	exit **Example:** HES-5106SFP+(config-if-5)# exit HES-5106SFP+(config)#	**Return to the global configuration mode.**
STEP26	exit **Example:** HES-5106SFP+(config)# exit HES-5106SFP+#	**Return to the Privileged mode.**
STEP27	write **Example:** HES-5106SFP+# write Save Config Succeeded!	**Save the running configuration into the startup configuration.**

After completing the QoS settings for your HES-5106SFP+ switches, you can issue the commands listed below for checking your configuration

Example 1,

HES-5106SFP+(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
```

Example 2,

HES-5106SFP+(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

HES-5106SFP+(config)#
```

2.5.16 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.

With the function of Port Linkup Delay, you are allowed to set up a period of time for postponing the specific port(s) to be active in the stage of the system initialization. As for the remaining ports of the switch, they will be normally activated and be able to learn the MAC address first.

Port Link Flap will notify the user the link-down and link-up alarm message of any port via SNMP trap and syslog when its port link flap times exceed the threshold. A port links down or links up, which will be considered as one time of this port's port link flap. Through this function, it will greately help technicians in the network operations center (NOC) exactly know the last time when the port linked down and linked up, and easily find out the major causes of the network unstability.

1. Enable or disable broadcast/unknown multicast/unknown unicast storm control, port isolation, Port Linkup Delay and Port Link Flap.

Security Command	Parameter	Description
Switch(config)# security delay time [0-1200]	[0-1200]	Specify the desired time the designated delay port(s) will delay to be activated. The allowable value is between 0 and 1200 seconds. "0" indicates "Disabled".
Switch(config)# security link-flap notification threshold [1-20]	[1-20]	Specify the maximum times of the port link flap for sending the alarm trap and syslog message. **Note: A port links down or links up, which will count as one time of this port's port link flap.**
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 link-flap notification threshold		Reset the maximum times of the port link flap for sending the alarm trap and syslog message back to the default.
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 delay		Show the current Port Linkup Delay configuration.
Switch(config)# show security link-flap		Show the current Port Link Flap configuration.
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).
Examples of Security command		
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 Port Linkup Delay 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 delay		Configure the selected port(s) as the delay port(s).
Switch(config-if-PORT-PORT)# security port-isolation		Configure the selected port(s) as uplinks that are allowed to

up-link-port		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 delay		Disable the delay port function on the selected port(s).
Switch(config-if-PORT-PORT)# no security port-		Disable the specified port(s) as non-up-link-port.

isolation 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)# security delay time 30 Switch(config-if-1-4)# security delay		Configure Port 1~ Port 4 as the delay ports. And the system will only activate Port 5 as well as Port 6 first, and wait for 30 seconds to activate Ports 1-4 in the next device's boot-up (initialization) stage.

2.5.17 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 | cold-start | cpu-load | cpu-temperature | port-link | port-link-flap | power-down| storm-control | warm-start]	[all | auth-fail | auto-backup | cold-start | cpu-load | cpu-temperature | port-link | port-link-flap| power-down| storm-control | warm-start]	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 unauthorized user attempts to login. **auto-backup:** A trap will be sent when the auto backup succeeds or fails. **cold-start:** A trap will be sent when the 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. **port-link:** A trap will be sent when the link is up or down. **port-link-flap:** A trap will be sent when a port’s port link flap exceeds the threshold. **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. **warm-start:** A trap will be sent when the Managed Switch restarts.
No command		
Switch(config)# no snmp-server trap-type [all | auth-fail | auto-backup | cold-start | cpu-load | cpu-temperature | port-link | port-link-flap| power-down| storm-control | warm-start]	[all | auth-fail | auto-backup | cold-start | cpu-load | cpu-temperature | port-link | port-link-flap| power-down| storm-control | warm-start]	Specify a trap type that will not be sent when a certain situation occurs.
Show command		
Switch(config)# show snmp-server trap-type		Show the current enable/disable status of each type of trap.
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 2.5.22.)

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.

2.5.18 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 [1-6]	[1-6]	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. (2 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.

2.5.19 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 [0-85]	[0-85]	Specify a value as CPU temperature threshold (Vaild Range: 0~85 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. (75 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.
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”.

2.5.20 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:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F :G:H]	Specify the secondary system log server's IPv4/IPv6 address.
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.

2.5.21 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.

2.5.22 User Command

1. Create a new login account.

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 authentication 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. Configure RADIUS server settings.

User Command	Parameter	Description
Switch(config)# user radius		Enable RADIUS authentication.
Switch(config)# user radius radius-port [1025-65535]	[1025-65535]	Specify RADIUS server port number.
Switch(config)# user radius retry-time [0-2]	[0-2]	Specify the retry time value. This is the number of times that the Managed Switch will try to reconnect if the RADIUS server is not reachable.
Switch(config)# user radius secret [secret]	[secret]	Specify a secret, up to 30 alphanumeric characters, for RADIUS server. This secret key is used to validate communications between RADIUS servers.
Switch(config)# user radius 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 RADIUS server's IPv4/IPv6 address.
Switch(config)# user radius 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 RADIUS server's IPv4/IPv6 address.
No command		
Switch(config)# no user radius		Disable RADIUS authentication.
Switch(config)# no user radius radius-port		Reset the radius port setting back to the default. (1812 port)
Switch(config)# no user radius retry-time		Reset the retry time setting back to the default.
Switch(config)# no user radius secret		Remove the configured secret value.
Switch(config)# no user radius server1		Delete the IPv4/IPv6 address of the primary RADIUS server.
Switch(config)# no user radius server2		Delete the IPv4/IPv6 address of the secondary RADIUS server.
Show command		
Switch(config)# show user radius		Show the current RADIUS configuration.
Examples of User command		
Switch(config)# user radius		Enable RADIUS authentication.
Switch(config)# user radius radius-port 1812		Set RADIUS server port number as 1812.
Switch(config)# user radius retry-time 2		Set the retry time value to 2. The Managed Switch will try to reconnect twice if the RADIUS server is not reachable.
Switch(config)# user radius secret abcxyzabc		Set up a secret for validating communications between RADIUS clients.
Switch(config)# user radius server1 192.180.3.1		Set the primary RADIUS server address to 192.180.3.1.
Switch(config)# user radius server2 192.180.3.2		Set the secondary RADIUS server address to 192.180.3.2.

2.5.23 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.

2.5.23.1 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.

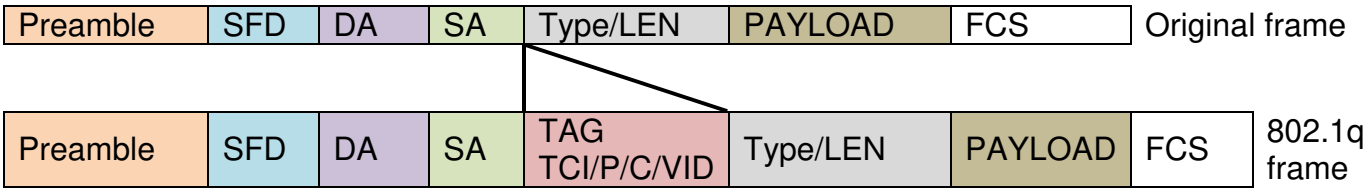
Since source addresses of the packets are listed in MAC address table of specific VLAN (except broadcast/multicast packets), in every VLAN the traffic between two ports will be two-way without restrictions.

2.5.23.2 802.1Q 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.

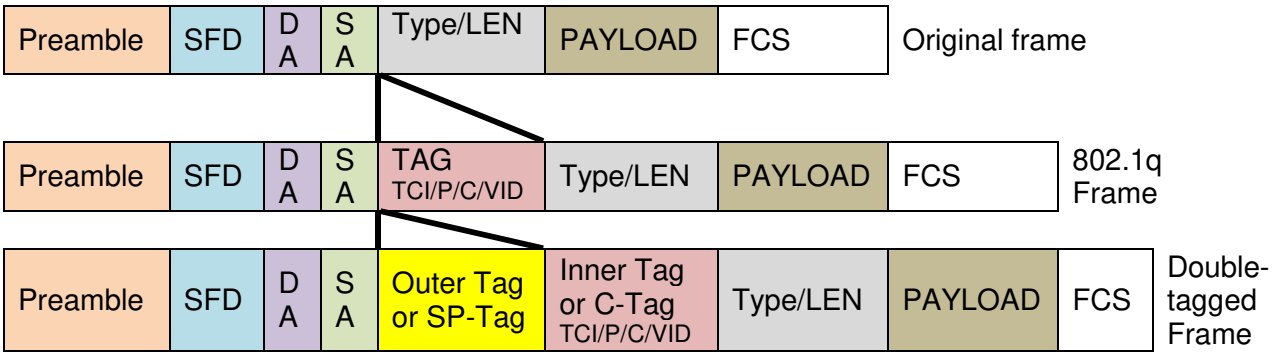
- Customer traffic tagged in the normal way with appropriate VLAN IDs comes from an IEEE 802.1Q trunk port on the customer device and into a tunnel port on the service-provider edge switch. The link between the customer device and the edge switch is asymmetric because one end is configured as an IEEE 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.

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)

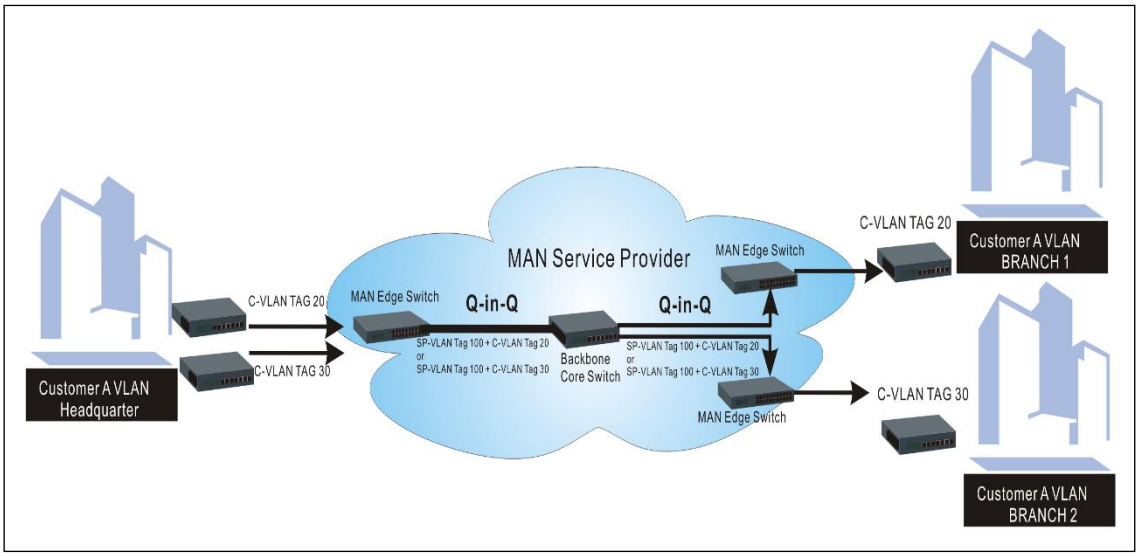
2.5.23.3 Introduction to Q-in-Q (DOT1Q-Tunnel)

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 [1-4094]	[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 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] management-port [port_list] mode [access | trunk | trunk-native]	[1-4094]	Enter the management VLAN ID.
	[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).

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 2.5.23.**
	[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.

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

Example 1,

We will configure HES-5106SFP+ 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

Table 2-3

1. **Create 802.1q VLAN IDs.**

HES-5106SFP+(config)# interface 1-2	Enter port 1 to port 2's interface mode.
HES-5106SFP+(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.
HES-5106SFP+(config-if-1,2)# vlan dot1q-vlan mode trunk	Set the selected ports to Trunk Mode (tagged).
HES-5106SFP+(config-if-1,2)# exit	Exit current ports interface mode.
HES-5106SFP+ (config)# interface 3-4	Enter port 3 to 4's interface mode.
HES-5106SFP+(config-if-3,4)# vlan dot1q-vlan pvid 50	Set port 3 to port 4's Access-VLAN ID (PVID) to 50.
HES-5106SFP+(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.
HES-5106SFP+(config-if-3,4)# vlan dot1q-vlan mode trunk native	Set the selected ports to Trunk-native Mode (tagged and untagged).
HES-5106SFP+(config-if-3,4)# exit	Exit current ports interface mode.
HES-5106SFP+ (config)# interface 5-6	Enter port 5 to port 6's interface mode.

HES-5106SFP+(config-if-5,6)# vlan dot1q-vlan pvid 60	Set port 5 to port 6's Access-VLAN ID (PVID) to 60.
HES-5106SFP+(config-if-5,6)# vlan dot1q-vlan mode access	Set the selected ports to Access Mode (untagged).
HES-5106SFP+(config-if-5,6)# exit	Exit current ports interface mode.

2. Modify 802.1q VLAN IDs' names.

HES-5106SFP+(config)# vlan dot1q-vlan 10	Enter VLAN 10.
HES-5106SFP+ (config-vlan-10)# name Sales	Specify "Sales" as the name for VLAN 10.
HES-5106SFP+ (config-vlan-10)# exit	Exit VLAN 10.
HES-5106SFP+(config)# vlan dot1q-vlan 20	Enter VLAN 20.
HES-5106SFP+(config-vlan-20)# name Sales	Specify "Sales" as the name for VLAN 20.
HES-5106SFP+(config-vlan-20)# exit	Exit VLAN 20.
HES-5106SFP+(config)# vlan dot1q-vlan 30	Enter VLAN 30.
HES-5106SFP+(config-vlan-30)# name RD	Specify "RD" as the name for VLAN 30.
HES-5106SFP+(config-vlan-30)# exit	Exit VLAN 30.
HES-5106SFP+(config)# vlan dot1q-vlan 40	Enter VLAN 40.
HES-5106SFP+(config-vlan-40)# name RD	Specify "RD" as the name for VLAN 40.
HES-5106SFP+(config-vlan-40)# exit	Exit VLAN 40.
HES-5106SFP+(config)# vlan dot1q-vlan 50	Enter VLAN 50.
HES-5106SFP+(config-vlan-50)# name RD	Specify "RD" as the name for VLAN 50.
HES-5106SFP+(config-vlan-50)# exit	Exit VLAN 50.
HES-5106SFP+(config)# vlan dot1q-vlan 60	Enter VLAN 60.
HES-5106SFP+(config-vlan-60)# name SQA	Specify "SQA" as the name for VLAN 60.
HES-5106SFP+(config-vlan-60)# exit	Exit VLAN 60.

Example 2,

We will configure two sets of HES-5106SFP+ Managed Switch(including #1 HES-5106SFP+ and #2 HES-5106SFP+) 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 HES-5106SFP+. Also issue the same commands to #2 HES-5106SFP+.

	Command	Purpose
STEP1	configure **Example:** HES-5106SFP+# config HES-5106SFP+(config)#	**Enter the global configuration mode.**
STEP2	vlan dot1q-tunnel ethertype *0xWXYZ* **Example:** HES-5106SFP+(config)# vlan dot1q-tunnel ethertype 9100 OK !	**In this example, it configures the dot1q-tunnel ethertype value as "9100"**
STEP3	interface *port_list* **Example:** HES-5106SFP+(config)# interface 1 HES-5106SFP+ (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:** HES-5106SFP+(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:** HES-5106SFP+(config-if-1)# vlan dot1q-vlan mode dot1q-tunnel OK !	**Configure Port 1's VLAN mode as "dot1q-tunnel" mode.**
STEP6	exit **Example:** HES-5106SFP+(config-if-1)# exit HES-5106SFP+(config)#	**Return to the global configuration mode.**
STEP7	interface *port_list* **Example:**	**Specify Port 2 that you would like to configure it as Trunk port.**

	HES-5106SFP+(config)# interface 2 HES-5106SFP+(config-if-2)#	
STEP8	vlan dot1q-vlan trunk-vlan *vlan_id* **Example:** HES-5106SFP+(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:** HES-5106SFP+(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* **Example:** HES-5106SFP+(config-if-2)# no vlan dot1q-vlan trunk-vlan 1 OK !	**Remove the Trunk-VLAN ID "1" from Port 2.**
STEP10	exit **Example:** HES-5106SFP+ (config-if-2)# exit HES-5106SFP+ (config)#	**Return to the global configuration mode.**
STEP11	interface *port_list* **Example:** HES-5106SFP+(config)# interface 3 HES-5106SFP+ (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:** HES-5106SFP+(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:** **HES-5106SFP+** (config-if-3)# vlan dot1q-vlan mode dot1q-tunnel OK !	**Configure Port 3's VLAN mode as "dot1q-tunnel" mode.**
STEP14	exit **Example:** HES-5106SFP+ (config-if-3)# exit HES-5106SFP+ (config)#	**Return to the global configuration mode.**
STEP15	interface *port_list* **Example:** HES-5106SFP+(config)# interface 4 HES-5106SFP+(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:** HES-5106SFP+(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:** **HES-5106SFP+** (config-if-4)# vlan dot1q-vlan mode dot1q-tunnel OK !	**Configure Port 4's VLAN mode as "dot1q-tunnel" mode.**
STEP18	exit **Example:** HES-5106SFP+ (config-if-4)# exit HES-5106SFP+ (config)#	**Return to the global configuration mode.**
STEP19	exit **Example:** HES-5106SFP+(config)# exit HES-5106SFP+#	**Return to the Privileged mode.**
STEP20	write **Example:** HES-5106SFP+# write Save Config Succeeded!	**Save the running configuration into the startup configuration.**

After completing the VLAN settings for your HES-5106SFP+ switches, you can issue the commands listed below for checking your configuration

Example 1,

HES-5106SFP+(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

HES-5156SFP+(config)#
```

Example 2,

HES-5106SFP+(config)# show vlan

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

U: Untagged, T: Tagged, D: Dot1q-Tunnel, V: Member, -: Not Member
--------------------------------------------------------------------------------------------------------------
VLAN Name       VLAN  1        CPU
-----------------     -------   ------     ---
Default_VLAN          1   ----UU   V
VLAN0010             10  DT----     -
VLAN0020             20  --DD--    -


HES-5156SFP+(config)#
```

2.5.24 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 2-14 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 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.

4. Set up port duplex mode.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# duplex [full]	[full]	Configure the port duplex as **full**. **Note: Port 5 cannot be configured as full duplex.**
No command		
Switch(config-if-PORT-PORT)# no duplex		Configure the port duplex as **half**. **Note: Ports 5-6 cannot be configured as half duplex.**

5. 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).

6. 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.

7. 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.

8. 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).

9. 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.

10. 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).

11. Configure QoS rate limit.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# qos rate-limit ingress rate [500-10000000 | 1-10000] Kbps/Mbps	500-10000000 | 1-10000] 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 for Ports 1~4 and 500-10000000 in unit of Kbps or 1-10000 in unit of Mbps for Ports 5~6.).
Switch(config-if-PORT-PORT)# qos rate-limit egress rate [500-10000000 | 1-10000] Kbps/Mbps	500-10000000 | 1-10000] 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 for Ports 1~4 and 500-10000000 in unit of Kbps or 1-10000 in unit of Mbps for Ports 5~6.).
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.

12. 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.

13. Set up port speed.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# speed [10000 | 5000 | 2500 | 1000 | 100 | 10 | auto_sense]	[10000 | 5000 | 2500 | 1000 | 100 | 10 | auto_sense]	Configure the port speed as 10000Mbps, 5000Mbps, 2500Mbps,1000Mbps, 100Mbps or 10Mbps. **Note1: Speed can only be configured when auto-negotiation is disabled.** **Note2: Only Port 5 can be configured as 5000Mbps or 2500Mbps.** **Note3: Ports 5-6 cannot be configured as 10/100Mbps.** **Note4: Only Ports 5-6 can be configured as 10000Mbps and auto_sense.**
No command		
Switch(config-if-PORT-PORT)# no speed		Reset the port speed setting back to the default.

14. 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.

2.5.25 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.

2.5.26 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.

2.5.27 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.

2.5.28 Show log Command

Show log Command	Parameters	Description
Switch# show log		Show all event logs currently stored in the Managed Switch.
Switch# show log clear		Remove all event logs currently stored in the Managed Switch.
Switch(config)# show log		Show all event logs currently stored in the Managed Switch.
Switch(config)# show log clear		Remove all event logs currently stored in the Managed Switch.

2.5.29 Show log link-flap Command

Command	Parameters	Description
Switch# show log link-flap [port_number]	[port_number]	Show the specific port's log history of trigger events such as the port link flap (a port's linkdown or linkup), the count of port's port link flap, the reason that causes these triggered events, the time duration that the port link flap lasts, Rx power(dBm) of SFP ports, and so on.
Switch# show log link-flap [port_number] clear		Remove all logs of the triggered event for the specified port.
Switch(config)# show log link-flap [port_number]	[port_number]	Show the specific port's log history of trigger events such as the port link flap (a port's linkdown or linkup), the count of port's port link flap, the reason that causes these triggered events, the time duration that the port

		link flap lasts, Rx power(dBm) of SFP ports, and so on.
Switch(config)# show log link-flap [port_number] clear		Remove all logs of the triggered event for the specified port.

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.

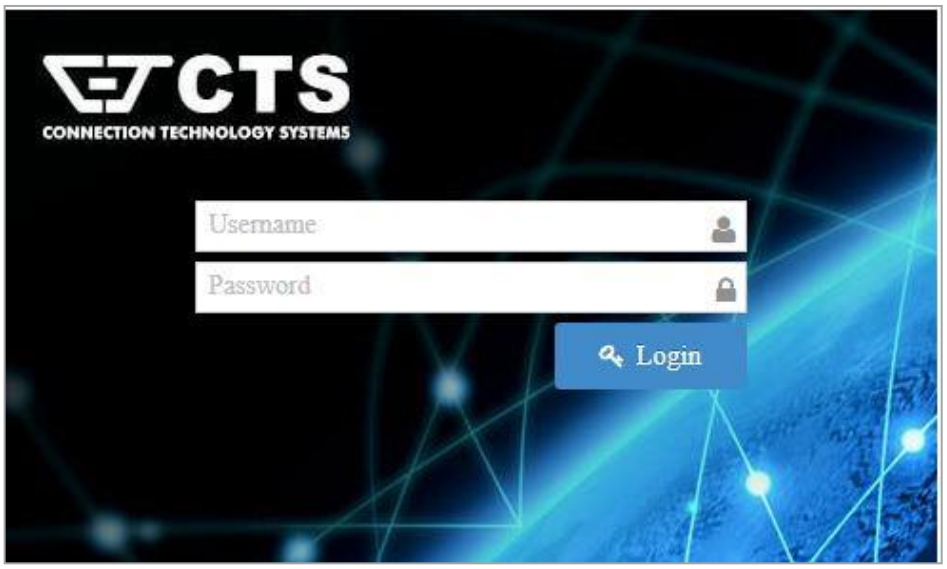
Trap: Trap is used by the managed device to report asynchronously a specified event to the SNMP Manager. When certain types of events occur, a managed device will send a trap to alert the SNMP Manager.
The system built-in management module also supports SNMP management. Users must install the MIB file 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.)

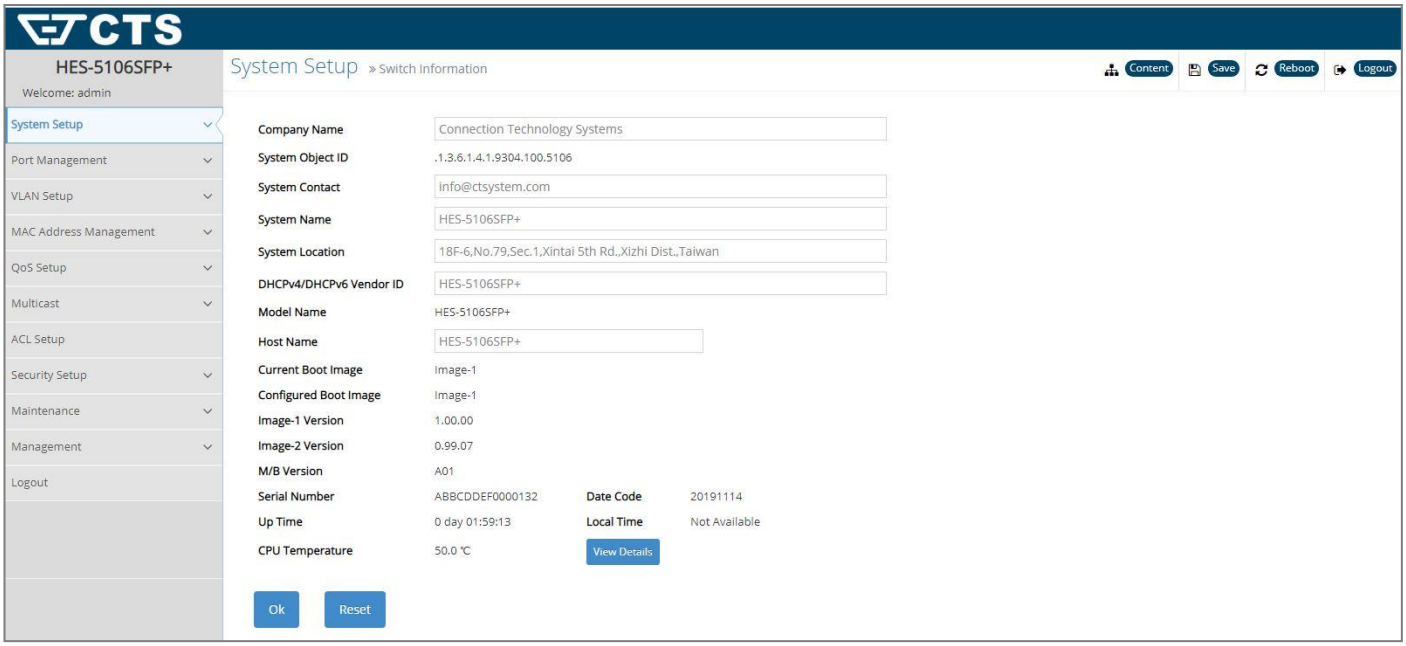
Initiate a web browser and input **http:**// **192.168.0.1** to enter the Managed Switch system. Once you gain the access, the following login window will appear. Also input the default administrator username ***admin*** and keep the administrator password field blank (By default, no password is required.)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

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.

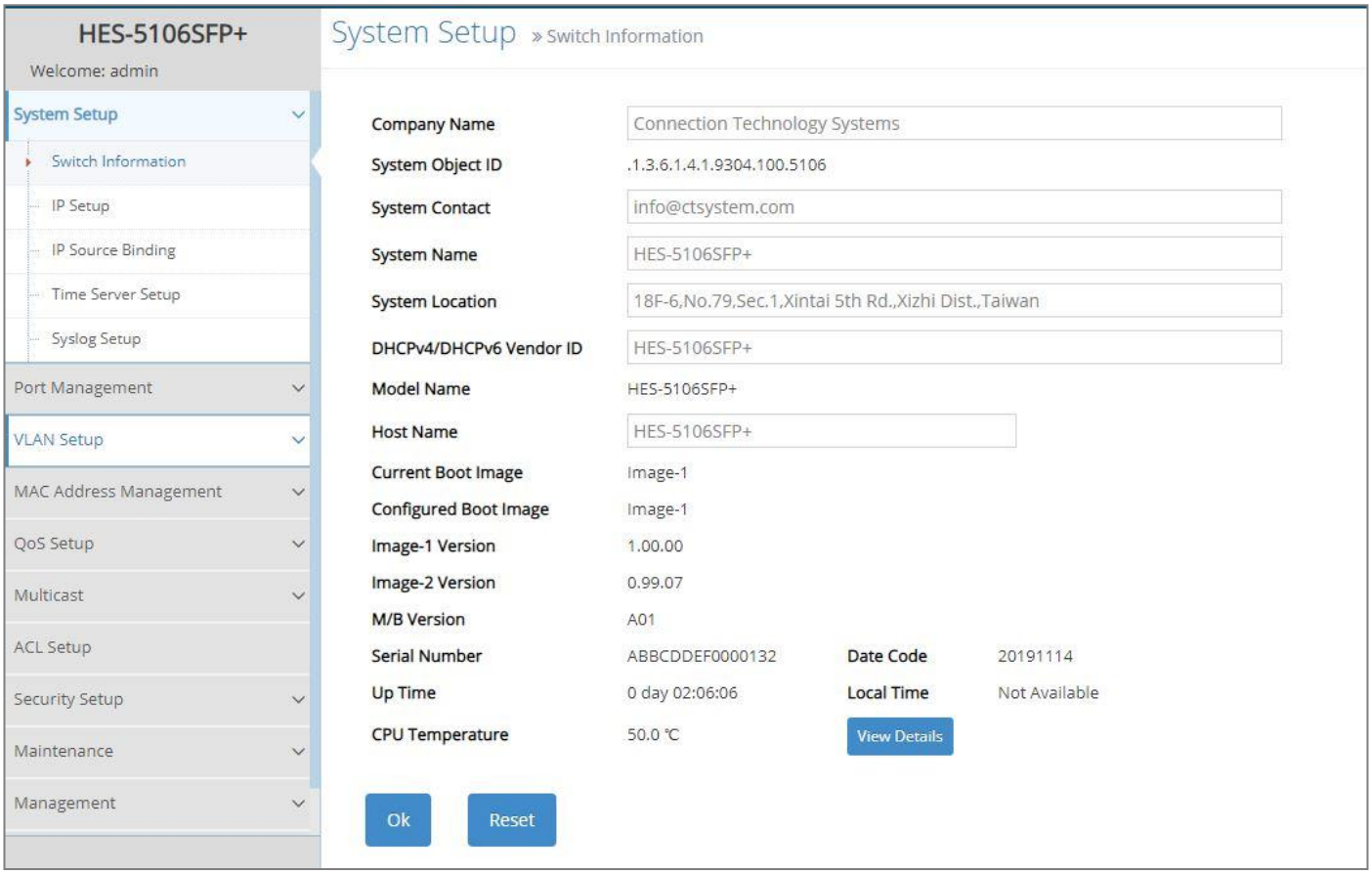


In the Main Menu, there are 11 main functions, including System Setup, Port Management, VLAN Setup, MAC Address Management, QoS Setup, Multicast, ACL Setup, Security Setup, Maintenance, Management and Logout contained. We will respectively describe their sub-functions in the following sections of this 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.
- **VLAN Setup:** Set up VLAN mode as well as VLAN configuration, and view the IEEE802.1q VLAN Table of the Managed Switch.
- **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 and static multicast 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, static IPv4/IPv6 table configuration, and so on.
- **Maintenance:** View the operation status and event logs of the system, ping, etc..
- **Management:** Enable or disable the specified network services, 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.

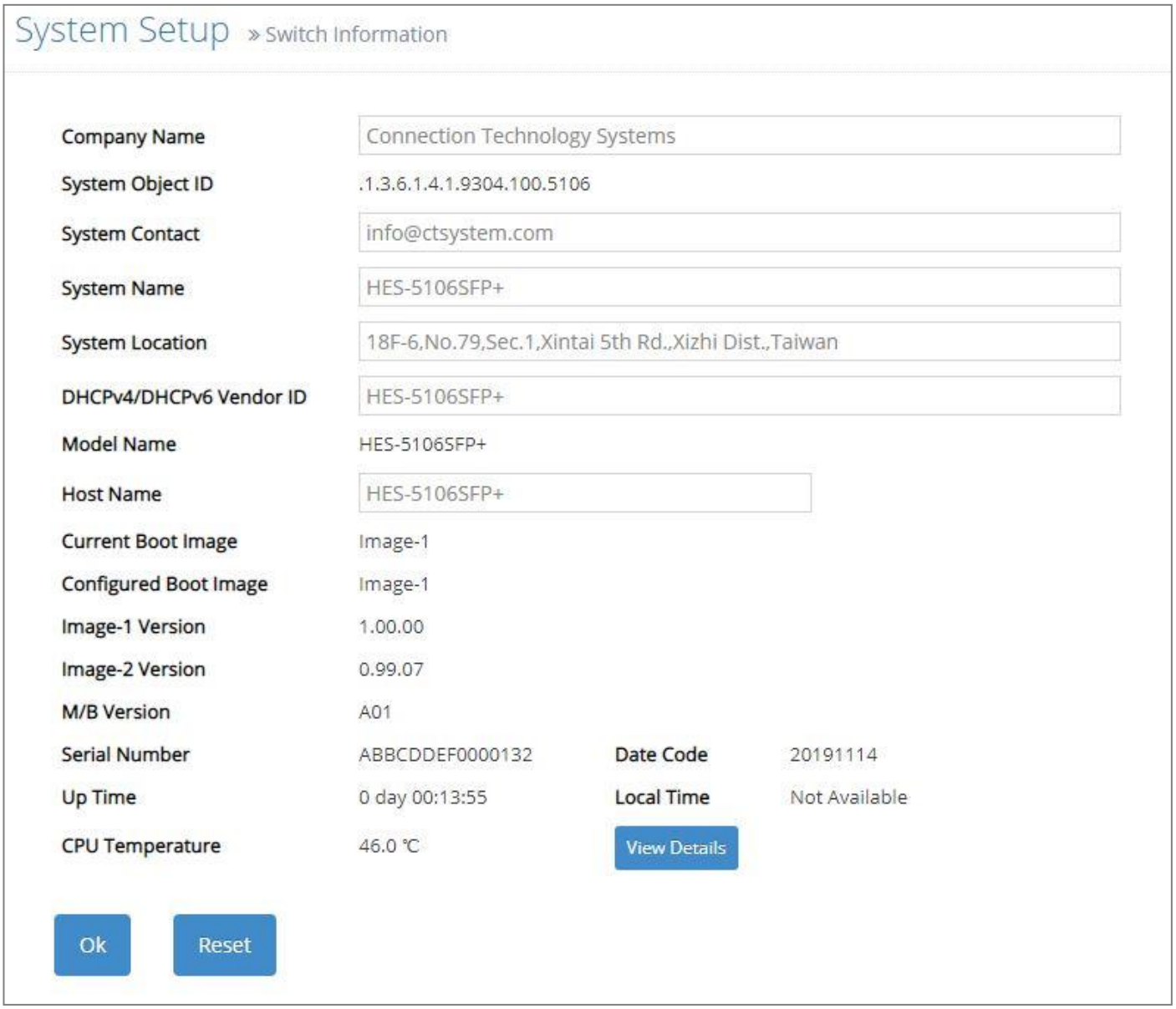
3. **IP Source Binding:** Set up the IP address for source binding.

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.

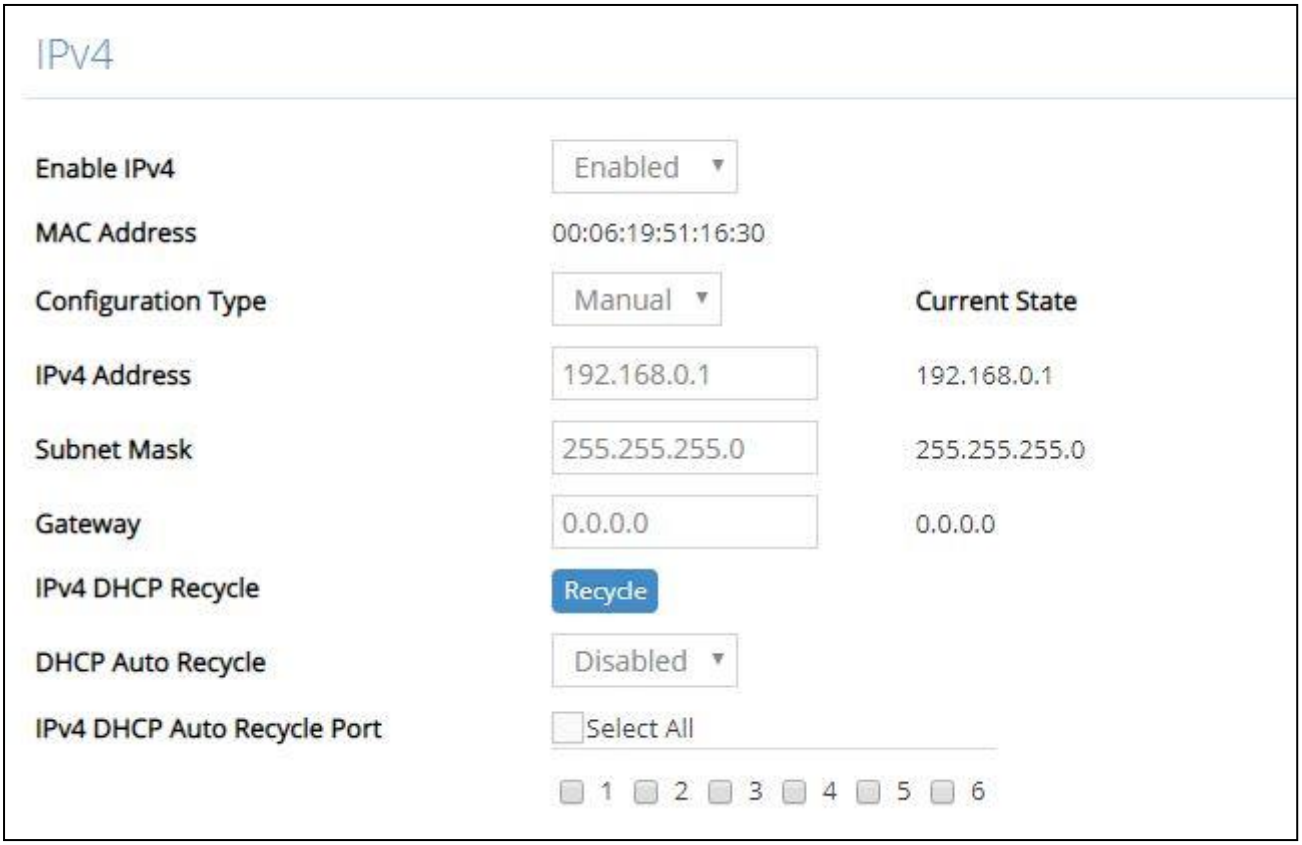
Up Time: Display the up time since last restarting.

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**.

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.

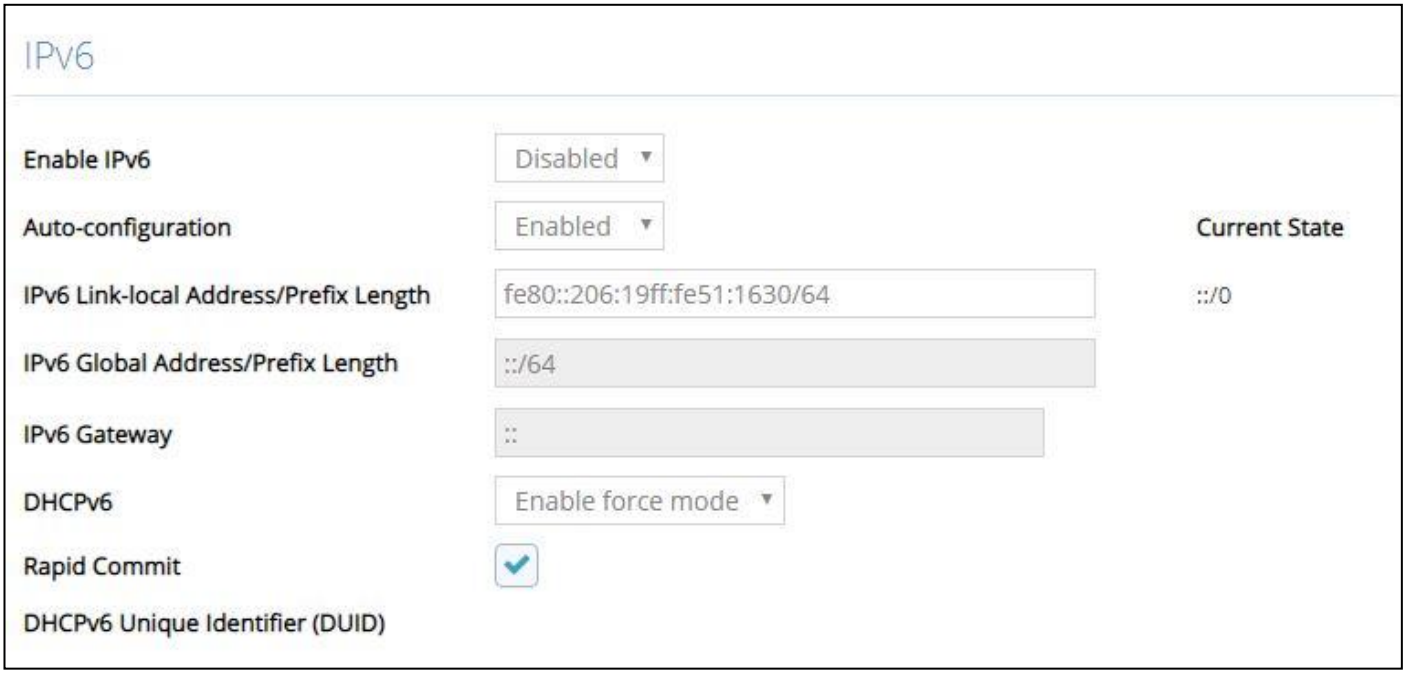
IPv4 DHCP Recycle: Click on **Recycle** manually, DHCP Release packets and Discover packets will be sent to DHCP server. And it will ask for IP address from DHCP server again. Please note that this parameter is just one-time setting and will not be saved into the configuration file of the Managed Switch.

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. 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,

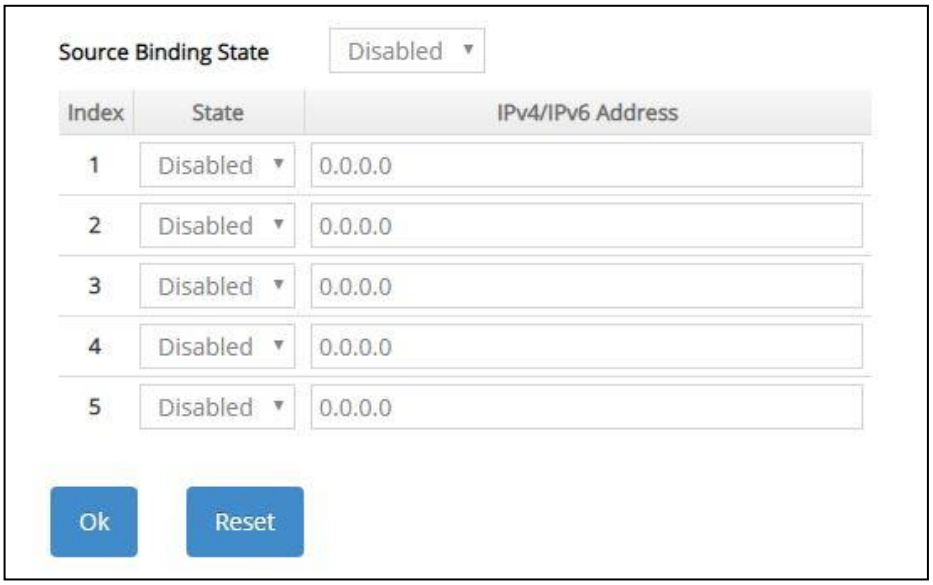
DHCPv6 Unique Identifier (DUID): View-only field that shows the DHCP Unique Identifier (DUID).

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.

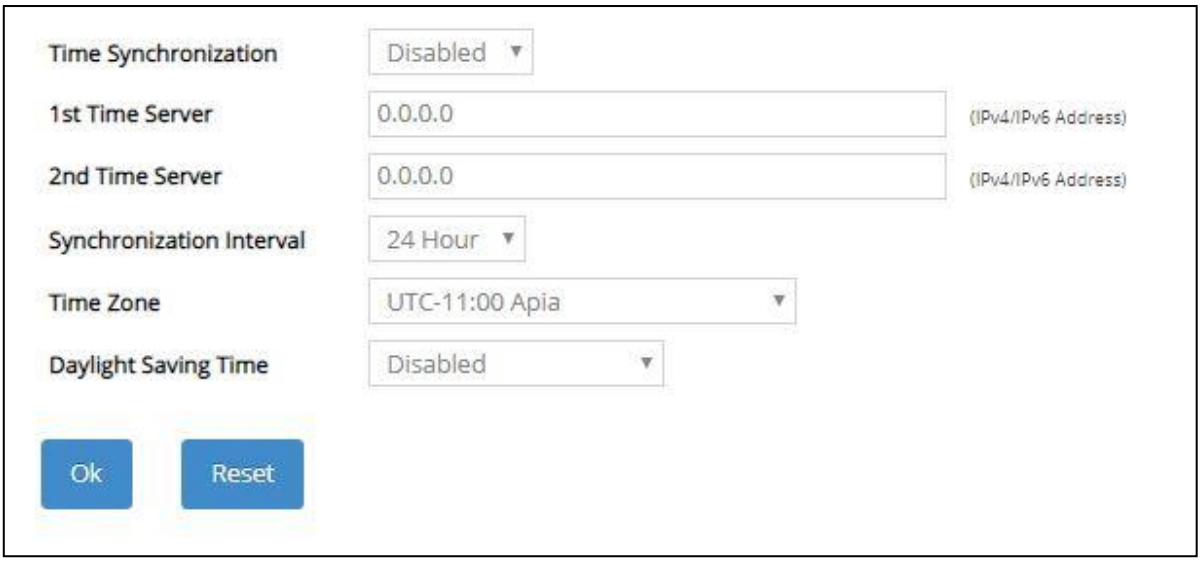
State: Disable or enable the assigned IP address to reach the management.

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.

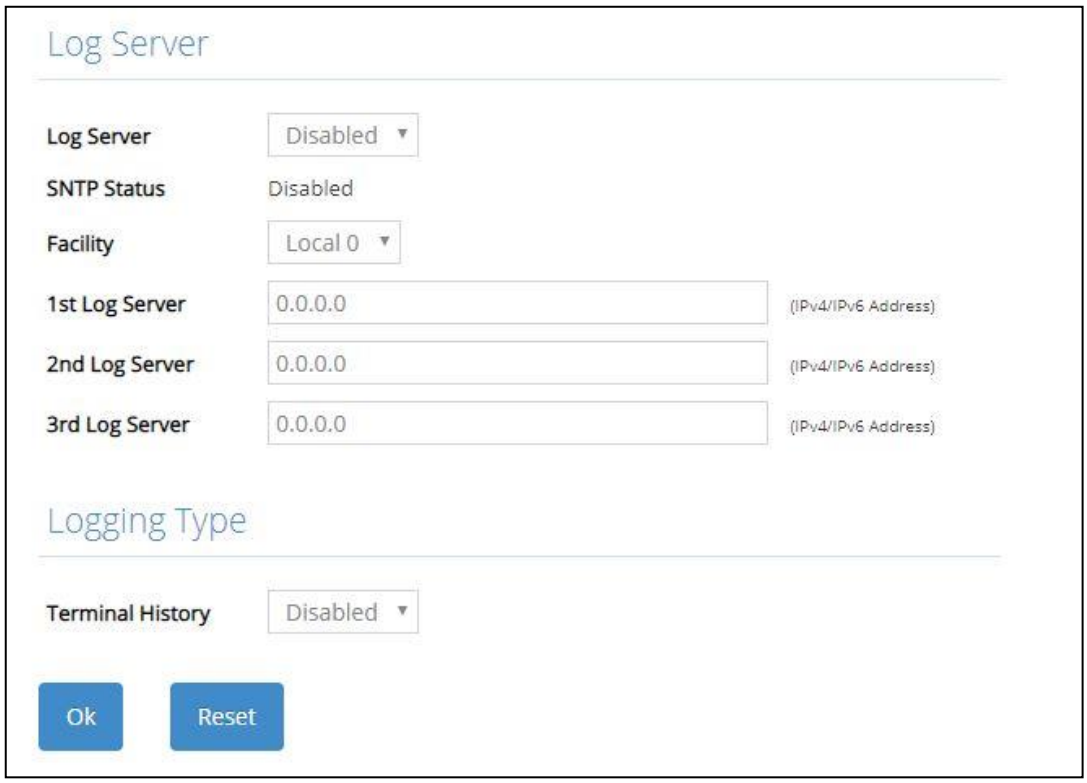
Daylight Saving Time Recurring Star: If the "recurring / Weekday" option is selected in Daylight Saving Time, click the pull-down menu to select the recurring start date of daylight saving time.

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.

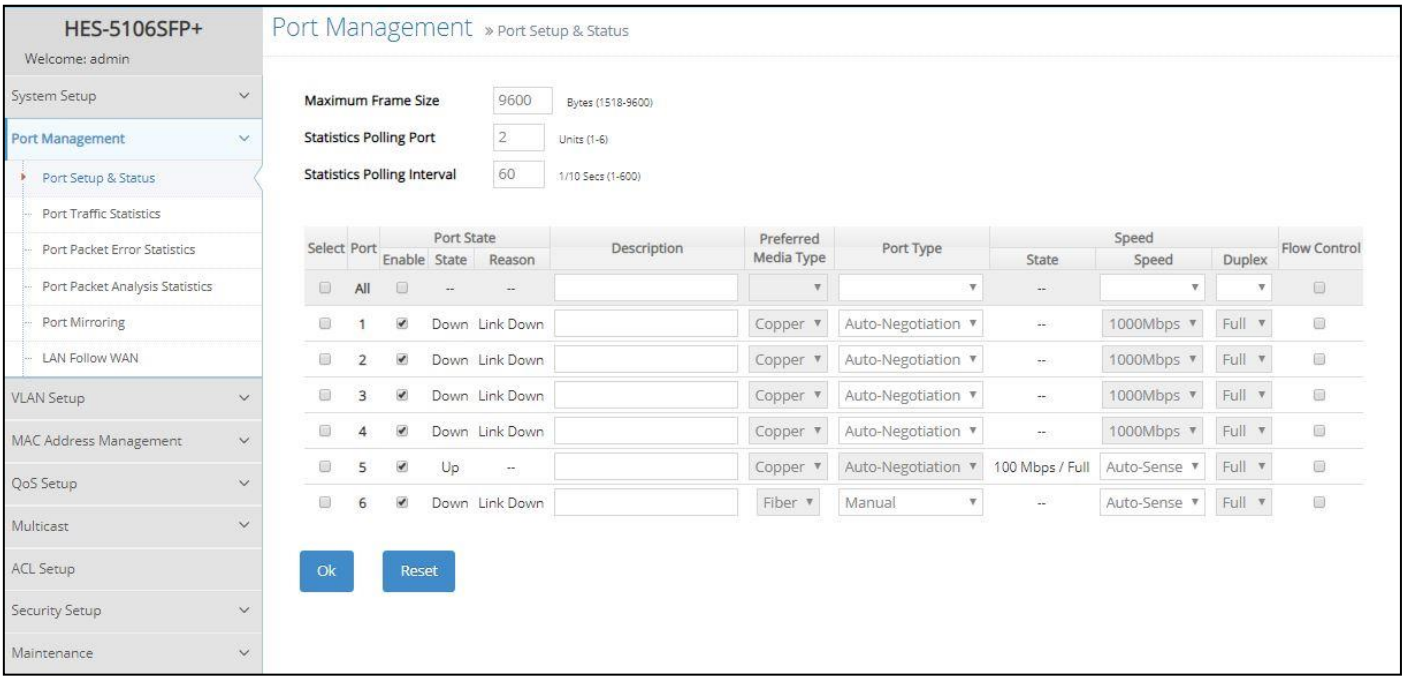
2nd Log Server: Specify the secondary log server's IPv4/IPv6 address. When the first log server is down, the Managed Switch will automatically contact the second or third Log server.

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.

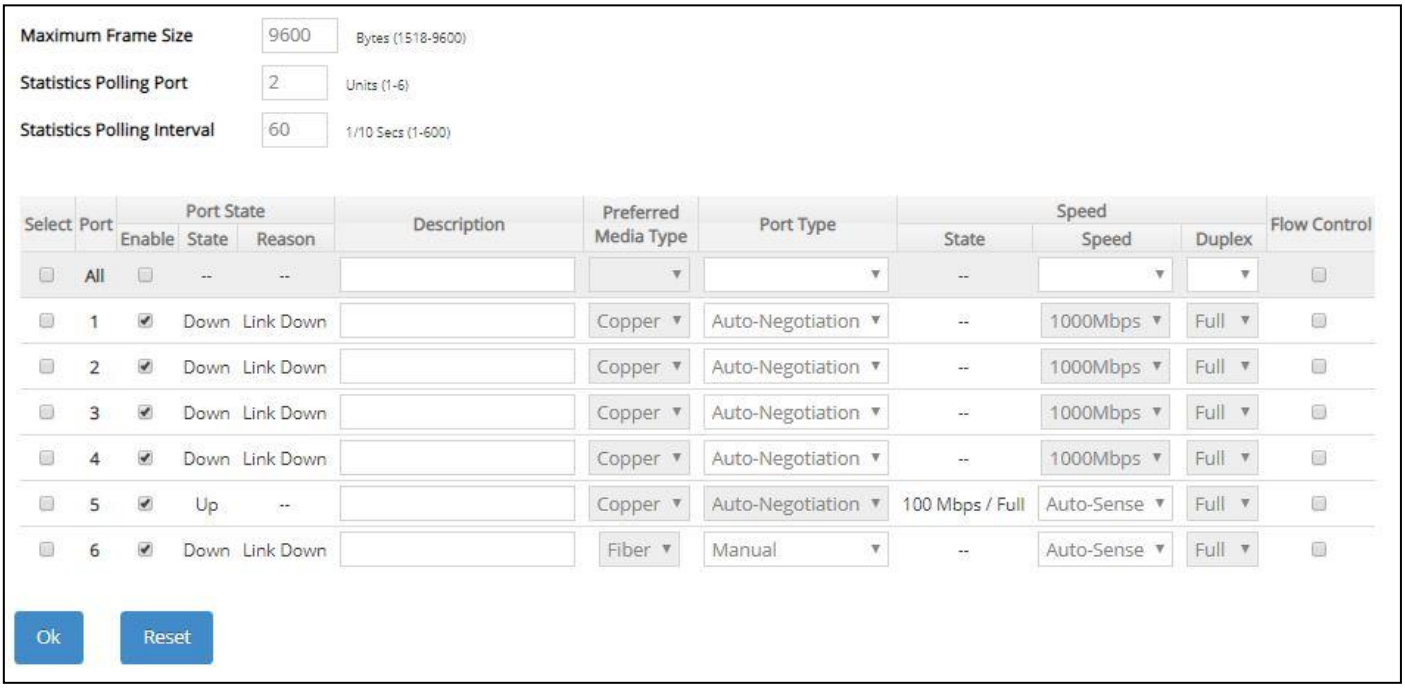
4. **Port Packet Analysis Statistics:** View each port's traffic analysis of packets, e.g. RX/TX frames of Multicast and Broadcast, etc.

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

6. **LAN Follow WAN:** Set up the specified LAN port(s) to follow WAN port's linkup/linkdown.

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 you can also configure the desired ports at a time by checking these ports, the new settings configured in the row of **All** port will be applied to these specified 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 10Mbps/100Mbps/1000Mbps in 1-4 TP port(s), 100Mbps/1000Mbps/2.5G/5G/10G in NBase-T Port 5 and 1000Mbps/10Gbps in SFP+ Port 6, 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 (10Mbps/100Mbps/1000Mbps) of 1-4 TP port(s) and (auto-sense/1000Mbps/10Gbps) of SFP+ Port 6.

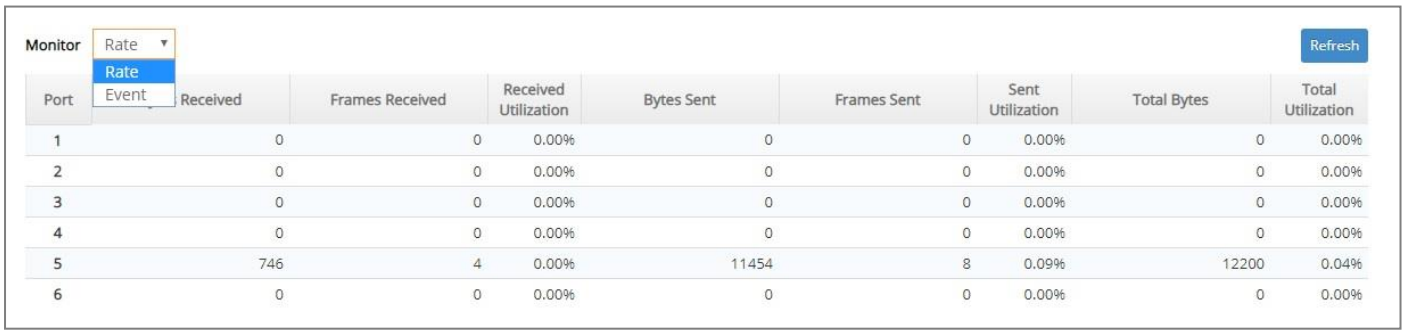
When you select “Auto-Negotiation” as port type for NBase-T Port 5 or SFP+ Port 6, 4-speed option (auto-sense/1000Mbps/2.5G/5G/10G) is supported in NBase-T Port 5 and the transmission speed of SFP+ Port 6 is 1000Mbps.

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.



Port	Received	Frames Received	Received Utilization	Bytes Sent	Frames Sent	Sent Utilization	Total Bytes	Total Utilization
1	0	0	0.00%	0	0	0.00%	0	0.00%
2	0	0	0.00%	0	0	0.00%	0	0.00%
3	0	0	0.00%	0	0	0.00%	0	0.00%
4	0	0	0.00%	0	0	0.00%	0	0.00%
5	746	4	0.00%	11454	8	0.09%	12200	0.04%
6	0	0	0.00%	0	0	0.00%	0	0.00%

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.

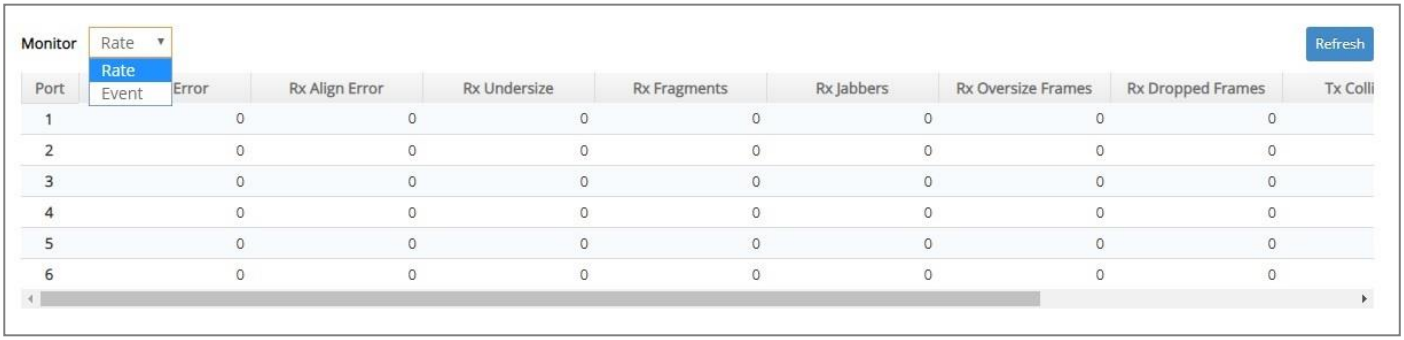
Refresh: Click **Refresh** to update the latest port traffic statistics.

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.

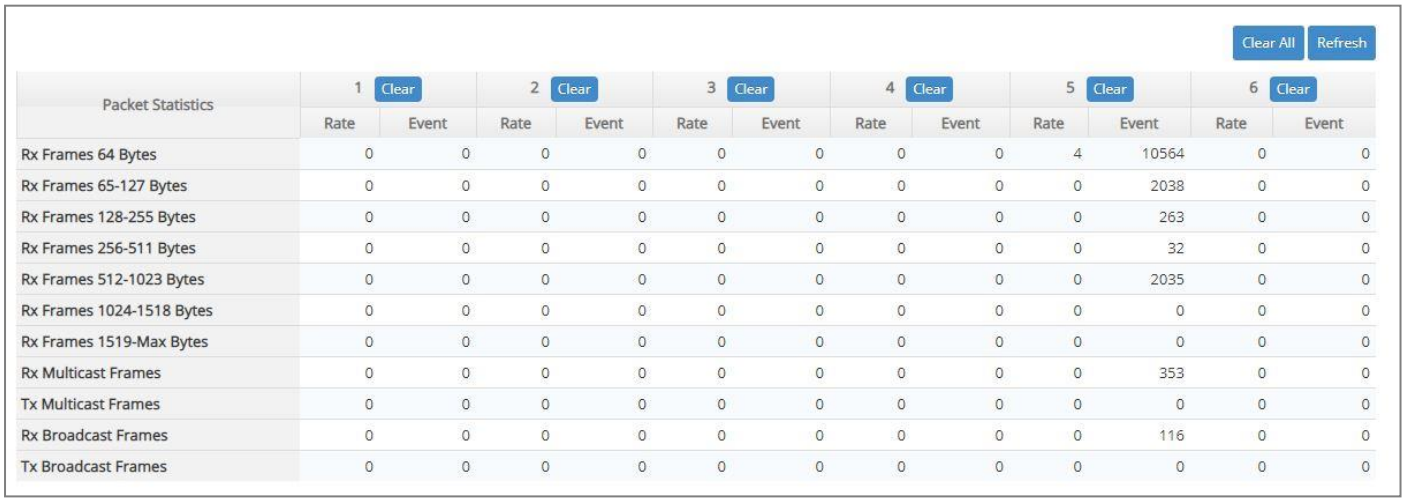
Refresh: Click **Refresh** to update the latest port packet error statistics.

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.



Packet Statistics	1 Clear		2 Clear		3 Clear		4 Clear		5 Clear		6 Clear	
	Rate	Event	Rate	Event	Rate	Event	Rate	Event	Rate	Event	Rate	Event
Rx Frames 64 Bytes	0	0	0	0	0	0	0	0	4	10564	0	0
Rx Frames 65-127 Bytes	0	0	0	0	0	0	0	0	0	2038	0	0
Rx Frames 128-255 Bytes	0	0	0	0	0	0	0	0	0	263	0	0
Rx Frames 256-511 Bytes	0	0	0	0	0	0	0	0	0	32	0	0
Rx Frames 512-1023 Bytes	0	0	0	0	0	0	0	0	0	2035	0	0
Rx Frames 1024-1518 Bytes	0	0	0	0	0	0	0	0	0	0	0	0
Rx Frames 1519-Max Bytes	0	0	0	0	0	0	0	0	0	0	0	0
Rx Multicast Frames	0	0	0	0	0	0	0	0	0	353	0	0
Tx Multicast Frames	0	0	0	0	0	0	0	0	0	0	0	0
Rx Broadcast Frames	0	0	0	0	0	0	0	0	0	116	0	0
Tx Broadcast Frames	0	0	0	0	0	0	0	0	0	0	0	0

RX Frames 64 Bytes: 64 bytes frames received.

RX Frames 65-127 Bytes: 65-127 bytes frames received.

RX Frames 128-255 Bytes: 128-255 bytes frames received.

RX Frames 256-511 Bytes: 256-511 bytes frames received.

RX Frames 512-1023 Bytes: 512-1023 bytes frames received.

RX Frames 1024-1518 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.

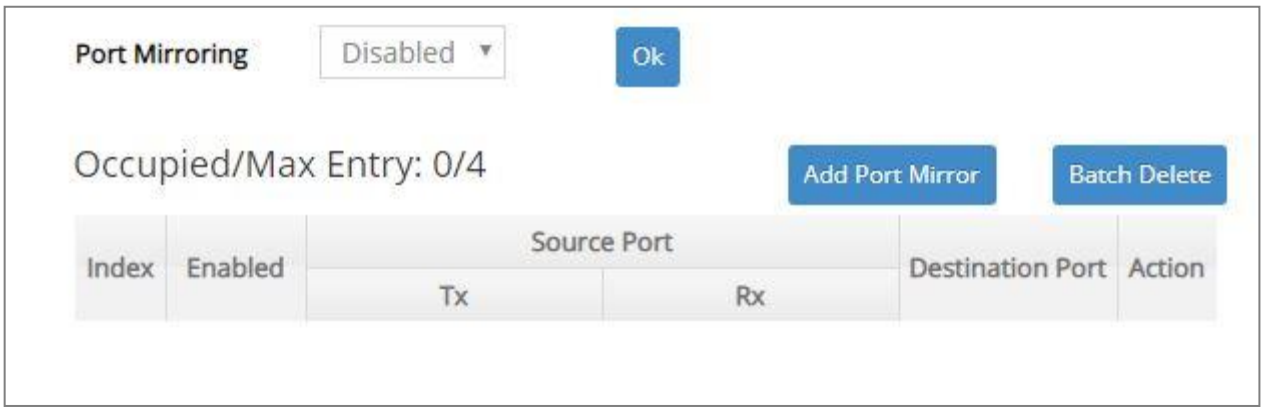
Refresh: Click **Refresh** to update the latest port packet analysis statistics.

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, 3-4) 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, 3-4) 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 6 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.

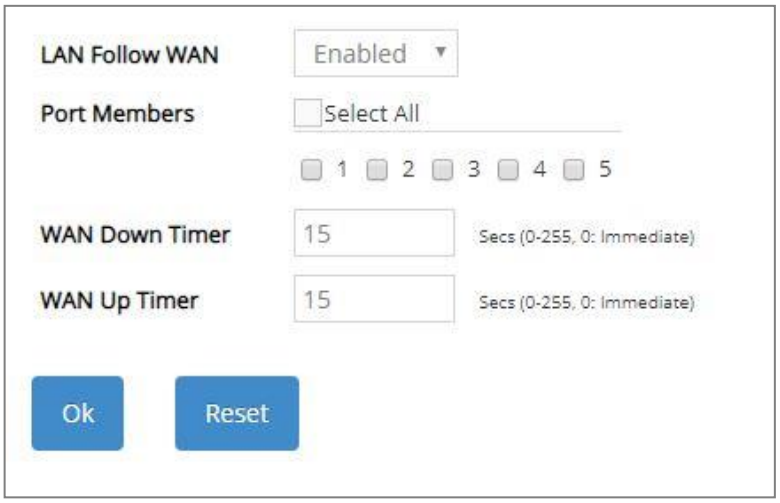
Click the icon to modify the settings of a specified port mirroring.

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.

4.2.6 LAN Follow WAN

With the lan-follow-wan function, the device(s) connected with the LAN port(s) of the Managed Switch can be immediately triggered by its link-up WAN port (SFP+ port that is located at the rear panel of the Managed Switch) switched from link-down into link-up status in order to obtain the new DHCP IP address and the related update information, such as the firmware or the configuration file, from the DHCP server.

Select the option **LAN Follow WAN** from the **Port Management** menu and then the following screen page appears.



LAN Follow WAN: Enable or disable the lan-follow-wan function globally.

Port Members: Click on the checkbox of corresponding port number to enable the lan-follow-wan function on the specific port(s). Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

WAN Down Timer: Specify the timer to count down in order to trigger the specific LAN port(s) to do the link down when WAN port's link is down. Vaild range: 0~255 (seconds). "0" stands for "immediate".

WAN Up Timer: Specify the timer to count down in order to trigger the specific LAN port(s) to do the link up when WAN port's link is up. Vaild range: 0~255 (seconds). "0" stands for "immediate".

4.3 VLAN Setup

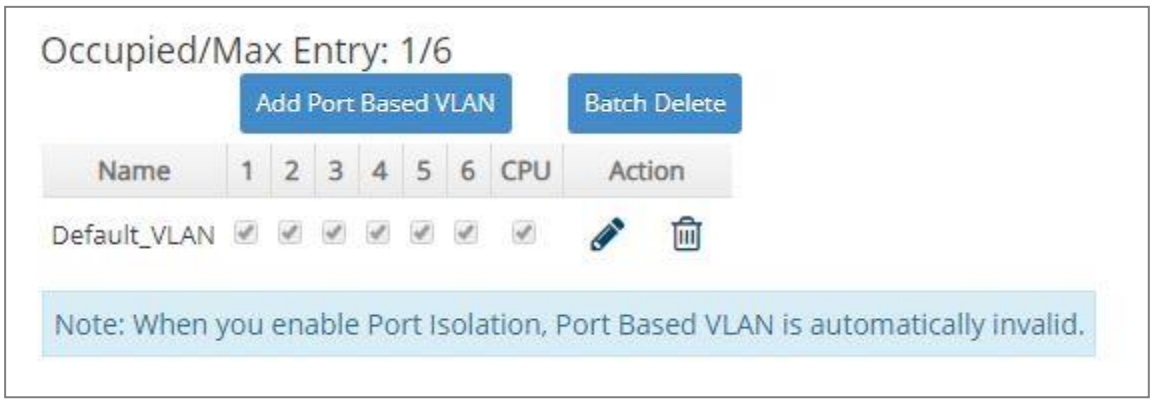
A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast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

4.3.1 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.

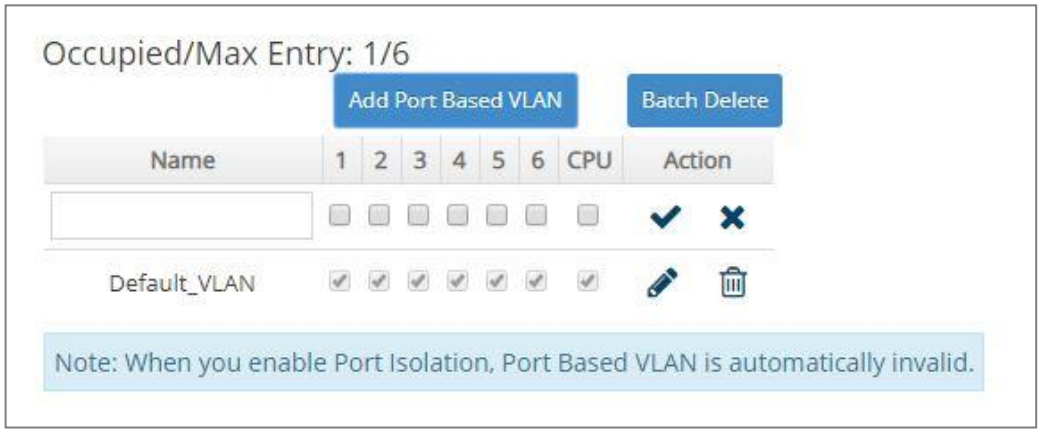


Since source addresses of the packets are listed in MAC address table of specific VLAN (except broadcast/multicast packets), in every VLAN the traffic between two ports will be two-way without restrictions.

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 6.

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.

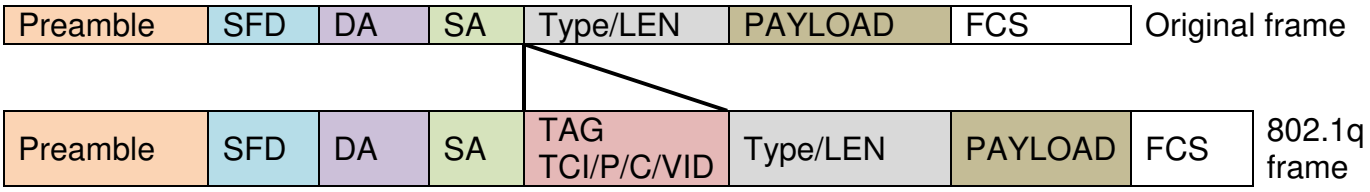
Click when the settings are completed, this new Port-Based VLAN will be listed on the Port-Based VLAN table, or click to cancel the settings.

4.3.2 802.1Q 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.

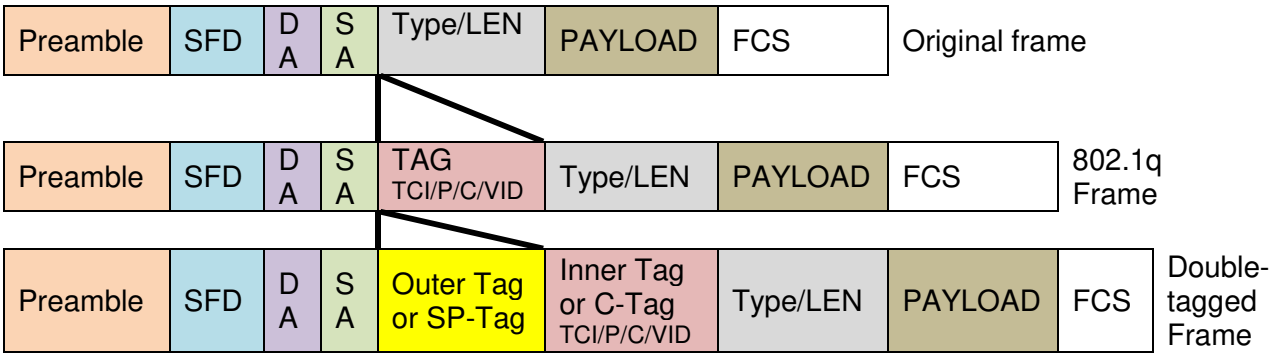
Example : PortX configuration

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)

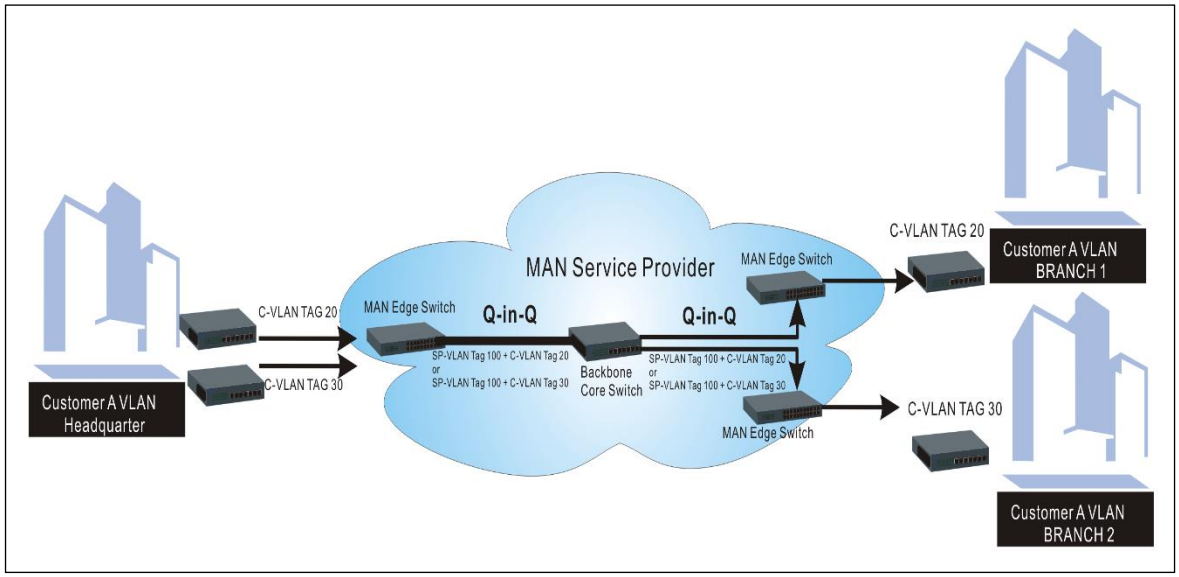
4.3.3 Introduction to Q-in-Q (DOT1Q-Tunnel)

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

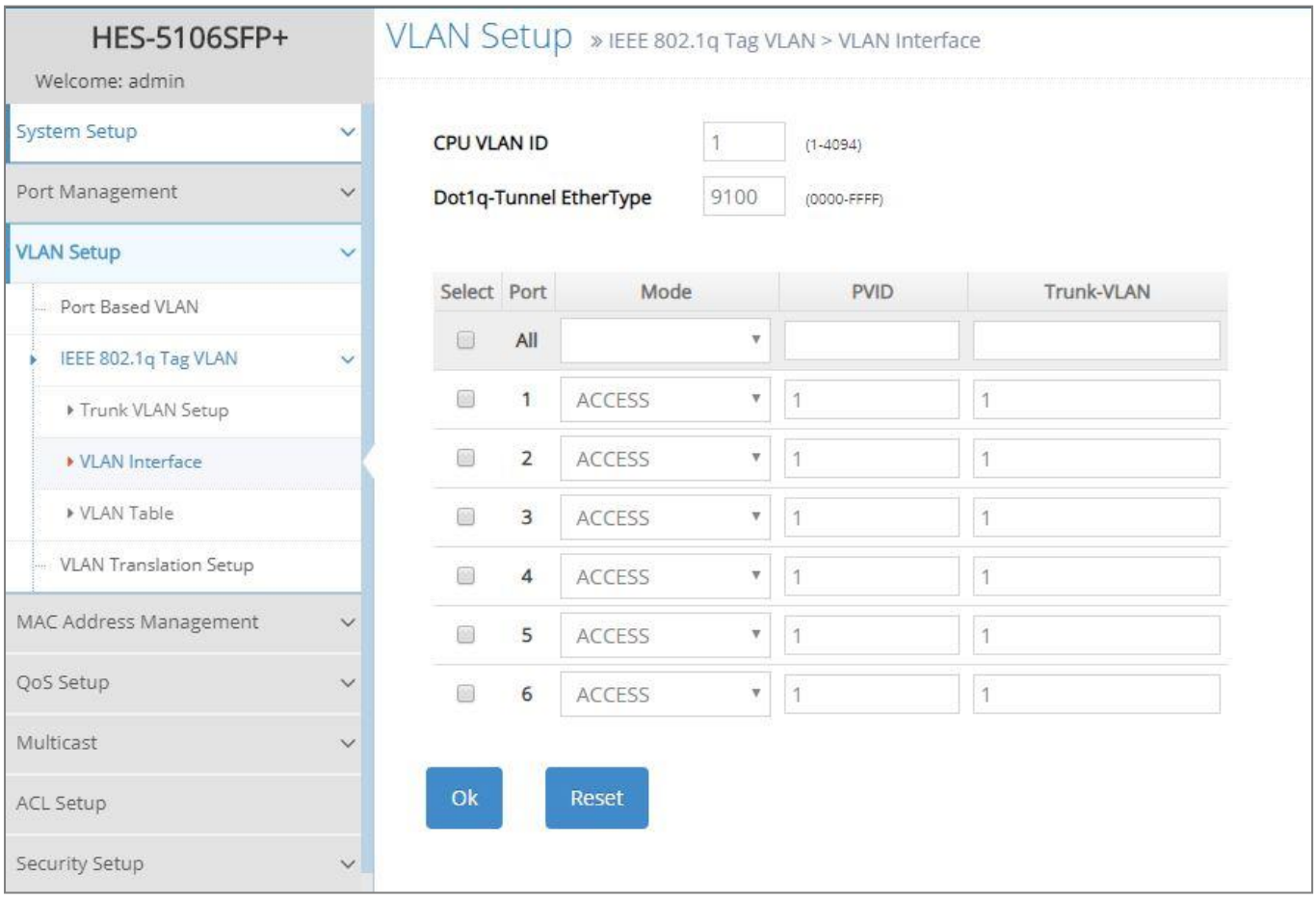
As shown below in “Q-in-Q Example” illustration, Headquarter A wants to communicate with Branch 1 that is 1000 miles away. One common thing about these two locations is that they have the same VLAN ID of 20, called C-VLAN (Customer VLAN). Since customer traffic will be routed to service provider’s backbone, 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

4.3.4 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.



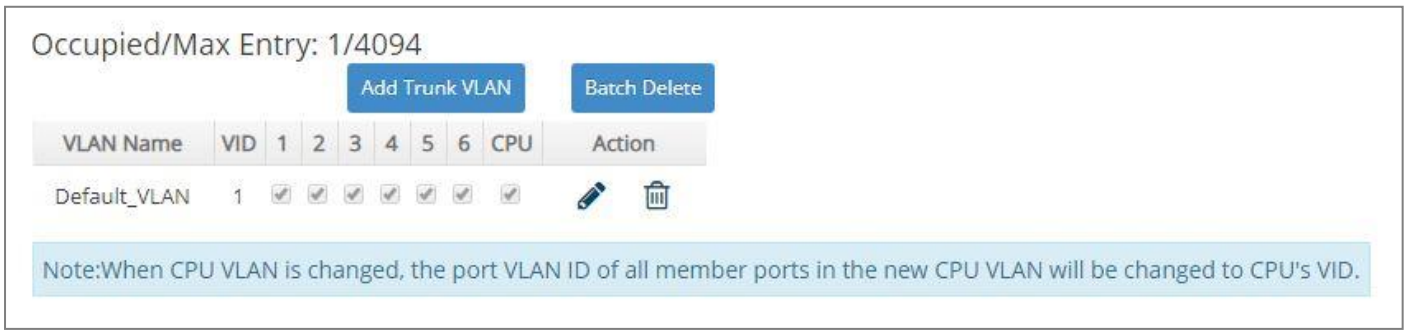
1. **Trunk VLAN Setup:** To create, modify or remove IEEE 802.1q Tag VLAN settings.

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.

4.3.4.1 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.

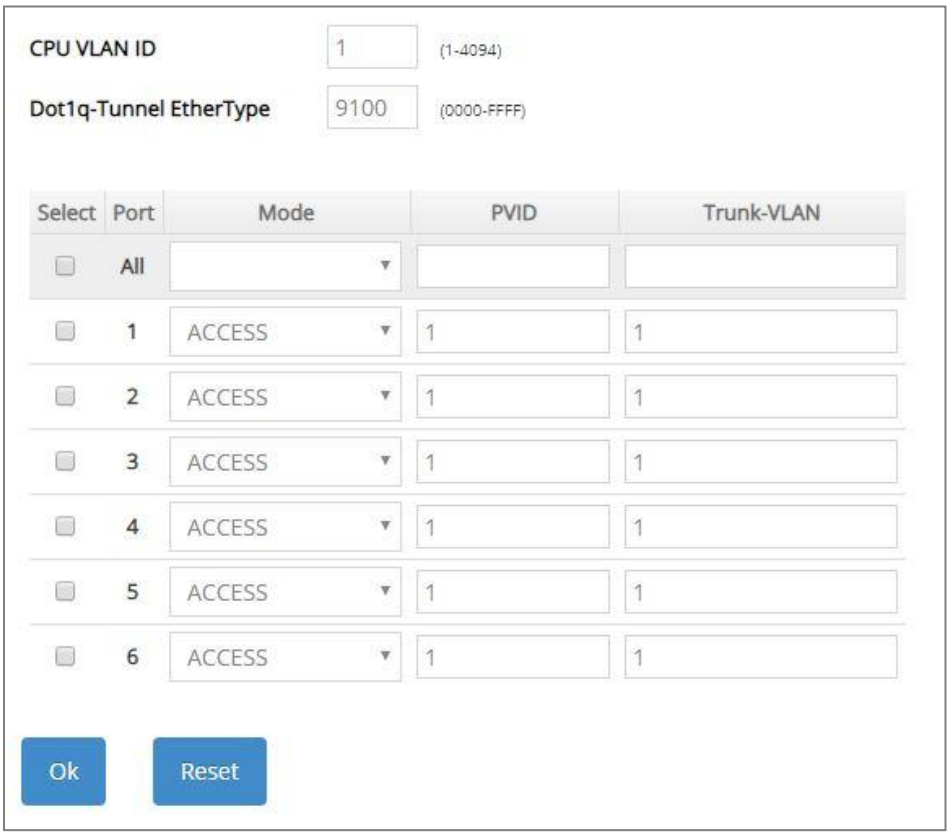
VID: Specify the VLAN ID of the VLAN. Valid range: 1-4094.

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.

4.3.4.2 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 you can also configure the desired ports at a time by checking these ports, the new settings configured in the row of **All** port will be applied to these specified 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).

4.3.4.3 IEEE 802.1q VLAN Table

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

VLAN Name: View-only field that shows the VLAN name.

VID: View-only field that shows the ID of the VLAN.

4.3.5 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 44 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 44.

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 4.3.4.2 “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.

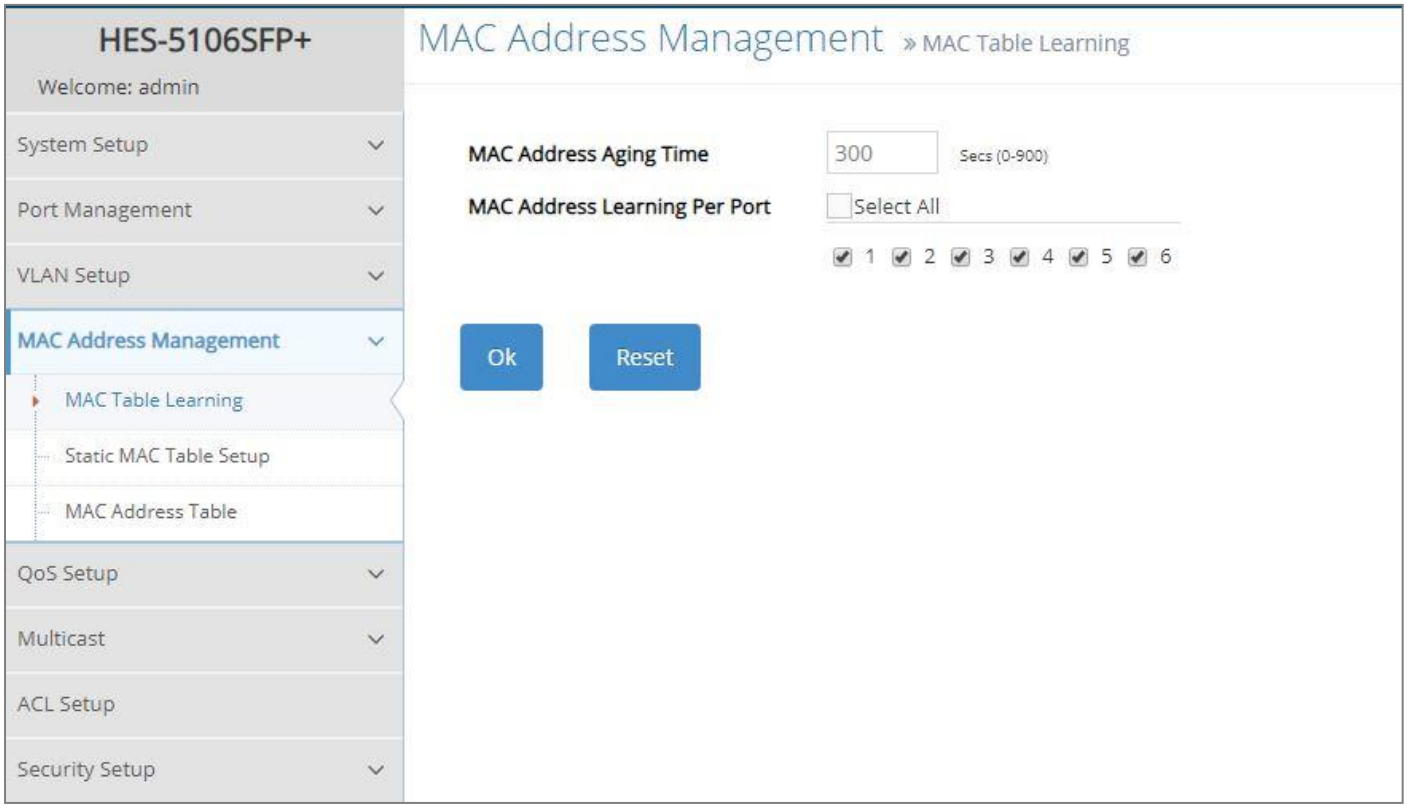
Click ✔ when the settings are completed, this new rule will be listed on the VLAN mapping rule table, or click ✖ to cancel the settings.

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 MAC Address Management

Select the folder **MAC Address Management** from the **Main Menu** and then 3 options will be displayed for your selection.



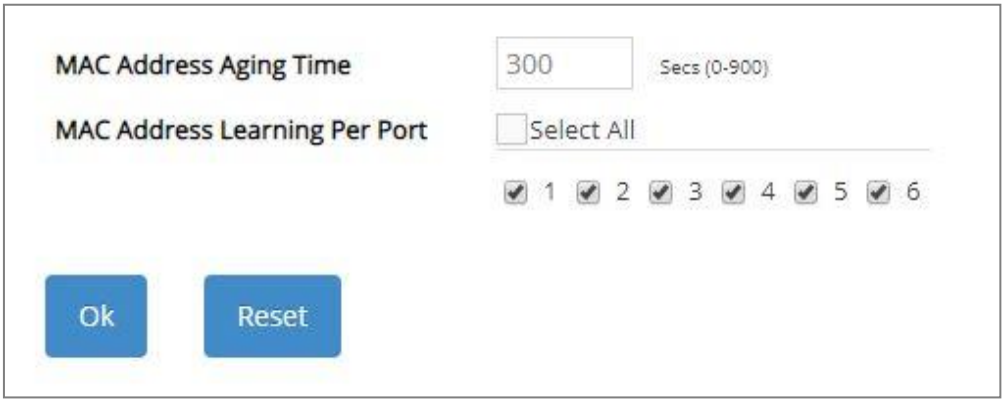
1. **MAC Table Learning:** Set up MAC address table aging time, and enable/disable MAC address learning function.

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.

4.4.1 MAC Table Learning

Click the option **MAC Table Learning** from the **MAC Address Management** menu and then the following screen page appears.

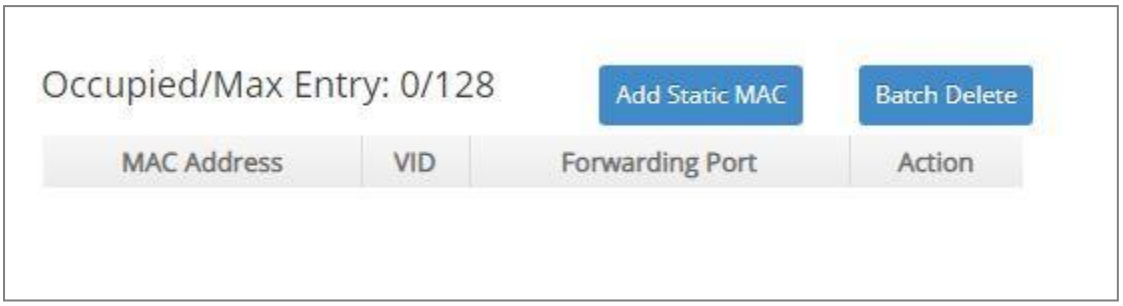


MAC Address Aging Time: Specify MAC address table aging time between 0 and 900 seconds. “0” means that MAC addresses will never age out.

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. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

4.4.2 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 the static source MAC addresses, which are manually added by clicking on the **Add Static MAC** button.

These manually added MAC addresses denote that they have been written into the running configuration file. Thus, if the **Save Configuration** function is executed before rebooting the Managed Switch, they still exist on the static MAC table.

NOTE: *The Managed Switch only supports switch-based MAC security and does not support port-based MAC security. The Managed Switch can support up to 128 entries of MAC security list.*

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total static MAC address that have already been created.

Max: This shows the maximum number available for static MAC address of the Managed Switch. The maximum number is 128.

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: 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.

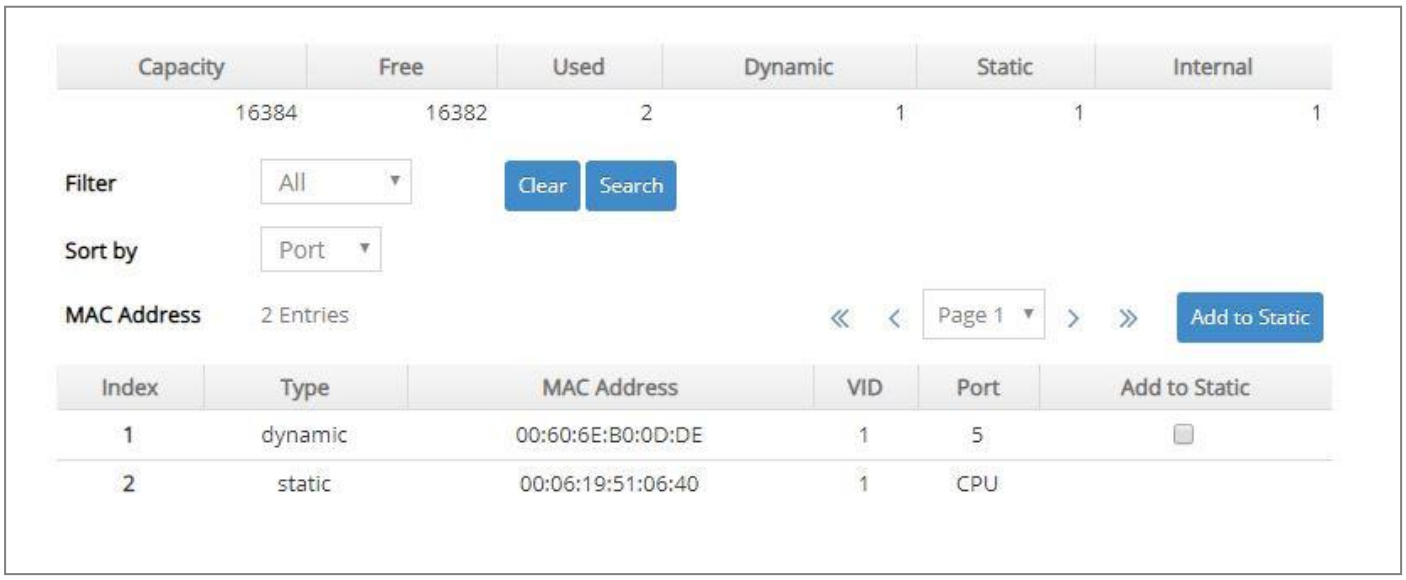
Click ✔ when the settings are completed, this new static MAC address will be listed on the static MAC address table, or click ✖ to cancel the settings.

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.

4.4.3 MAC Address Table

MAC Address Table displays MAC addresses learned 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 above is composed of the MAC addresses that are automatically learned from each port of Managed Switch or manually created by the users.

Click **Search** to update the MAC Address table by selecting **All**/**Port List**/**Static**/**MAC**/**VLAN** five conditions from **Filter** pull-down menu, and sort these searched MAC addresses by selecting **Port**/**MAC**/**VLAN** option from the **Sort by** pull-down menu.

Click **Clear** when choosing **All** condition to clear all dynamic MAC addresses in the MAC address table. Or click **Clear** when choosing **Port List** condition to clear the dynamic MAC addresses for the specified port(s).

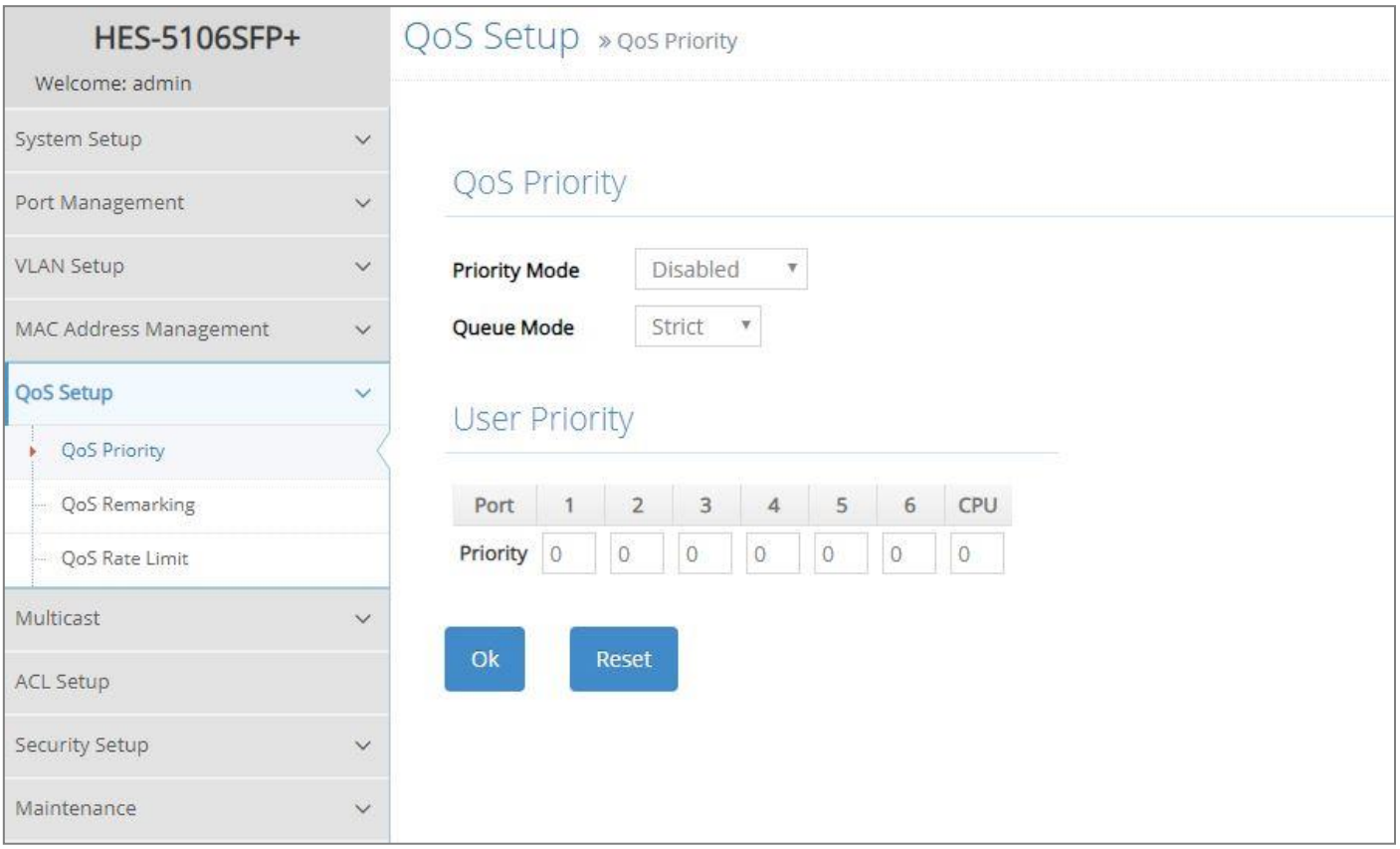
To transfer the MAC address type from “dynamic” into "static", please click on the checkbox belonging to the specific dynamic MAC address in the **Add to Static** field, and then press the **Add to Static** button located at the top-right corner of the table. The specified dynamic MAC address will be turned into a static one when clicking **Search** to refresh the MAC address table.

To view the 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.

4.5 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.



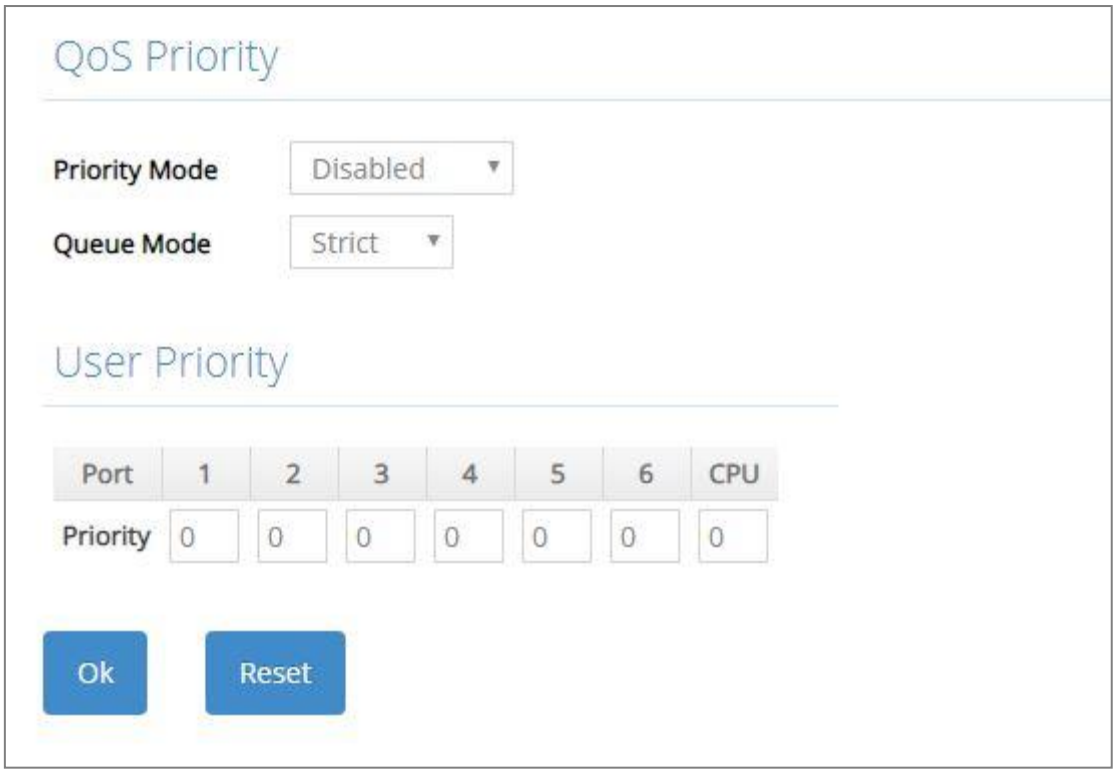
1. **QoS Priority:** To set up each port's QoS default class, Priority, Queuing Mode, Queue Weighted, and so on.

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.

4.5.1 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.

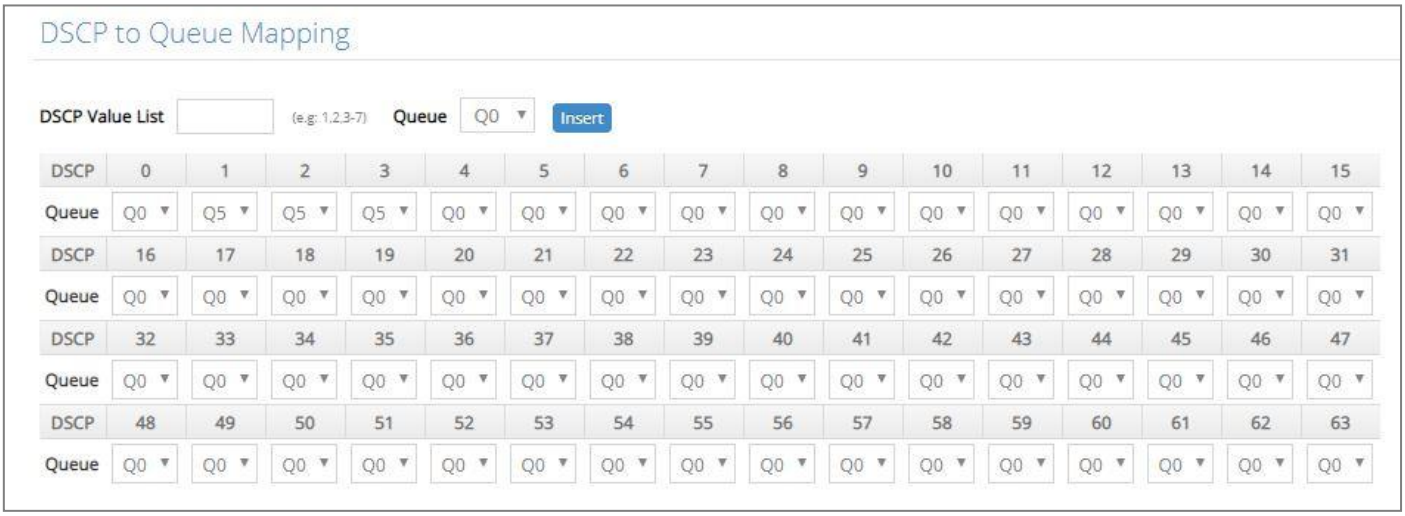
Strict: This indicates that services to the egress queues are offered in the sequential order and all traffic with higher priority queues is transmitted first before lower priority queues are serviced.

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:

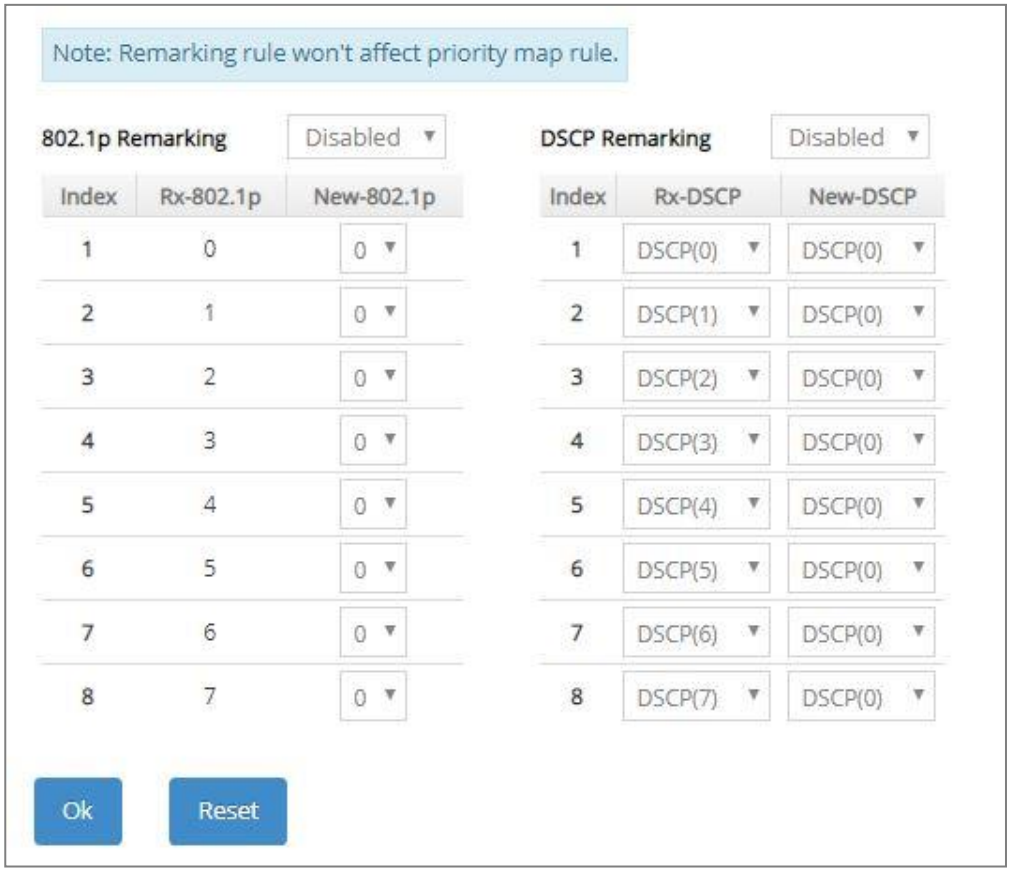
There are eight priority levels that you can choose to classify data packets. Specify one of the listed options for CoS (Class of Service) priority tag values. The default value is “0”.

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

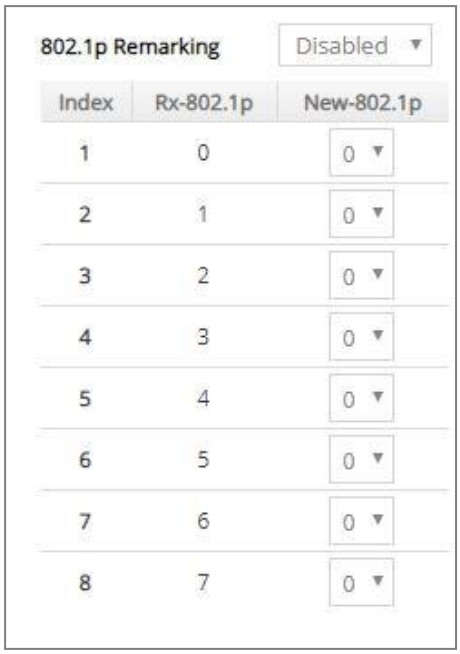
4.5.2 QoS Remarking

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.

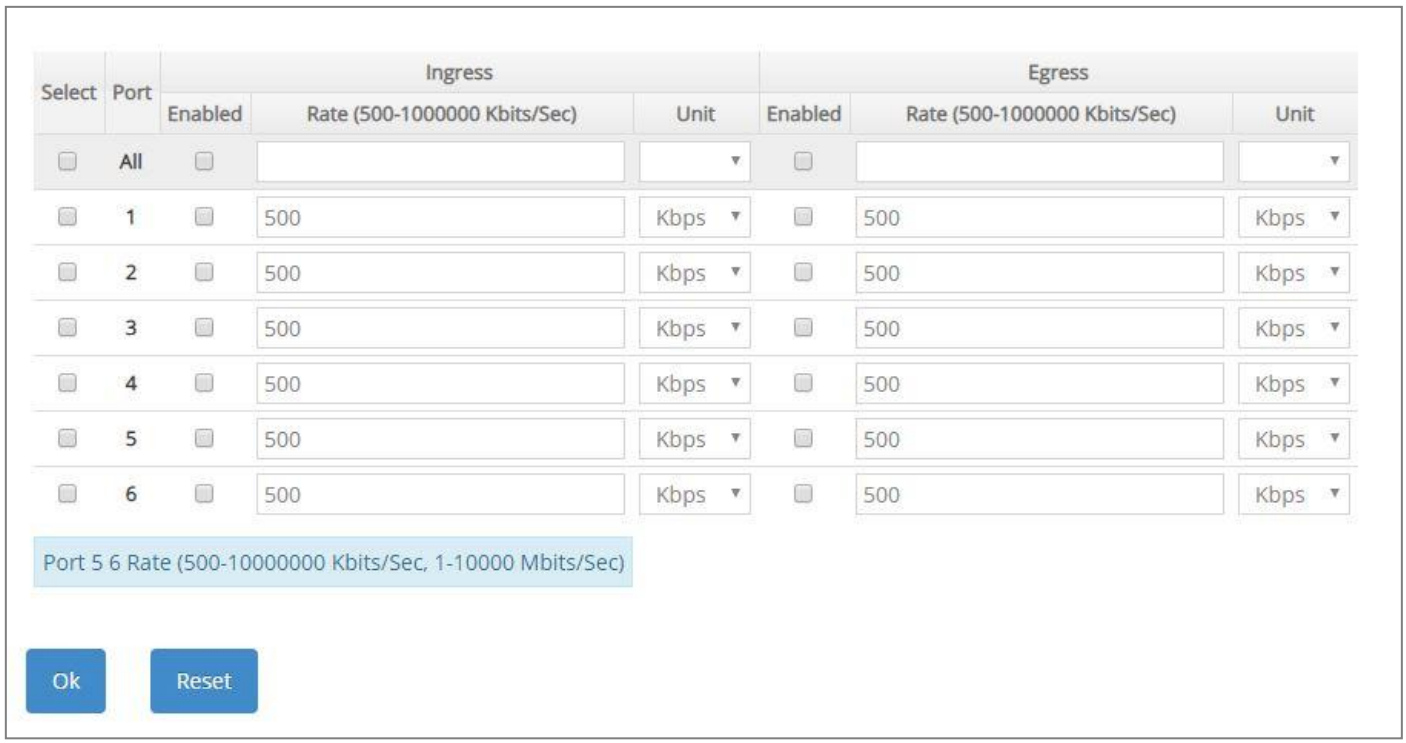


Configure DSCP Remarking:

This allows you to enable or disable DSCP remarking for each priority by pulling down the **DSCP Remarking** menu. The default setting is disabled.

4.5.3 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 you can also configure the desired ports at a time by checking these ports, the new settings configured in the row of **All** port will be applied to these specified 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 for Ports 1~4 and 500-10000000 in unit of Kbps or 1-10000 in unit of Mbps for Ports 5~6.

Unit in Ingress/Egress field**:** Either Kbps or Mbps can be selectd as the unit of the inbound and outbound bandwidth.

4.6 Multicast Configuration

Select the folder **Multicast** from the **Main Menu**, **IGMP/MLD Snooping** subfolder and **Static Multicast Setup** option for multicast setup will be displayed.

4.6.1 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.

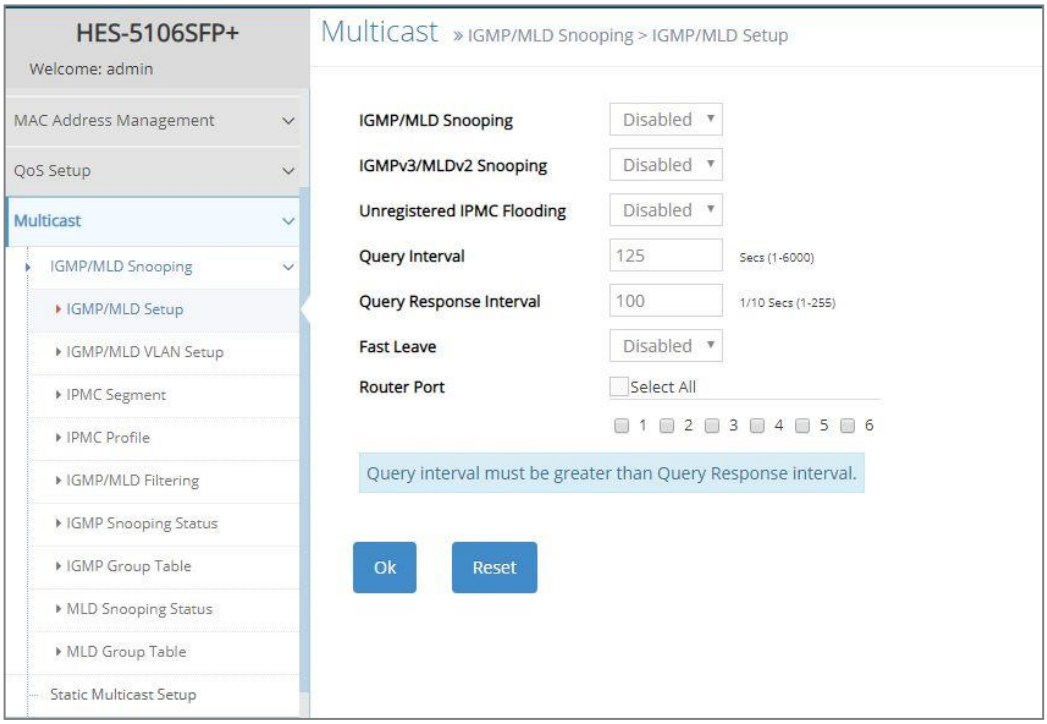
IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers by processing the layer 3 packets that IGMP packets sent in a multicast network.

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 9 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.

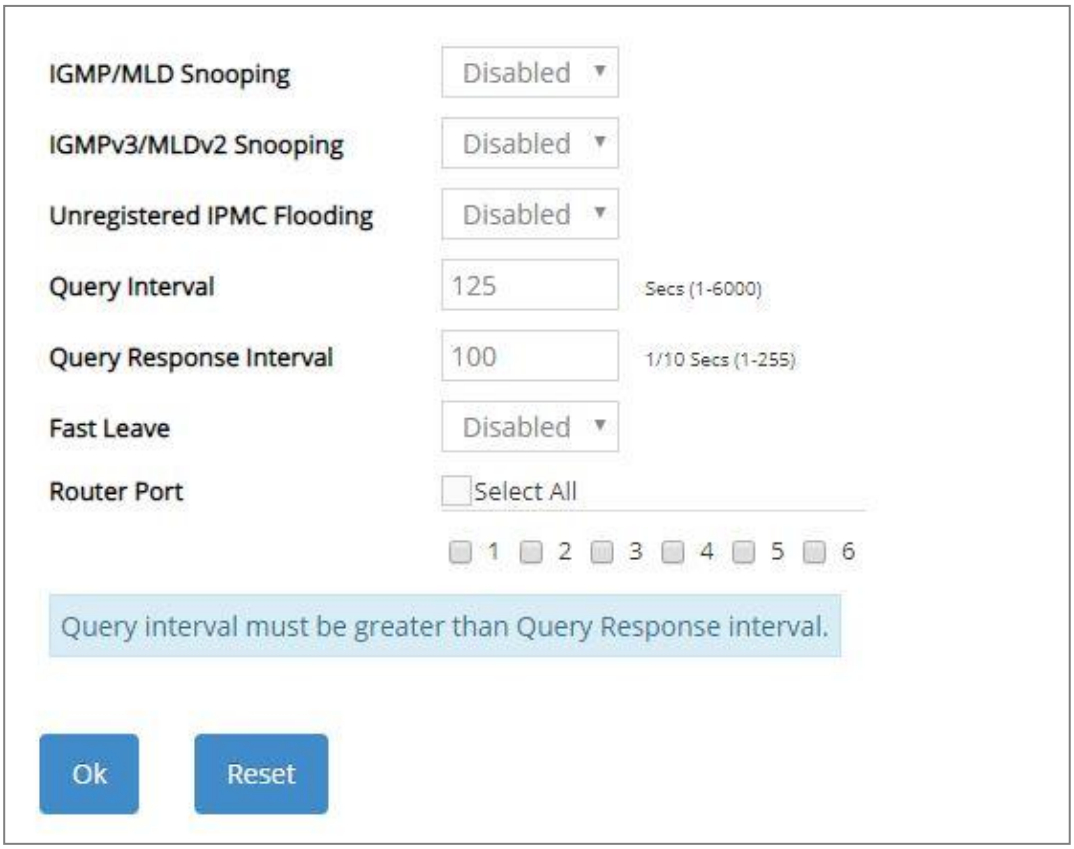
7. **IGMP Group Table:** View the IGMP Groups table.

8. **MLD Snooping Status:** View the MLD snooping status.

9. **MLD Group Table:** View the MLD Groups table.

4.6.1.1 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)

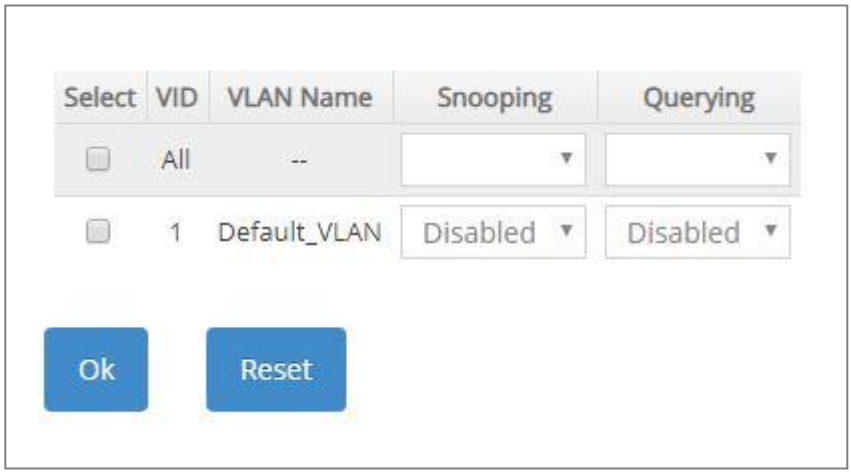
Query Response Interval: This determines the maximum amount of time allowed before sending an IGMP response report. (Default value is 100, One Unit=0.1 second)

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”.

Router Port: When ports are connected to the IGMP administrative routers, they should be checked. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

4.6.1.2 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.

VID: VID of the specific VLAN.

VLAN Name: View-only field that shows the VLAN name.

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.

4.6.1.3 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.

4.6.1.4 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.

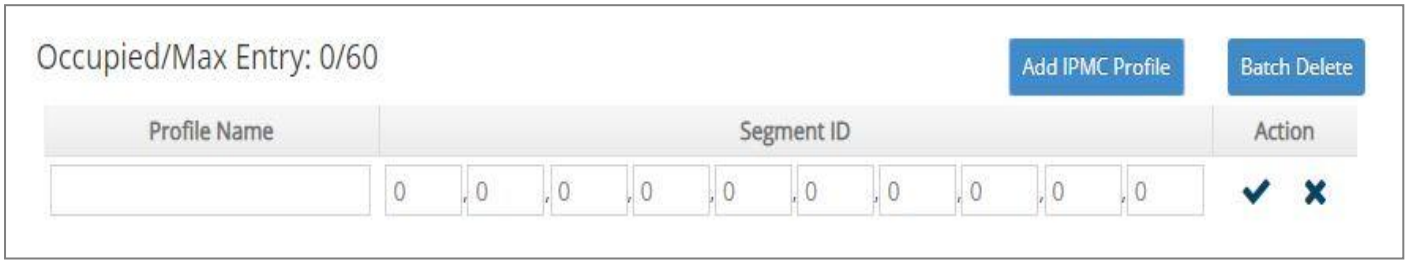
This table will display the overview of each configured IPMC profile. Up to 60 IPMC profiles can be registered.

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.

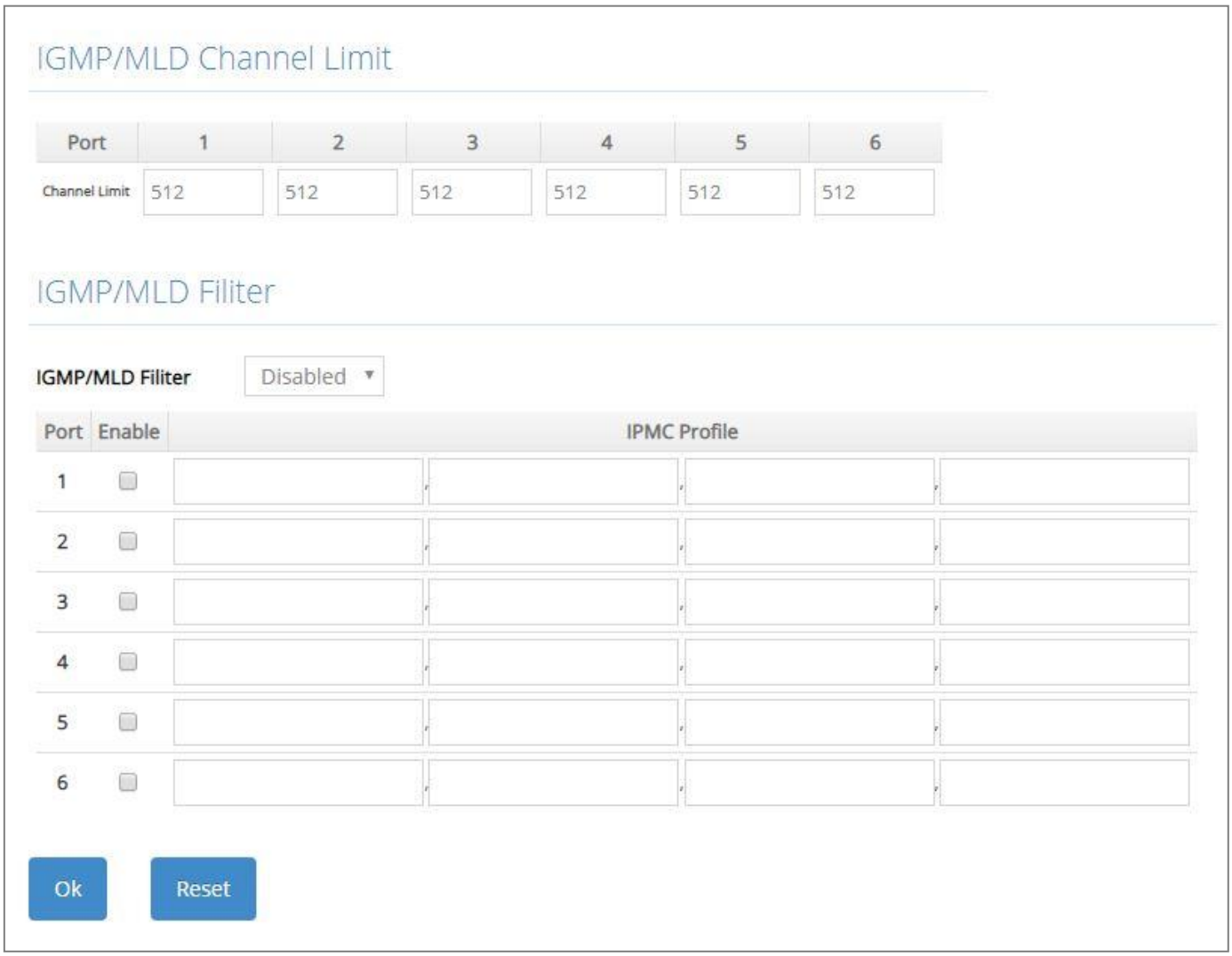
Click ✔ when the settings are completed, this new IPMC profile will be listed on the IPMC profile table, or click ✖ to cancel the settings.

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.

4.6.1.5 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.

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.)

4.6.1.6 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.

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).

4.6.1.7 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.

Refresh: Click **Refresh** to update the latest IGMP group table.

VLAN ID: VID of the specific VLAN.

Group: The multicast IP address of IGMP querier.

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

4.6.1.8 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.

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).

4.6.1.9 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.

Group: The multicast IP address of MLD querier.

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

4.6.2 Static Multicast Configuration

Select the option **Static Multicast Setup** from the **Multicast** menu and then the following screen page appears.

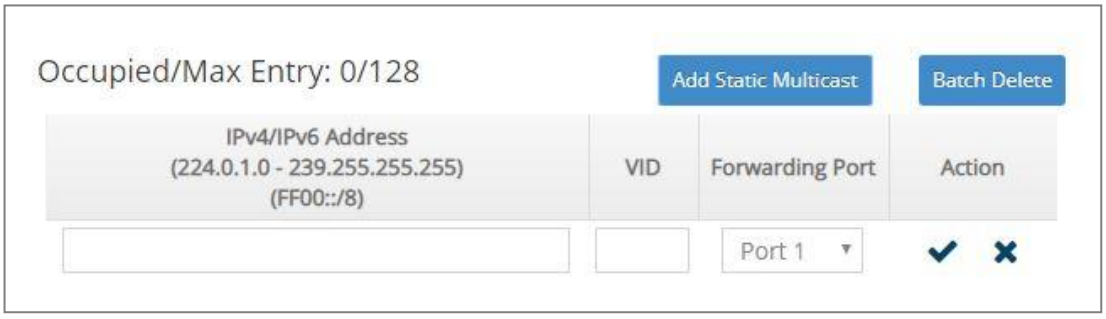
This table will display the overview of each configured static multicast entry. Up to 128 static multicast entries can be created.

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.

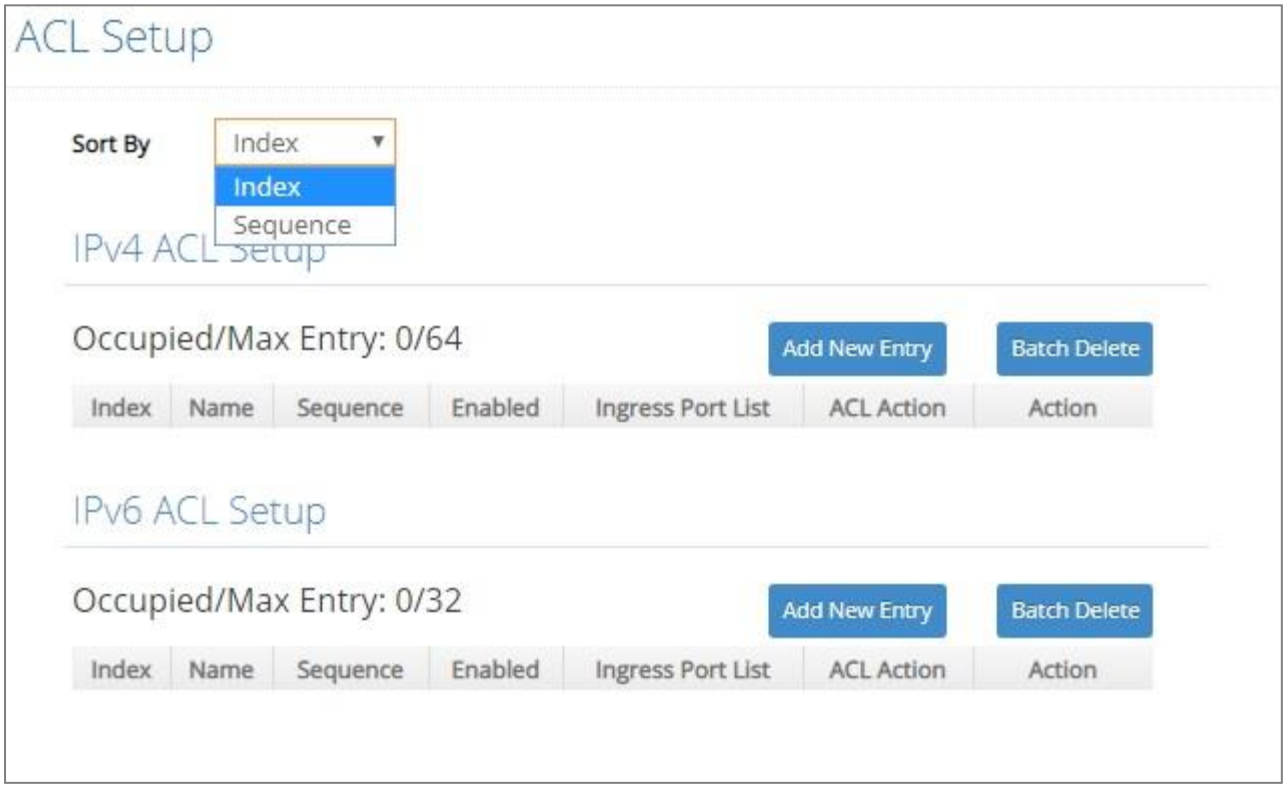
Click the icon to modify the settings of a specified static multicast entry.

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.

4.7 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.

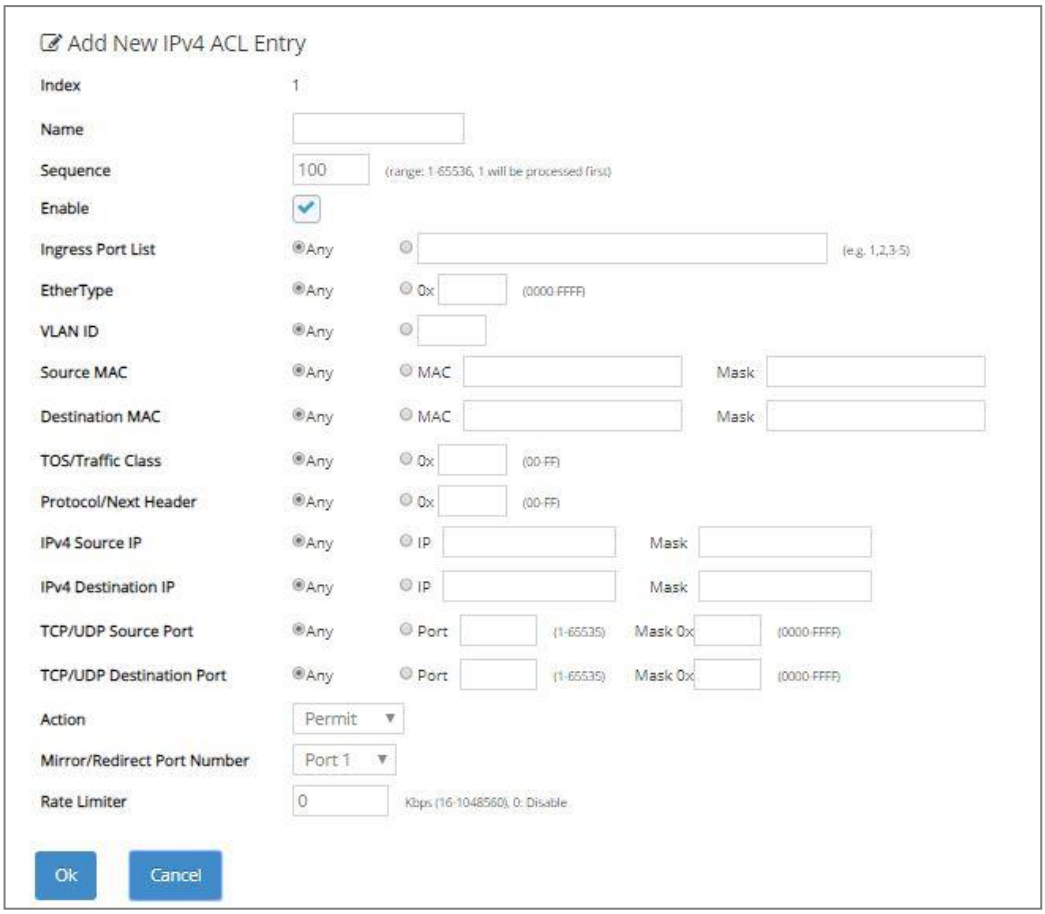


The IPv4 or IPv6 ACL tables will display the overview of each configured IPv4 or IPv6 ACL entry respectively. Up to 64 IPv4 ACL entries and 32 IPv6 ACL entries can be created.

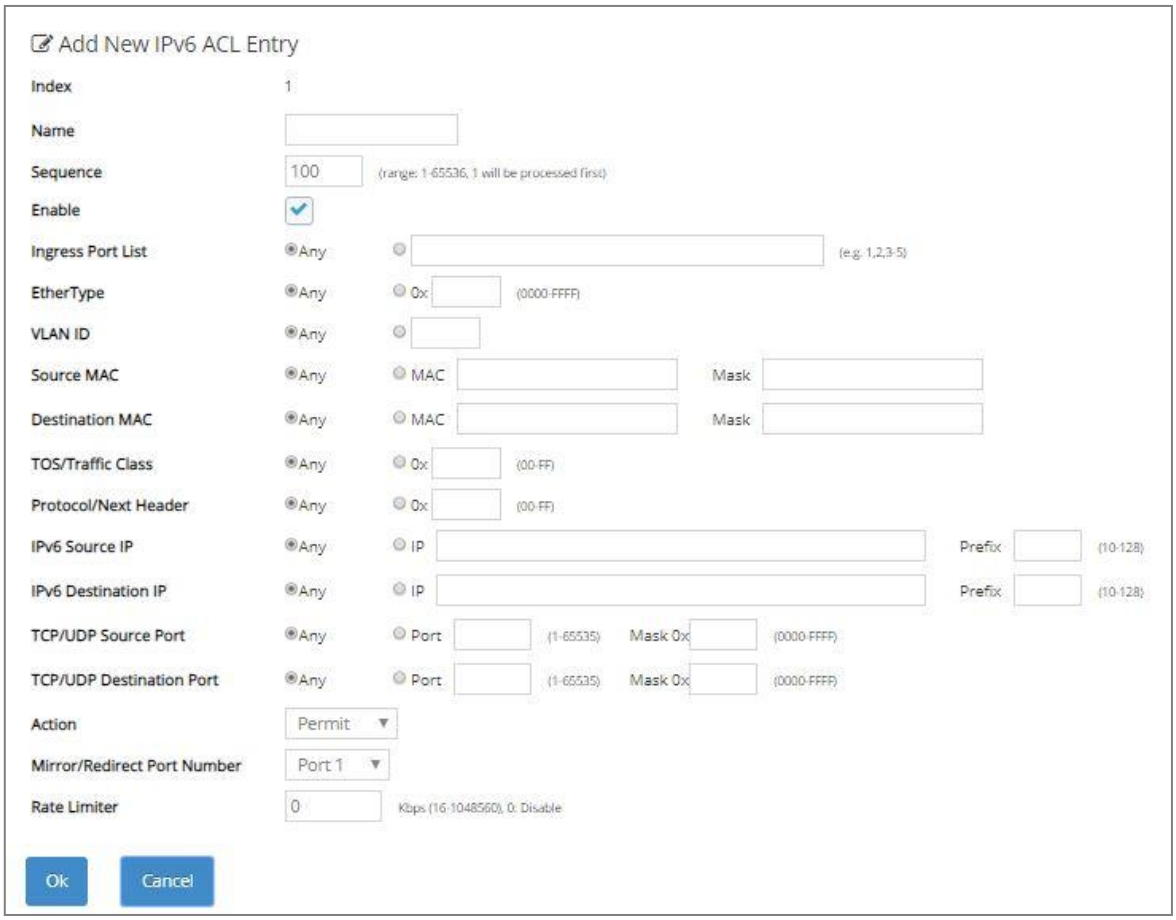
Occupied/Max Entry: View-only field.

> **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.

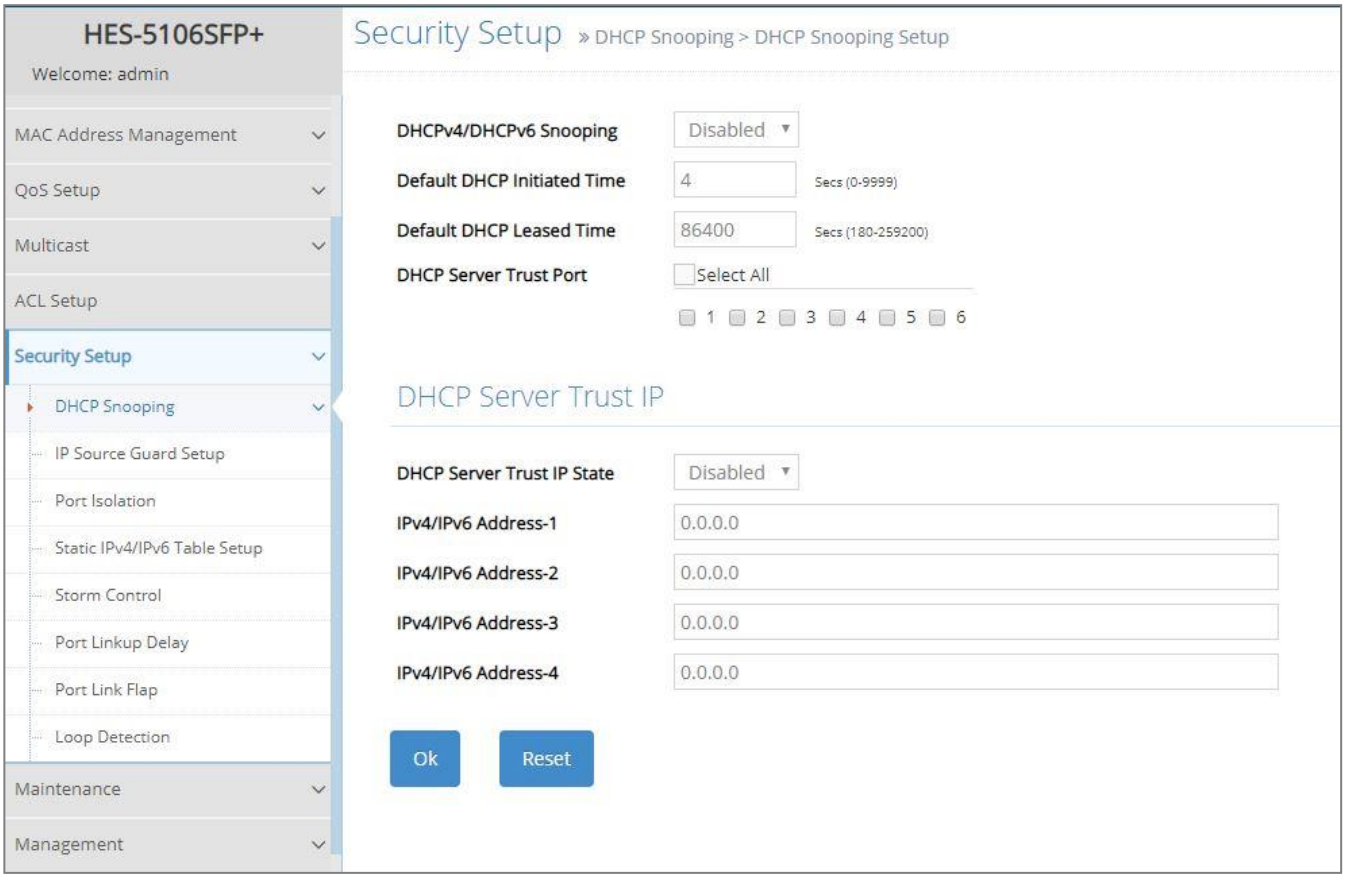
Click the  icon to modify the settings of a specified ACL entry.

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.

4.8 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. **Port Linkup Delay:** Set up the delay time for activating the delay port(s).

7. **Port Link Flap:** Set up the maximum times of a port's port link flap (linkdown or linkup) for sending the alarm message out via SNMP trap and syslog.

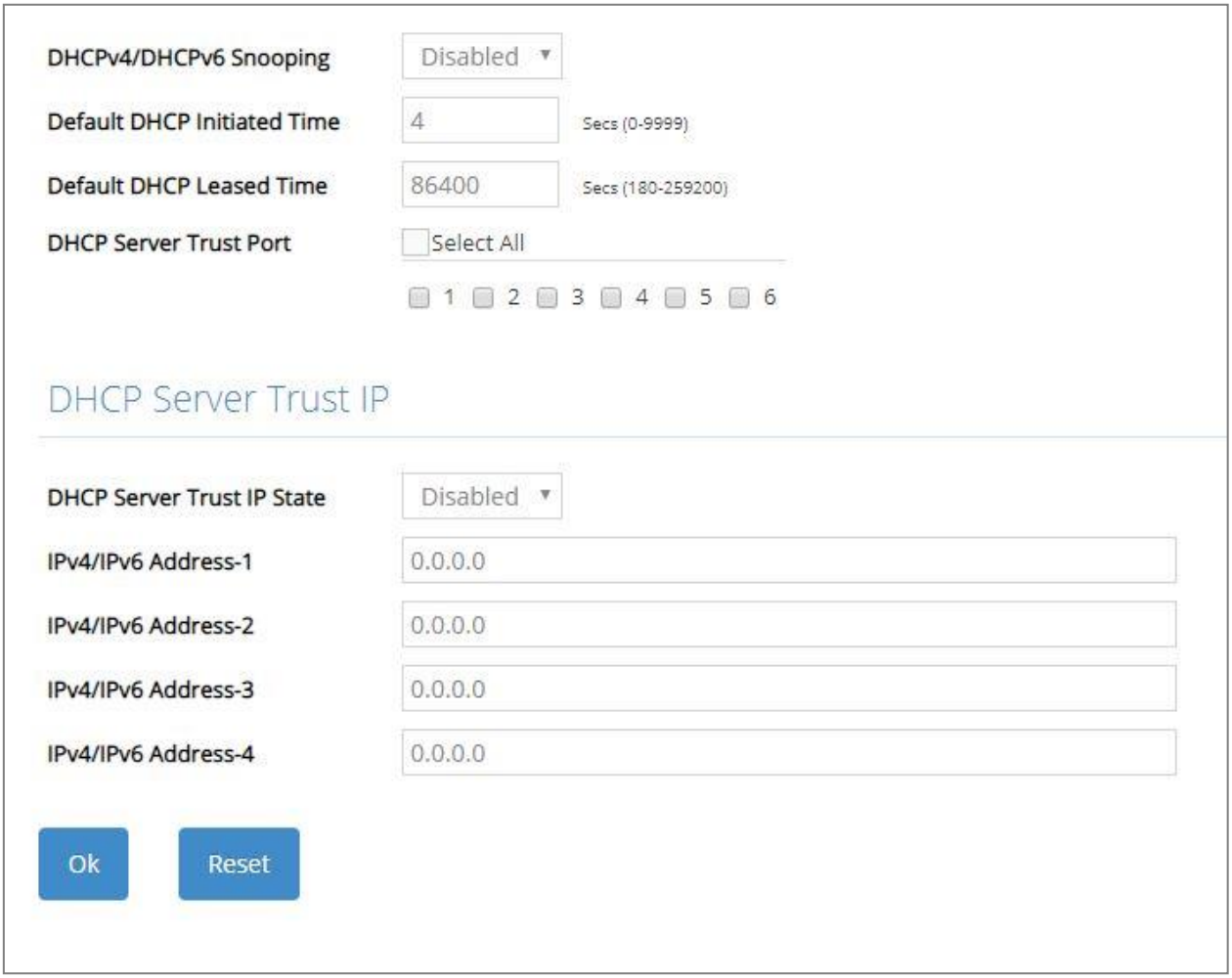
8. **Loop Detection:** Enable or disable Loop Detection function, set up Loop Detection configuration and view the Loop Detection status of each port.

4.8.1 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.

4.8.1.1 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 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. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

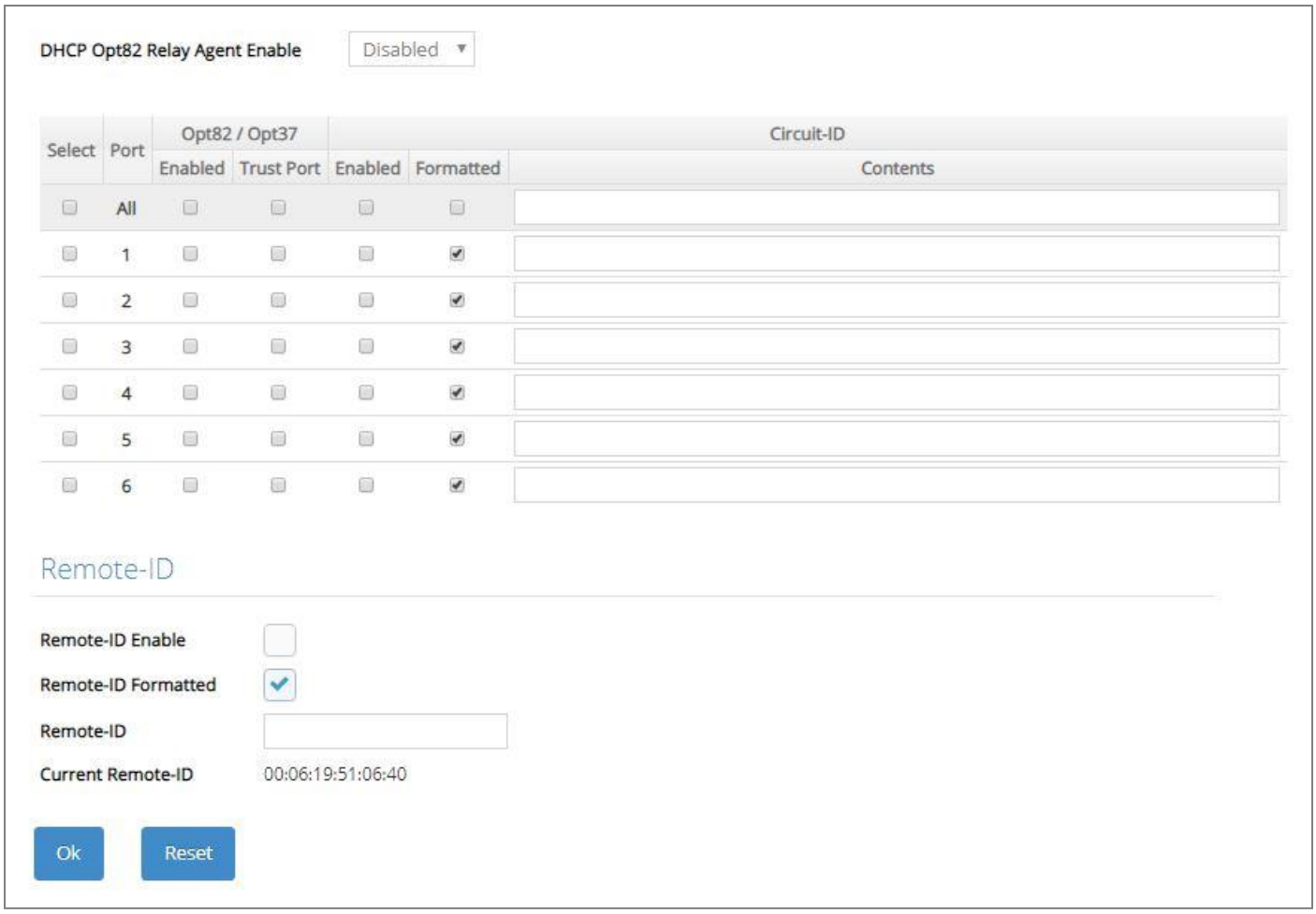
DHCP Server Trust IP State: After enabling Trust Port, you may additionally specify Trust IP address for identification of DHCP server. Click the drop-down menu and select "Enabled", then specify Trust IP address.

4.8.1.2 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 you can also configure the desired ports at a time by checking these ports, the new settings configured in the row of **All** port will be applied to these specified ports.

Port: The number of each port.

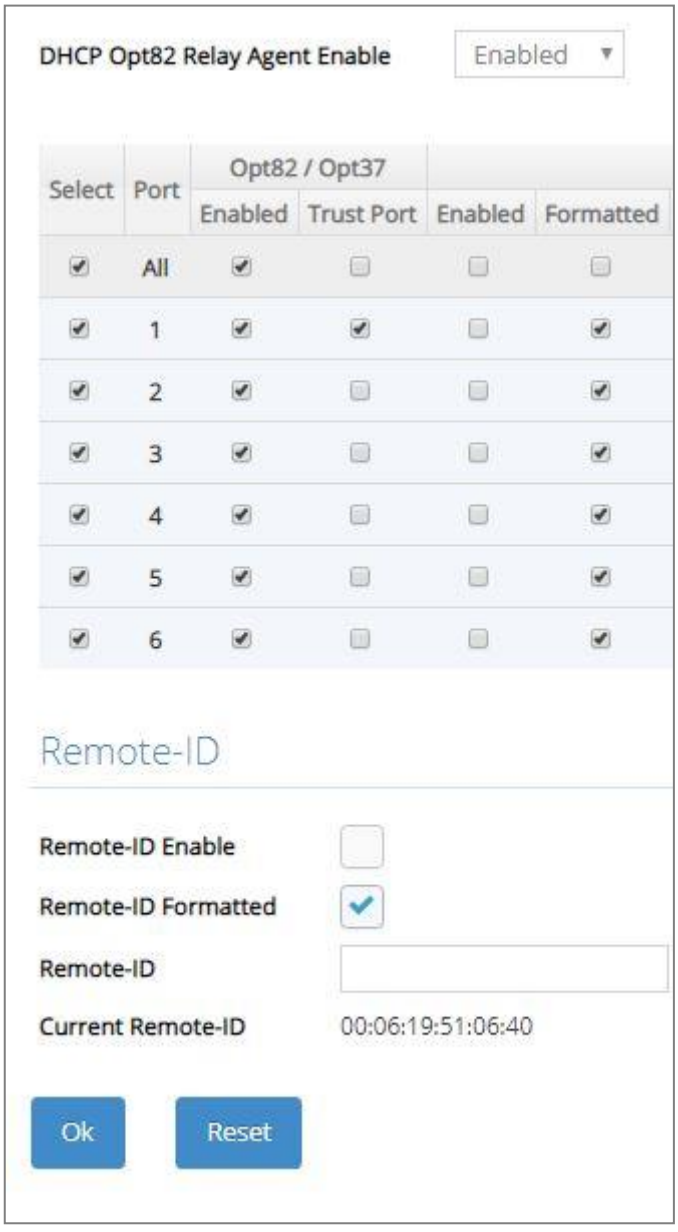
Enabled in Opt82/Opt37 field**:**

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.

4.8.1.3 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.

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.

4.8.2 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 you can also configure the desired ports at a time by checking these ports, the new settings configured in the row of **All** port will be applied to these specified 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).

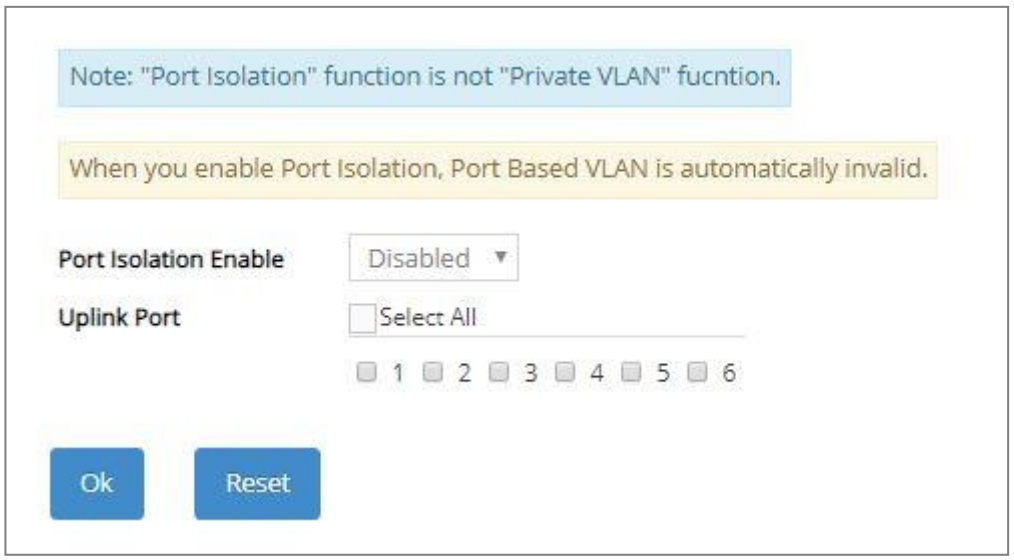
DHCP: DHCP-assigned IP address only.

Fix-IP: Only static IP (You must create Static IP table first. Refer to **Static IPv4/IPv6 Table Setup** for further information.).

4.8.3 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. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

4.8.4 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 1~6)

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.

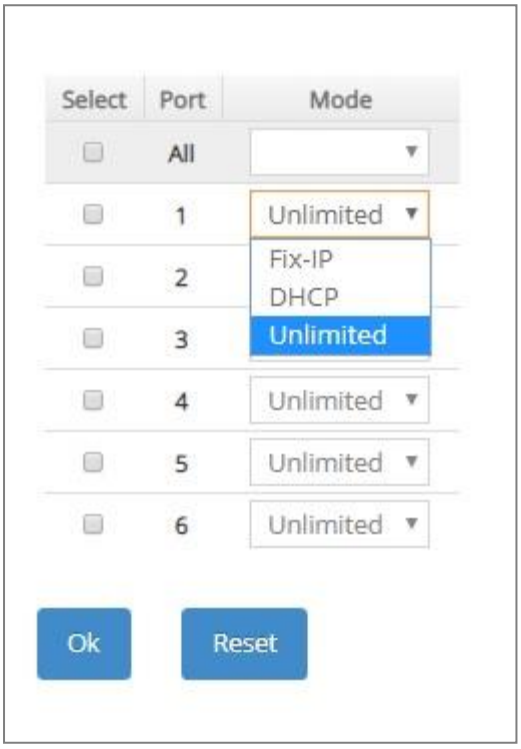
Click the icon to modify the settings of a specified static IP address.

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.

4.8.4.1 Configure DHCP Snooping

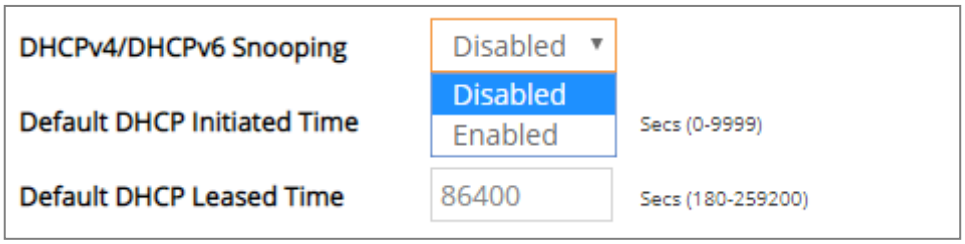
When you would like to use DHCP Snooping function, follow the steps described below to enable a client to receive an IP from DHCP server.

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

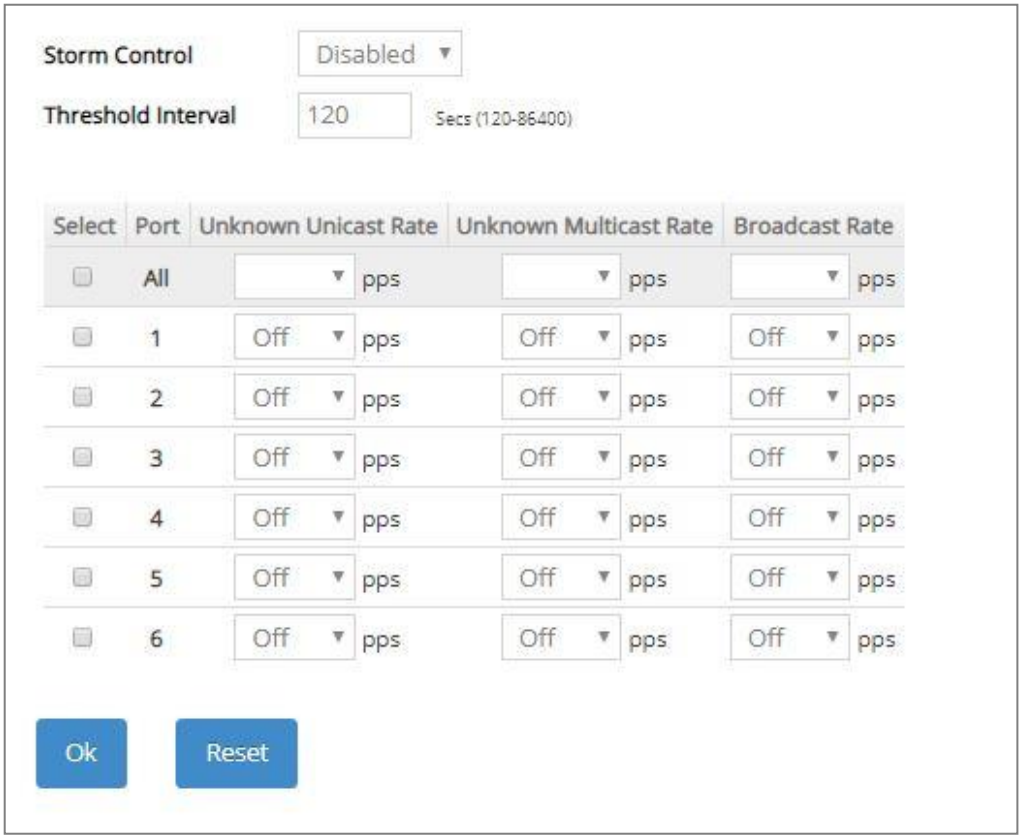
After you complete Step 1 & 2, connect your clients to the Managed Switch. Your clients will send a DHCP Request out to DHCP Server soon after they receive a DHCP offer. When DCHP Server responds with a DHCP ACK message that contains lease duration and other configuration information, the IP configuration 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.

4.8.5 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 you can also configure the desired ports at a time by checking these ports, the new settings configured in the row of **All** port will be applied to these specified 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.

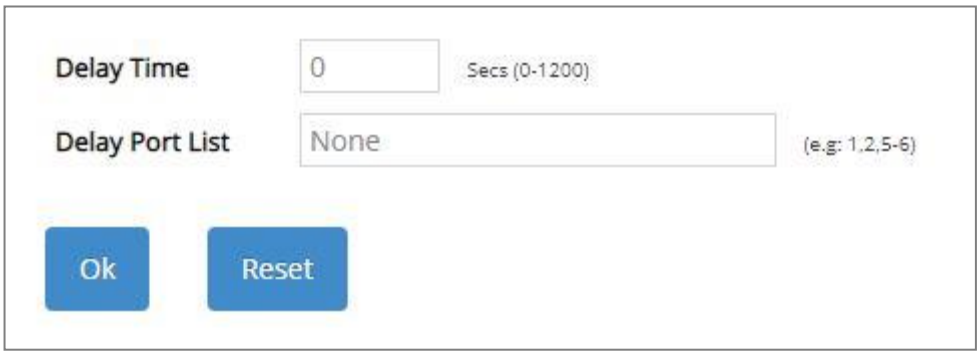
Unknown Multicast Rate: Enable or disable Unknown Multicast traffic control and set up Unknown Multicast Rate packet per second (pps) for each port. 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k can be chosen from the pull-down menu of each port.

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.

4.8.6 Port Linkup Delay

Port Linkup Delay is to set up a period of time for postponing the specific port(s) to be active in the stage of the system initialization. As for the remaining ports of the switch, they will be normally activated and be able to learn the MAC address first.

Select the option **Port Linkup Delay** from the **Security Configuration** menu to set up delay time, dealy port list and release delay rule, and then the following screen page appears.



Delay Time: Specify the desired time the designated delay port(s) will delay to be activated. Valid range: 0~1200 seconds. Default setting is “0”. “0” indicates “Disabled”.

Delay Port List: Specify the port(s) that will not be activated until the configured delay time ends.

4.8.6.1 Configure Port Linkup Delay by Following Delay Time

The system will delay to activate the port(s) specified in the **Delay Port List** parameter by following the delay time you configure.

For example,

In case that **Delay Time** is configured as 15 seconds and **Delay Port List** is configured as port number 1-4 (see the figure below), then, the system will only activate Port 5 as well as Port 6 first, and wait for 15 seconds to activate Ports 1-4 in the next device’s boot-up (initialization) stage.

4.8.7 Port Link Flap

Port Link Flap will notify the user the link-down and link-up alarm message of any port via SNMP trap and syslog when its port link flap times exceed the threshold. A port links down or links up, which will be considered as one time of this port's port link flap. Through this function, it will greately help technicians in the network operations center (NOC) exactly know the last time when the port linked down and linked up, and easily find out the major causes of the network unstability.

Select the option **Port Link Flap** from the **Security Configuration** menu to set up Port Link Flap parameters and then the following screen page appears.

Link Flap Threshold: To configure the maximum time of each port's port link flap for sending the alarm trap and the syslog message. For example, if the threshold is configured as "3", it means that the Managed Switch will send the alarm trap and the syslog message out to the specified SNMP server and log server respectively when one port links down or links up 3 times. Valid range: 1~20 times. Default is 6 times.

4.8.8 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:

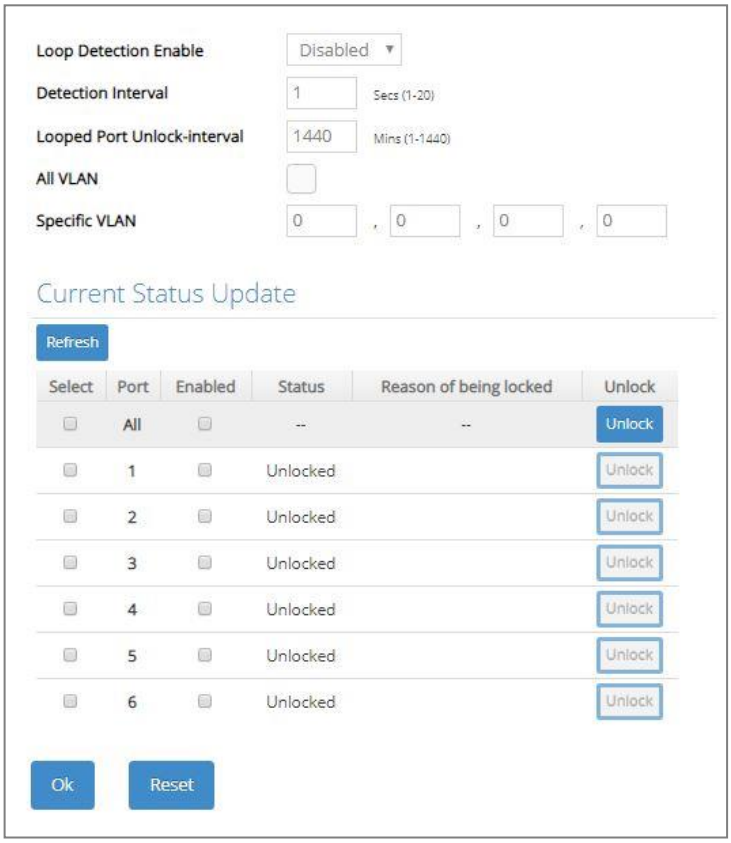
4. It blocks the relevant port to prevent broadcast storms, and send out SNMP trap to inform the network administrator. In other words, the system stops forwarding all the traffic via the looped port. However, the system will process the Loop Detection packets received on the looped port.
5. It slowly blinks the LED of looped port in orange (Ports 1~4) or in blue (Ports 5~6).
6. 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:

4. It un-blocks the relevant port. In other words, the system normally forwards all the traffic via the relevant port.
5. It stops slowly blinking the LED of looped port in orange (Ports 1~4) or in blue (Ports 5~6).
6. 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* (Ports 1~4) or in blue (Ports 5~6) *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 4.3.4.2)

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 you can also configure the desired ports at a time by checking these ports, the new settings configured in the row of **All** port will be applied to these specified 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.*

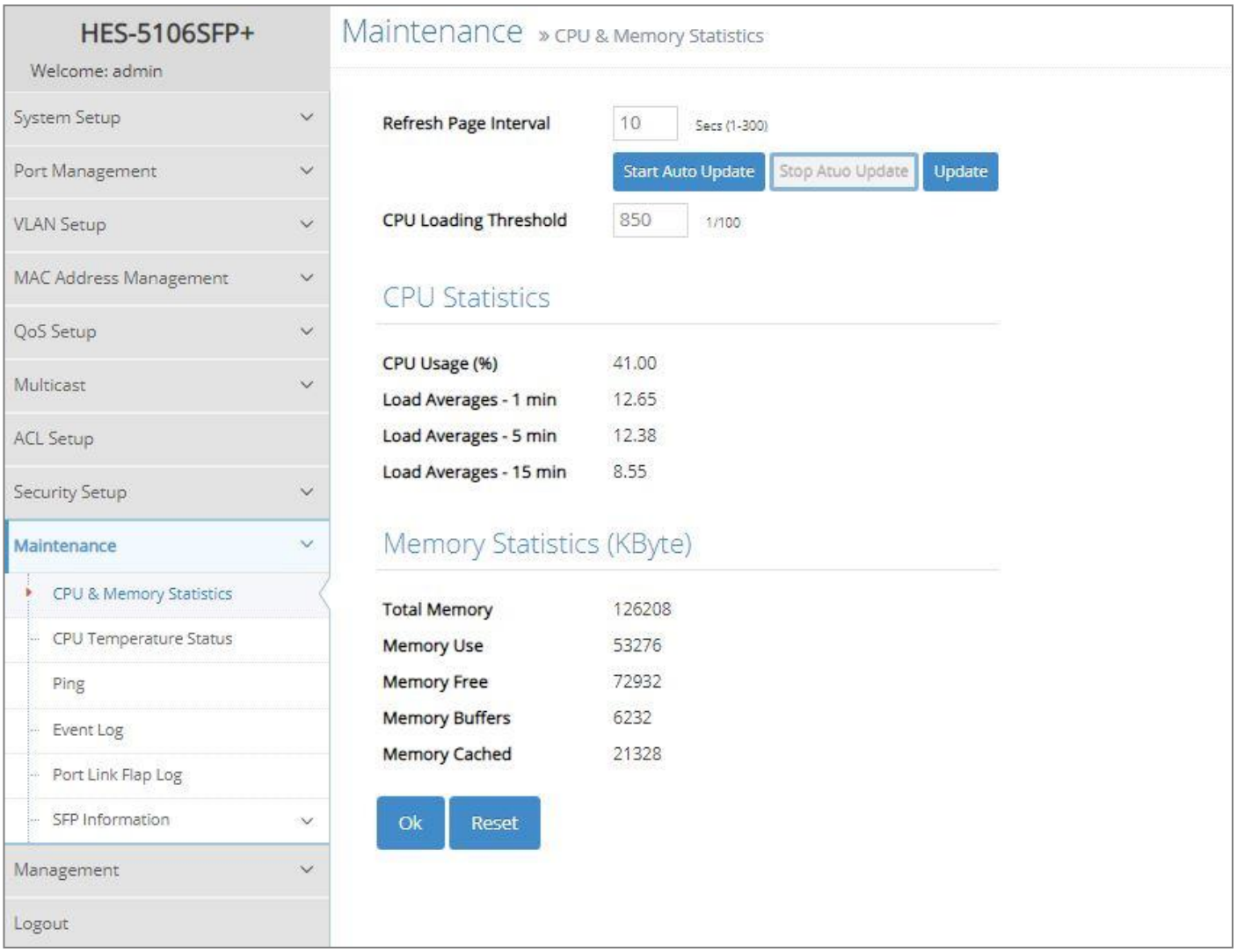
Status: View-only field that shows the loop status of each port.

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.

4.9 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 6 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. **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.

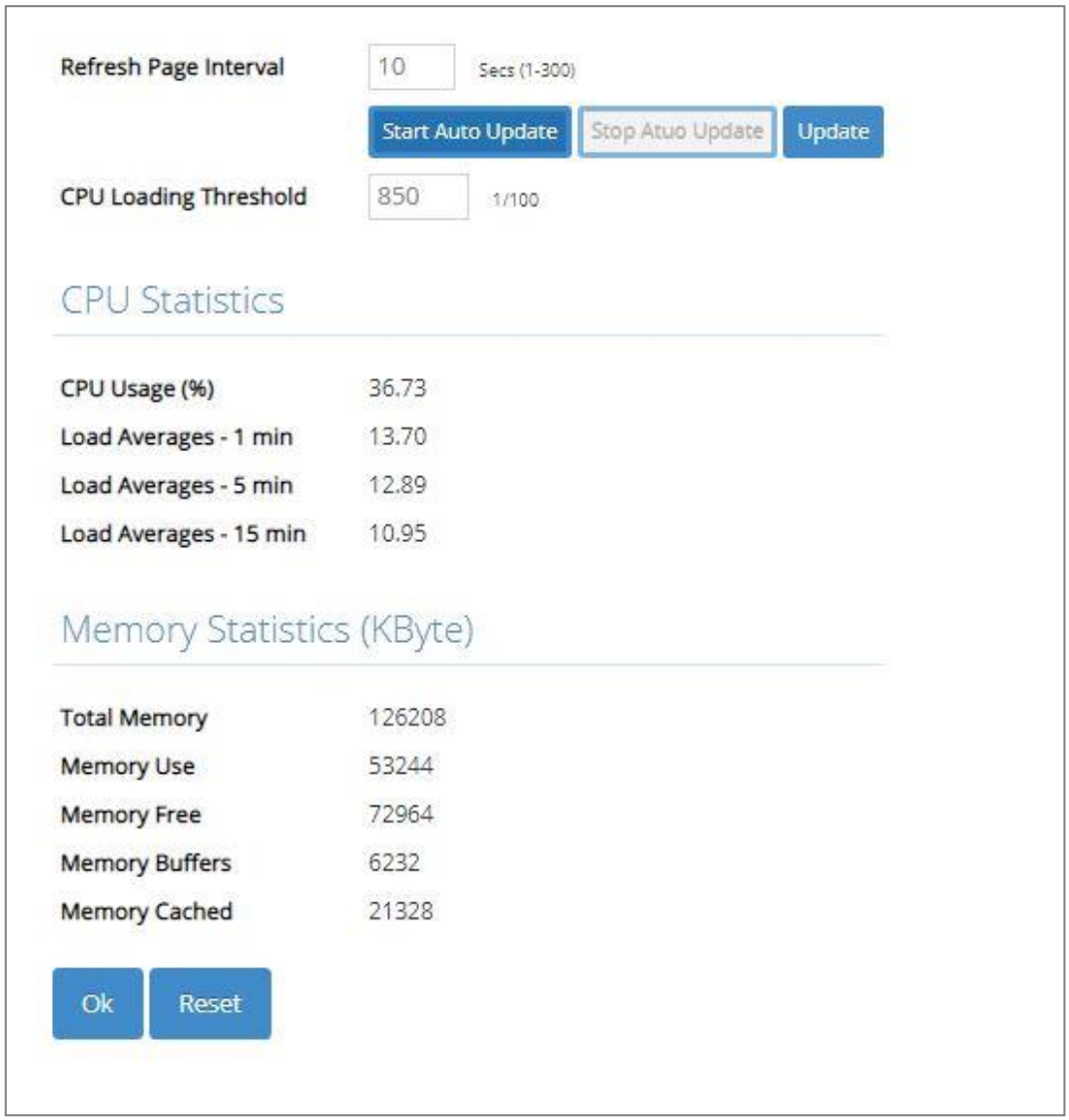
4. **Event Log:** Event log can keep a record of system's log events such as system warm start, cold start, link up/down, user login/logout, etc. They will be kept only when your CPU version is A06 with Boot ROM version A08 or later version. If your CPU or Boot ROM version is older than the one mentioned above, all events will lose when the system is shut down or rebooted.

5. **Port Link Flap Log:** Count and record each port's port link flap (a port's linkdown or linkup) history, causes, and so on.

6. **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..

4.9.1 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.

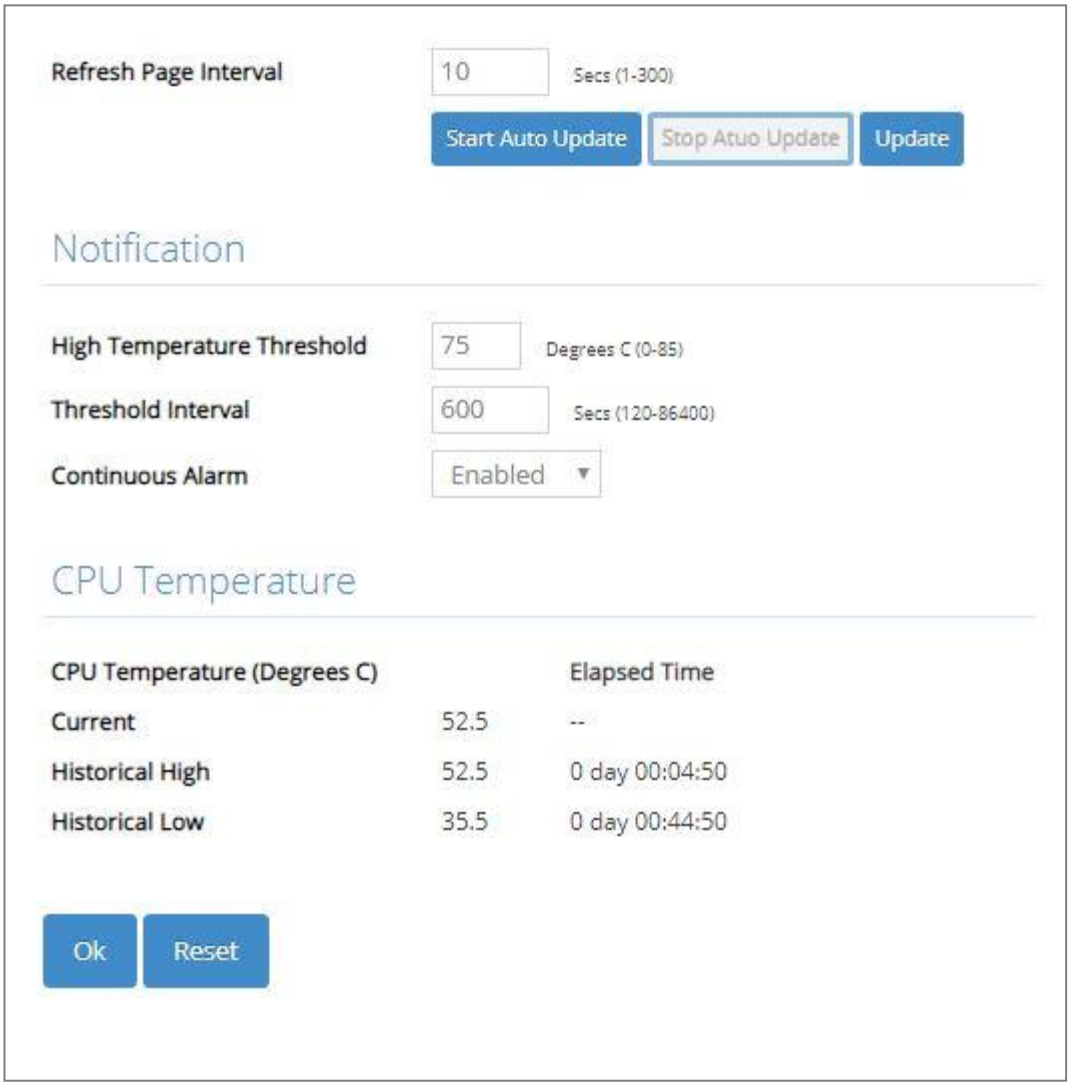
Memory Cached: The memory in kilobytes stored in a cache area that is where the data can be accessed faster in the future. The data can be retrieved more quickly from the cache than from its source origin.

4.9.2 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: 0~85 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.

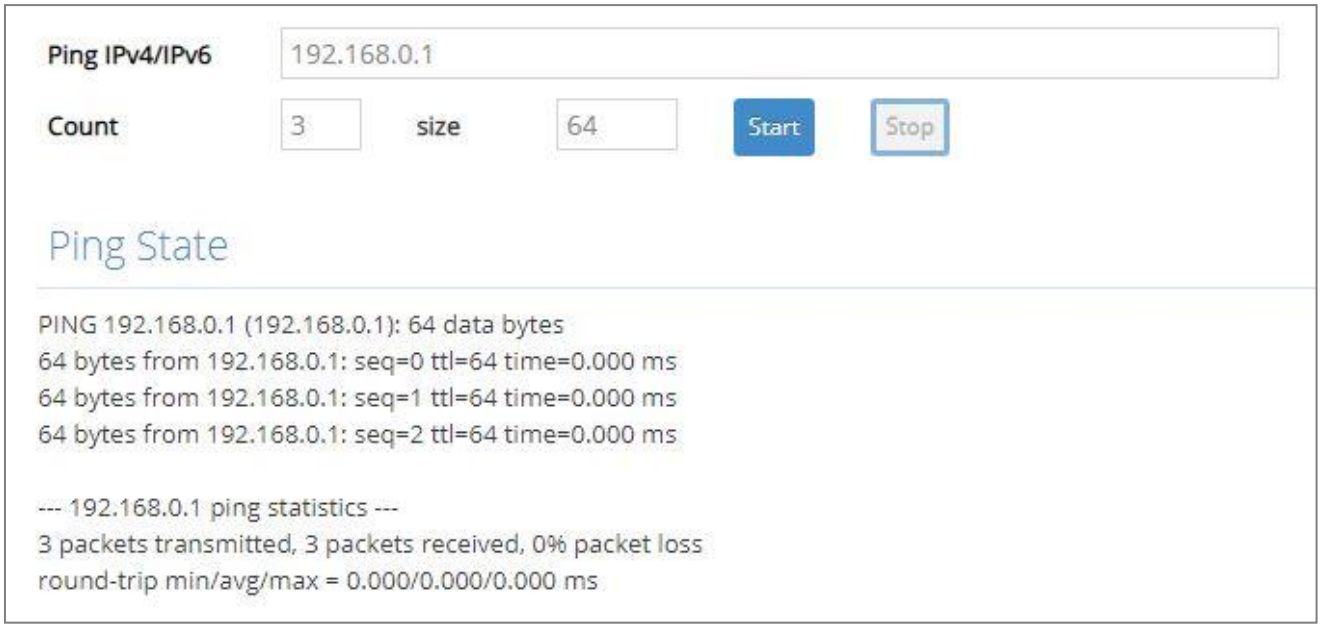
Historical Low: Display the lowest record of CPU temperature that had ever been reached since this system boot-up. It will show “Failed” in red color if the temperature sensor fails.

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.

4.9.3 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.

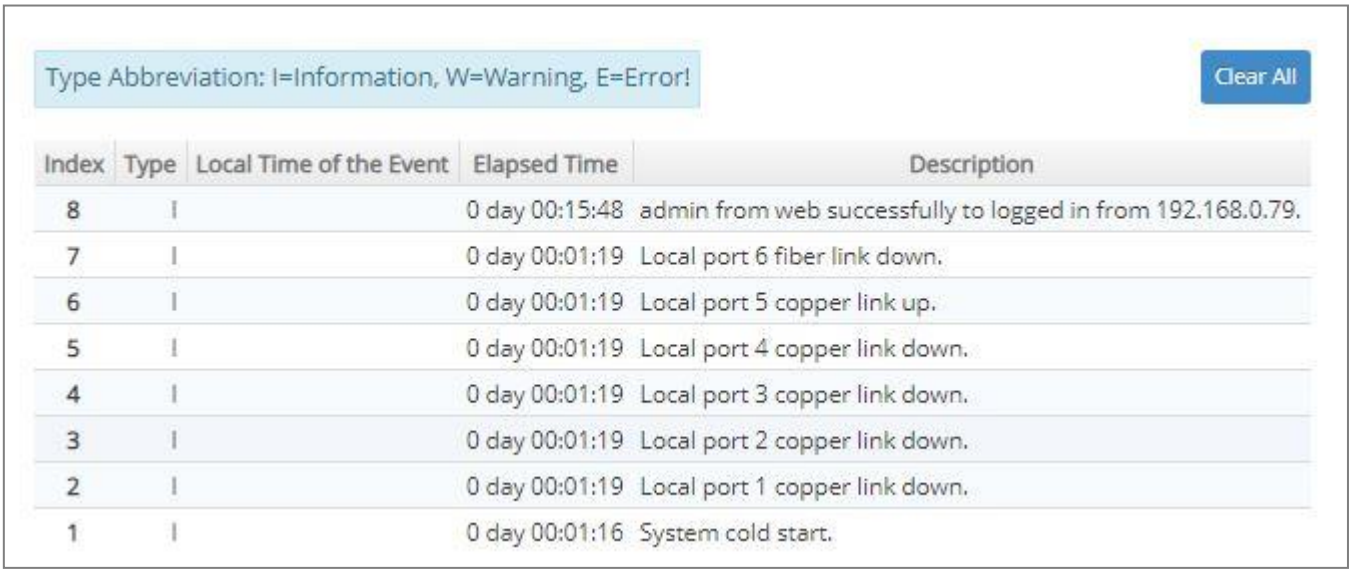


Enter the IPv4/IPv6 address of the host you would like to ping. You can also specify the count and size of the Ping packets. Click **Start** to start the Ping process or **Stop** to pause this Ping process.

4.9.4 Event Log

Event log keeps a record of switch-related information, such as user login, logout timestamp and so on. In the **Type** field, "**I**" is the abbreviation of "Information", "**W**" is the abbreviation of "Warning", and "**E**" is the abbreviation of "Error".

Select the option **Event Log** from the **Maintenance** menu and then the following screen page appears. All event logs will be cleared when the system reboot occurs.



Index	Type	Local Time of the Event	Elapsed Time	Description
8	I		0 day 00:15:48	admin from web successfully to logged in from 192.168.0.79.
7	I		0 day 00:01:19	Local port 6 fiber link down.
6	I		0 day 00:01:19	Local port 5 copper link up.
5	I		0 day 00:01:19	Local port 4 copper link down.
4	I		0 day 00:01:19	Local port 3 copper link down.
3	I		0 day 00:01:19	Local port 2 copper link down.
2	I		0 day 00:01:19	Local port 1 copper link down.
1	I		0 day 00:01:16	System cold start.

Click **Clear All** to clear the record of all event logs.

4.9.5 Port Link Flap Log

Port Link Flap Log shows each port's log history of trigger events such as the port link flap (a port's linkdown or linkup), the count of port's port link flap, the reason that causes these triggered events, the time duration that the port link flap lasts, Rx power(dBm) of SFP ports, and so on.

In the Port Link Flap Log table, up to 100 entries can be accommodated for each port. Like the event log, the oldest record will be overwritten by the newly-generated one when total records reach the limit. Select the option **Port Link Flap Log** from the **Maintenance** menu and then the following screen page appears.

To view the latest log data of the port link flap, just pull down the menu of **Port Number** and choose the preferred port. The logs belonging to the designated port will be listed. All logs will be cleared as well when the system reset occurs.

Refresh: Click **Refresh** to update the latest Port Link Flap Log table.

Clear: Click **Clear** to remove all logs of the triggered event for the specified port.

Local Time: Display the local time of the system. To obtain the correct local time, please make sure that the device's NTP function is enabled. (For more details on NTP settings, refer to Section 4.1.4 "Time Server Setup".)

Total Port Flaps: Total times of the linkdown or linkup for the specific port.

Index: The number of the specific port's triggered events arranged in order of time.

NTP Time: Display the local time when the specific port's triggered event occurred.

Up Time: Display the up time since the specific port's triggered event has been occurred.

Port Status: This shows each port's link state, which can be Link up, Link down, or "--".

Description: Display the reason why the specific port is triggered.

When Flapped: The period of time passed by since the specific port's port link flap has been taken place. This value is equal to the above parameters "**Local Time**" – "**NTP Time**" of the specific index or system's "**Up Time**" displayed on the **System Information** webpage – "**Up Time**" of the specific index. The value of this parameter will be updated over time.

Status Duration: The period of time that the specific port's port link flap lasts until a new one occurs. This value is equal to the above parameters "**Up Time**" of the next index – "**Up Time**" of the specific index. (e.g. Index 5's status duration = Index 6's "Up Time" – Index 5's "Up Time".)

As to the status duration of the newest link flap, it will be equal to system's "**Up Time**" displayed on the **System Information** webpage – "**Up Time**" of this newest link flap, which will be updated over time until the next port link flap occurs.

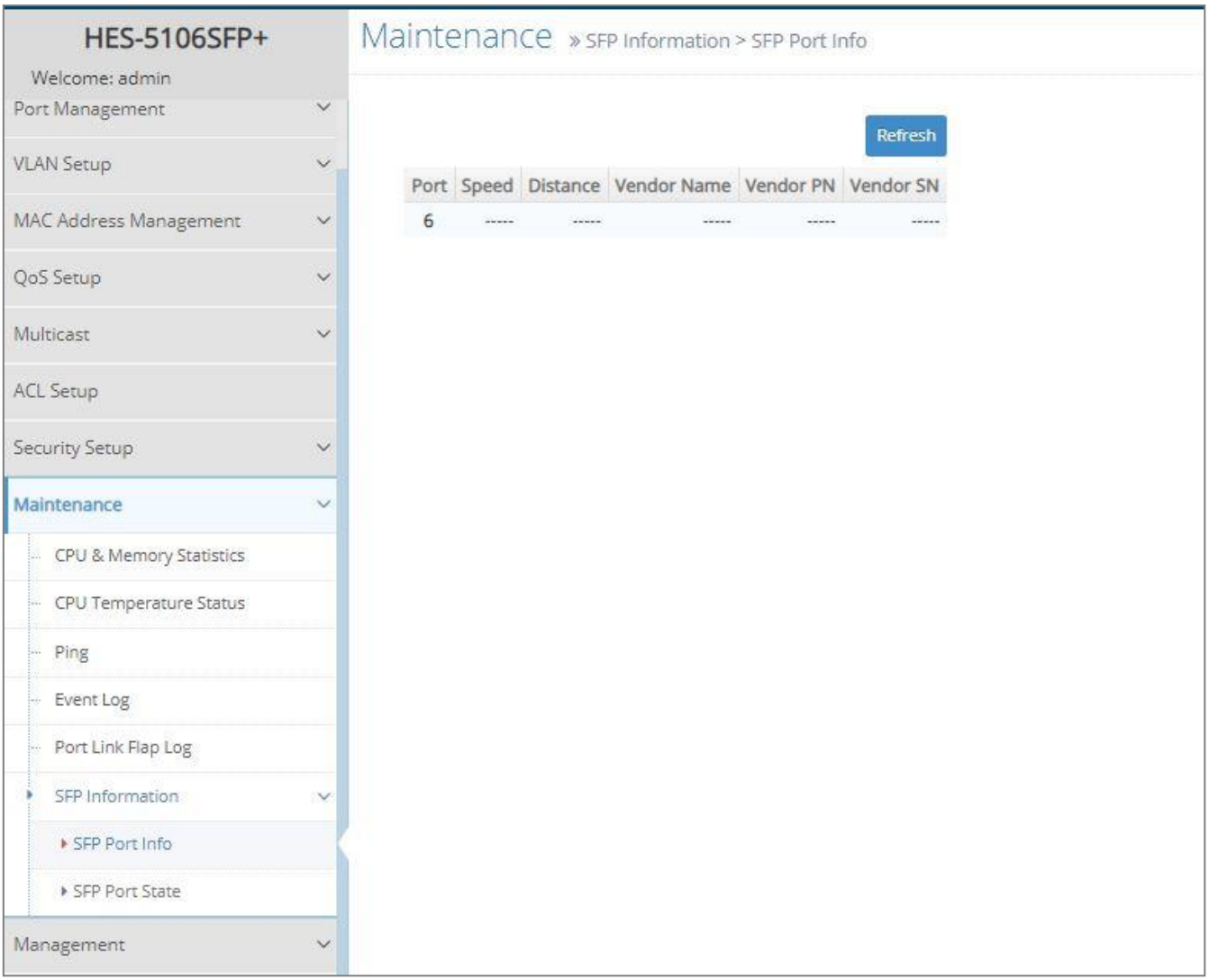
SFP RX Power(dBm): The value of RX power in unit of dBm. Only the fiber ports will display this value based on the following cases, other TP ports will display "--".

- In case of the fiber port status is from *link-down* to *link-up*, it will display the value of current Rx power after this fiber port link is up and its power signal is steady (it may take 5 seconds around). The RX power value obtained is a fixed one that will not be changed over time.

- In case of the fiber port status is from *link-up* to *link-down*, it will display the last value of power signal before this fiber port link is down. The RX power value obtained is a fixed one that will not be changed over time.

4.9.6 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.



4.9.6.1 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.

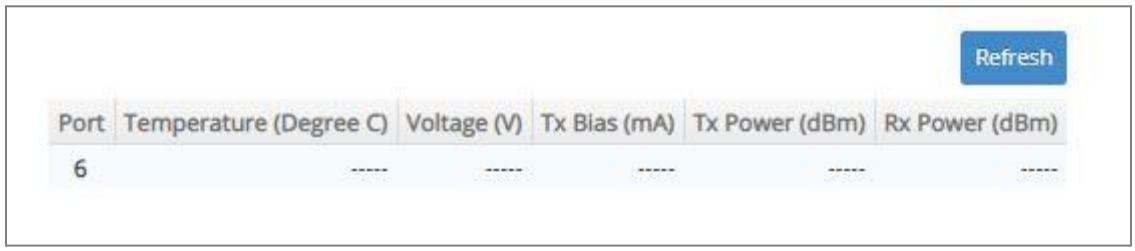
Vendor Name: Vendor name of the slide-in SFP/SFP+ Transceiver.

Vendor PN: Vendor PN of the slide-in SFP/SFP+ Transceiver.

Vendor SN: Vendor SN of the slide-in SFP/SFP+ Transceiver.

4.9.6.2 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.

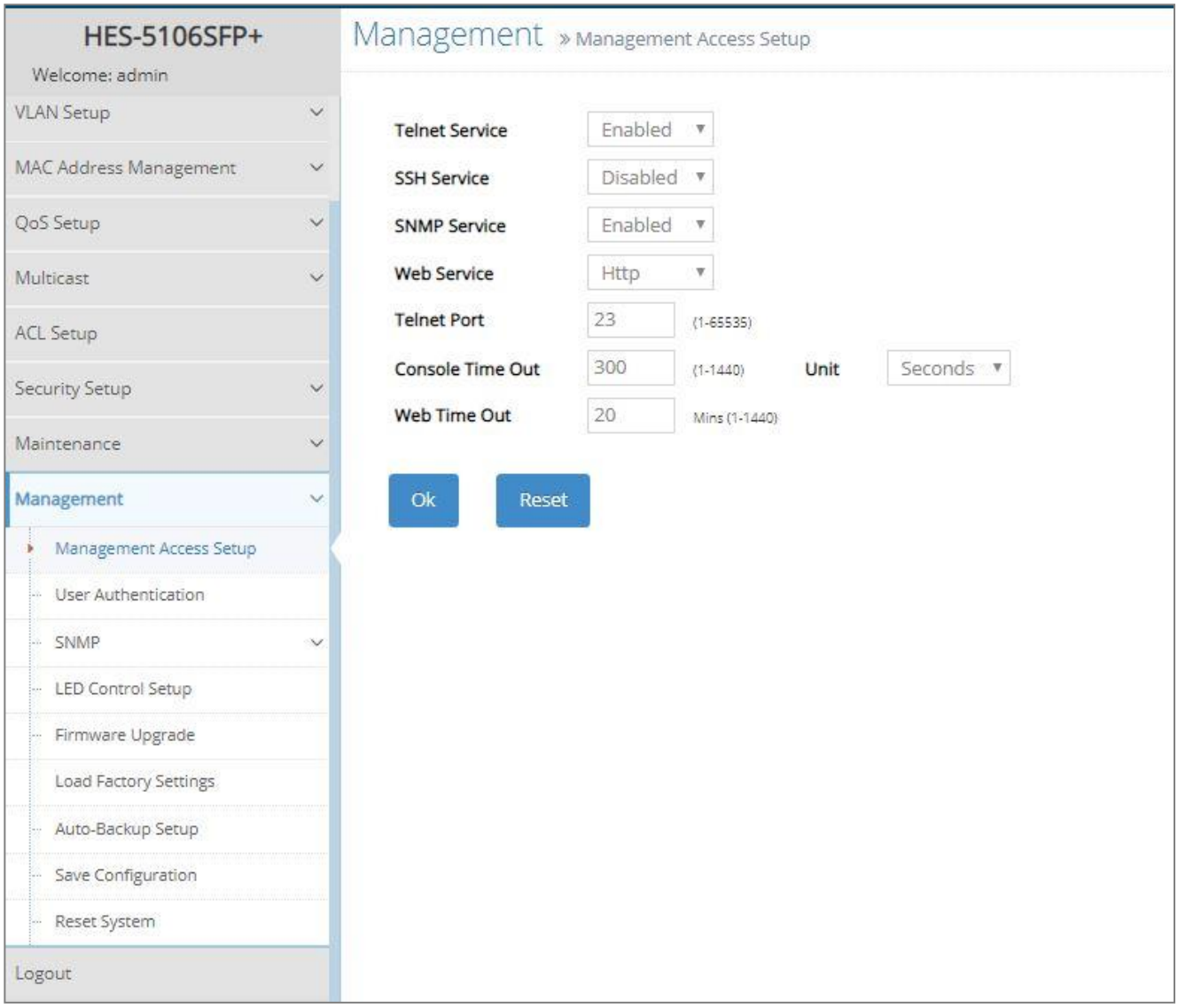
TX Bias (mA): The operation current of slide-in SFP/SFP+ module currently detected.

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.

4.10 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 9 options will be displayed for your selection.



1. **Management Access Setup:** Enable or disable the specified network services, and set up the specific Telnet and Console services.

2. **User Authentication:** View the registered user list, add a new user or remove an existing user.

3. **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.

4. **LED Control Setup:** Control the light intensity level of all LEDs.

5. **Firmware Upgrade:** This allows users to update the latest firmware, save current configuration or restore previous configuration to the Managed Switch.

6. **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.

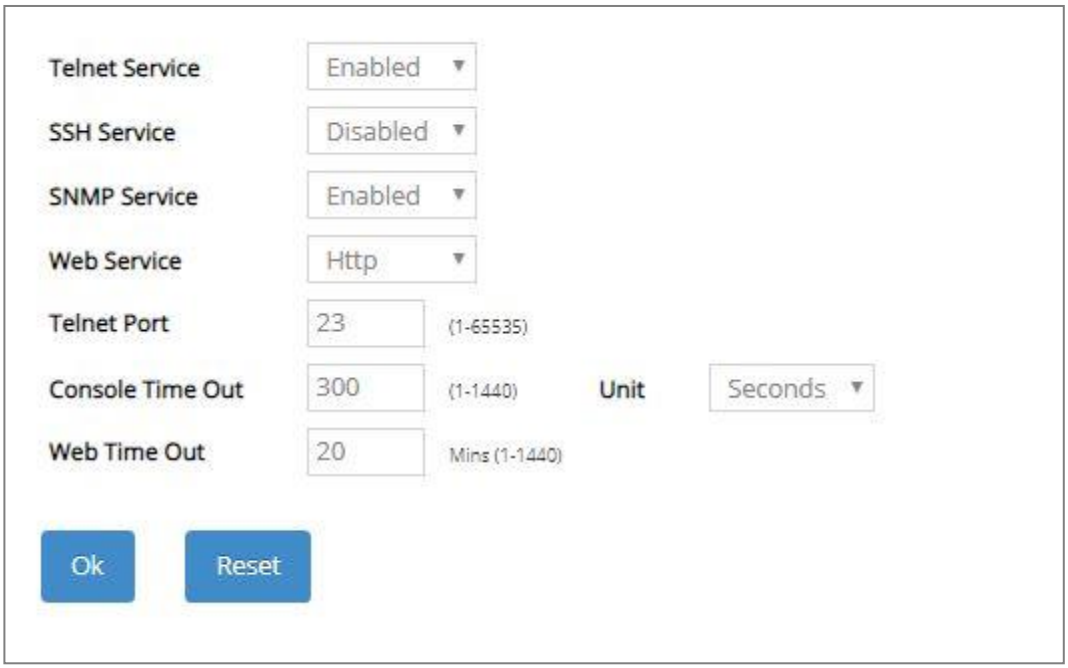
7. **Auto-Backup Setup:** Periodically execute the automatic backup of the start-up configuration files based on the given time you set up.

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

9. **Reset System:** Reset the Managed Switch.

4.10.1 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.

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.

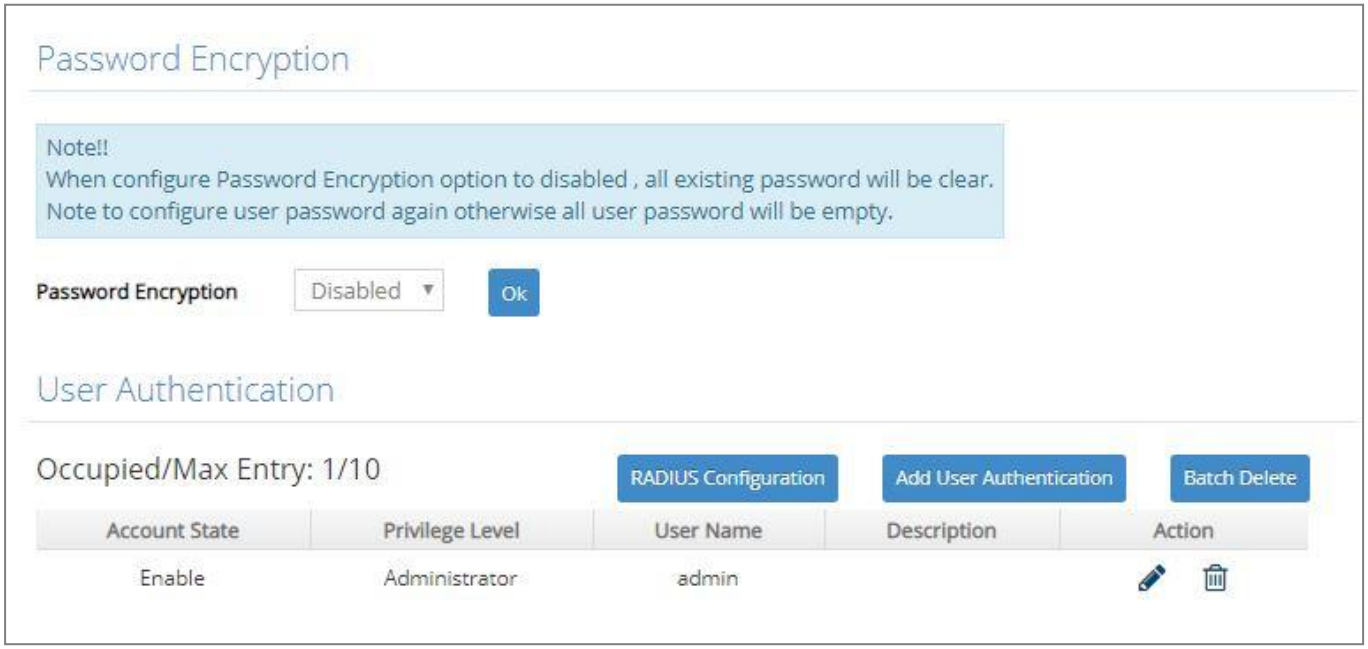
Unit: Specify the unit for the **Console Time Out** parameter.

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

4.10.2 User Authentication

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 Authentication** 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.

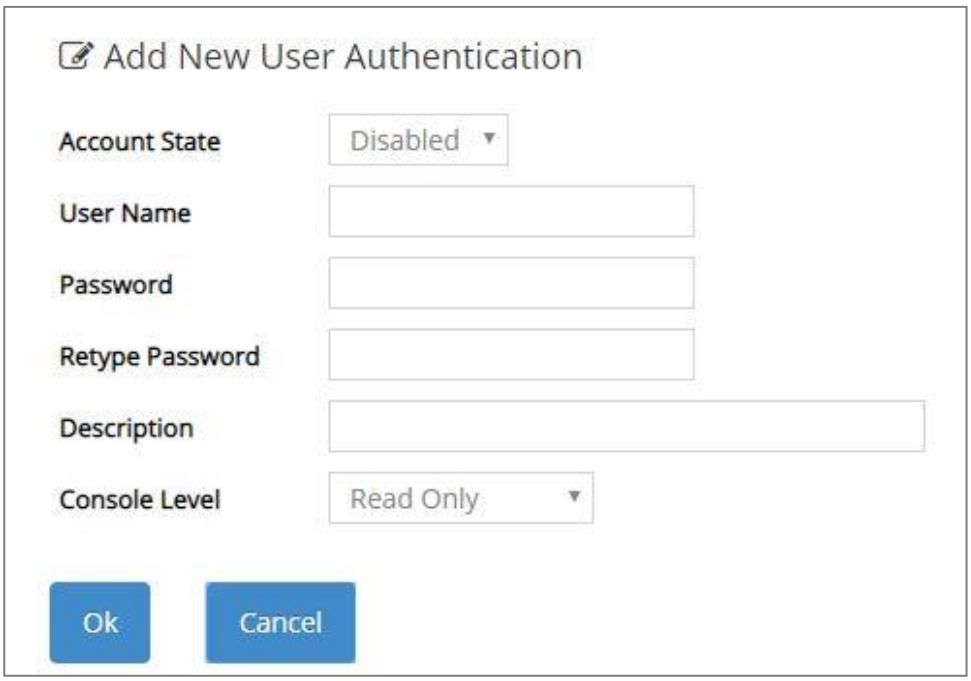
This user list will display the overview of each configured user account. Up to 10 users can be registered.

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 Authentication** to add a new user and then the following screen page appears for the further user registration settings.

Or click **RADIUS Configuration** for authentication setting via RADIUS. For more details on these settings, please refer to Section 4.10.2.1.



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.

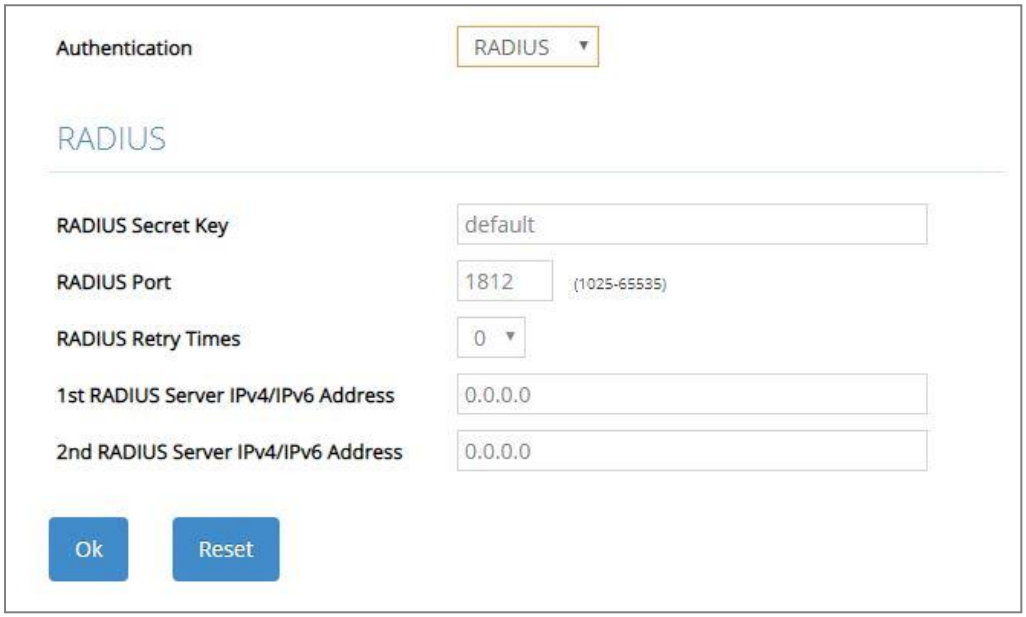
4.10.2.1 RADIUS Configuration

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

Authentication: From the **Authentication** pull-down menu, you can choose **RADIUS** option to respectively enable authentication via RADIUS. To disable the authentication, just select **Disabled** option from this menu.

When **RADIUS Authentication** is selected, the user login will be upon those settings on the RADIUS server(s).

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.*



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

RADIUS Port: The RADIUS service port on RADIUS server.

RADIUS Retry Times: Times of trying to reconnect if the RADISU server is not reachable.

1st RADIUS Server IPv4/IPv6 Address: IPv4/IPv6 address of the primary RADIUS server.

2nd RADIUS Server IPv4/IPv6 Address: IPv4/IPv6 address of the secondary RADIUS server.

4.10.3 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.

4.10.3.1 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.

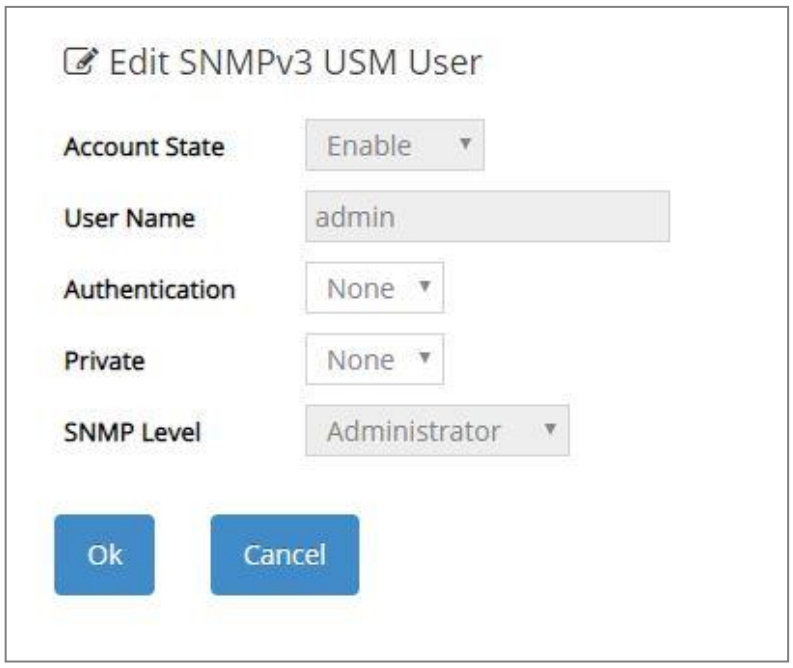
Note: *The SNMPv3 user account is generated from "User Authentication". (Refer to Section 4.10.2)*

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.

4.10.3.2 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.

4.10.3.3 Trap Destination

The following screen page appears if you choose **Trap Destination** function.

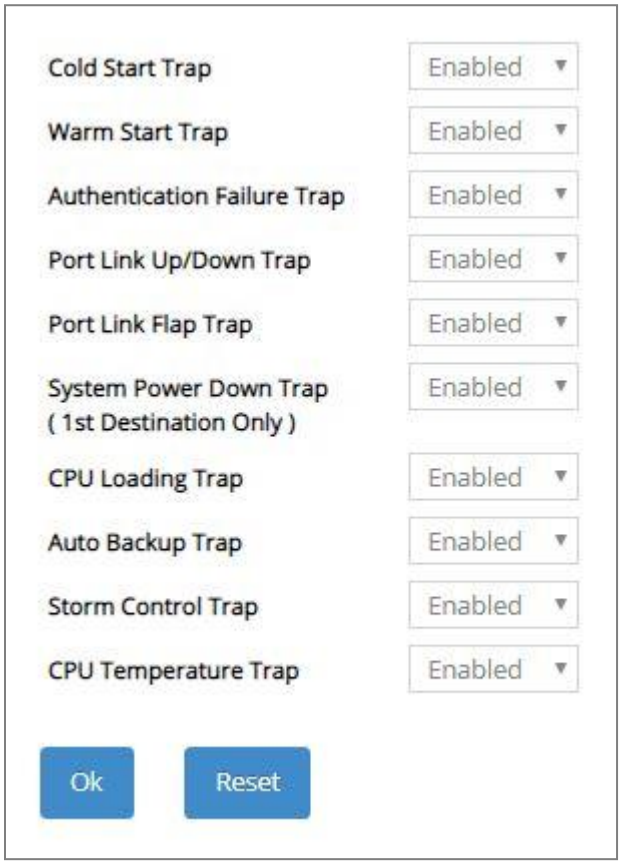
State: Enable or disable the function of sending trap to the specified destination.

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.

4.10.3.4 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.

Port Link Flap Trap: Enable or disable the Managed Switch to send a trap when a port's port link flap exceeds the threshold.

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.

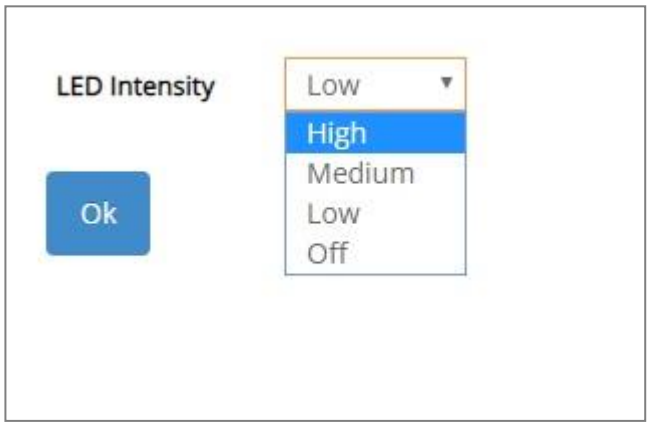
Auto Backup Trap: Enable or disable the Managed Switch to send a trap when the auto backup succeeds or fails.

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.

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 (0~85 degrees centigrade), or the temperature sensor fails to detect CPU temperature.

4.10.4 LED Control Setup

LED Control Setup allows the user to control the light intensity of all LEDs at will on the Managed Switch in order to decrease the possibility of the light pollution damage. Select the option **LED Control Setup** from the **Management** menu and then the following screen page shows up.



LED Intensity: Assign the intensity of the light for all LEDs. The LED behavior of each option from the pull-down list is described below.

High: It indicates LEDs of Ports 1~6, Status LED and Power LED on the Managed Switch will light with the highest level.

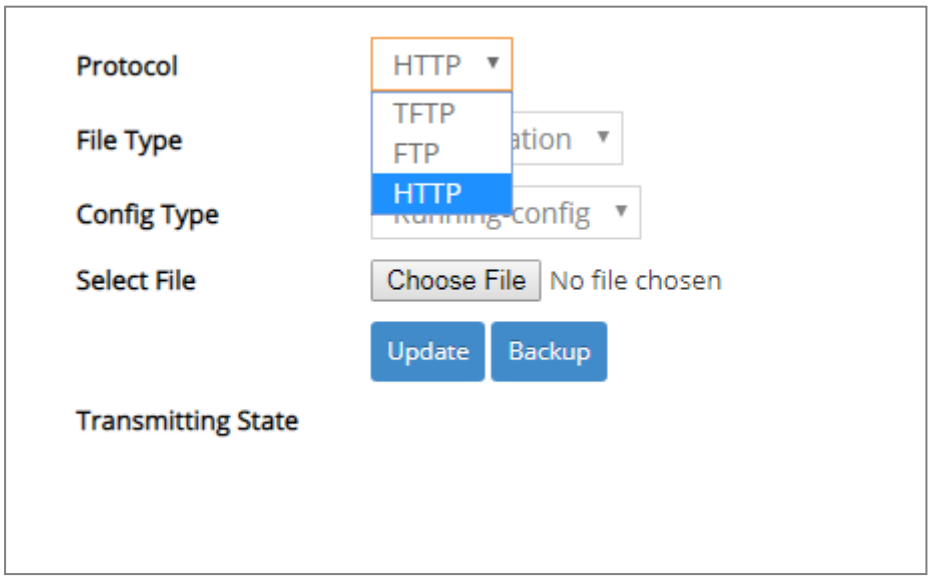
Medium: It indicates LEDs of Ports 1~6, Status LED and Power LED on the Managed Switch will light with the medium level.

Low: It indicates LEDs of Ports 1~6, Status LED and Power LED on the Managed Switch will light with the lowest level.

Off: It indicates all LEDs except Power LED on the Managed Switch will be off. Power LED will light with the lowest level.

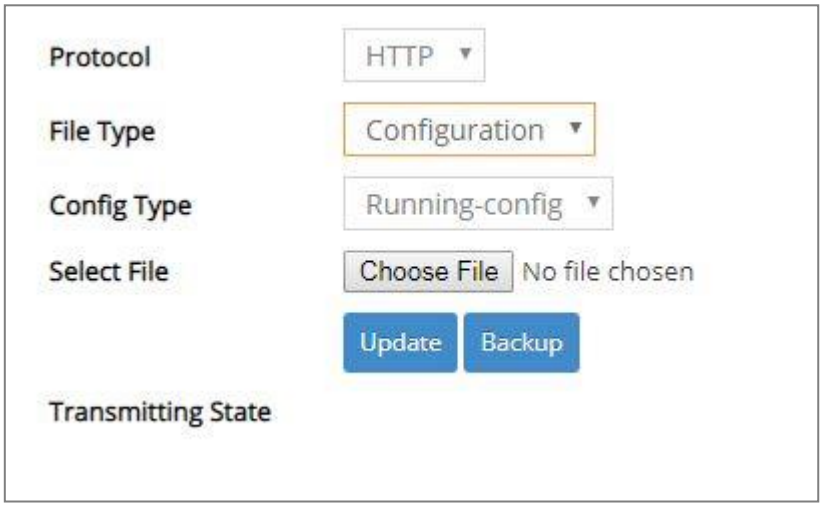
4.10.5 Firmware Upgrade

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.



4.10.5.1 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.

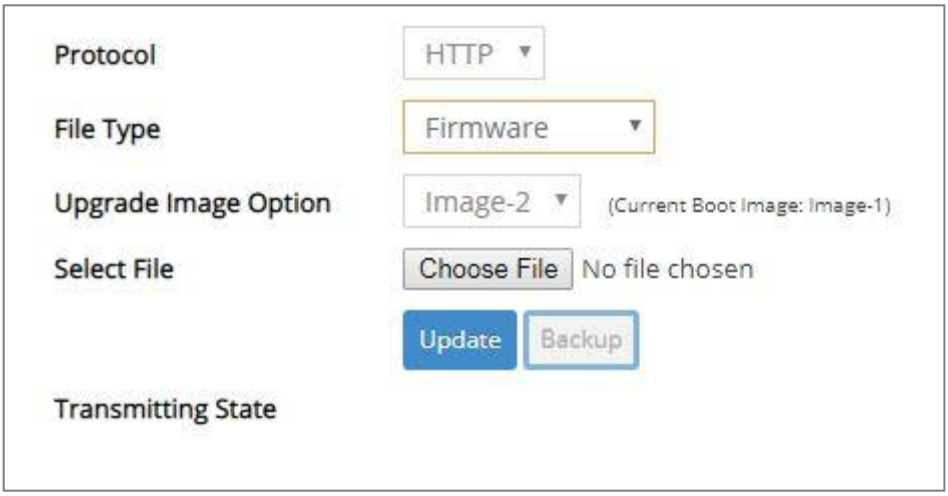
- **Running-config:** Back up the data you're processing.
- **Default-config:** Back up the data same as the factory default settings.
- **Start-up-config:** Back up the data same as last saved data.

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.

4.10.5.2 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.

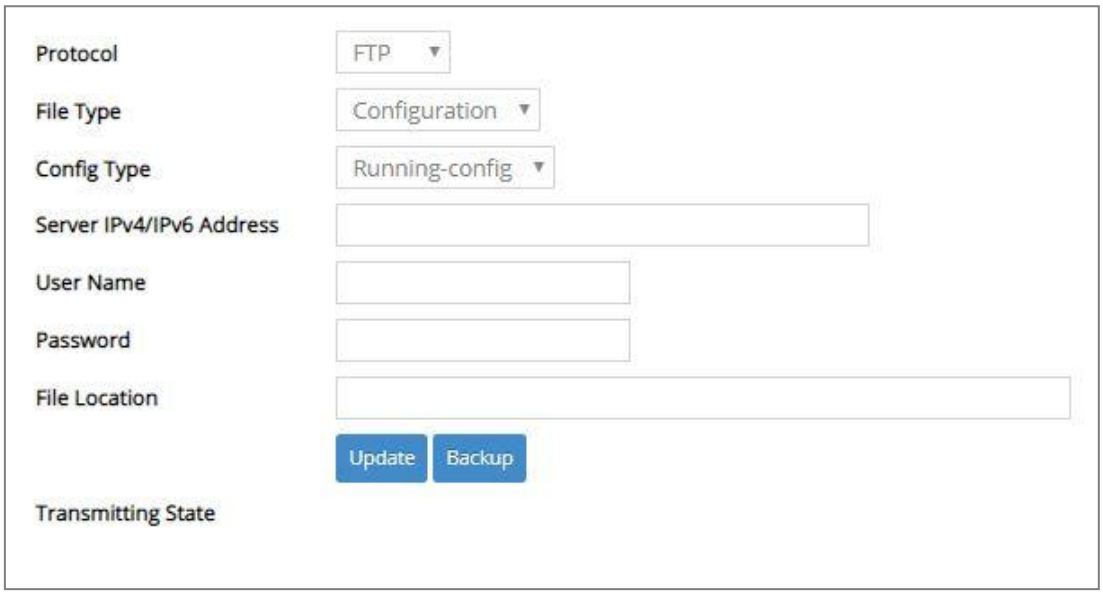


Upgrade Image Option: Pull down the list to choose the image you would like to upgrade.

Select File: Click **Choose File** to select the desired file and then click **Update** to begin the firmware upgrade.

4.10.5.3 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.

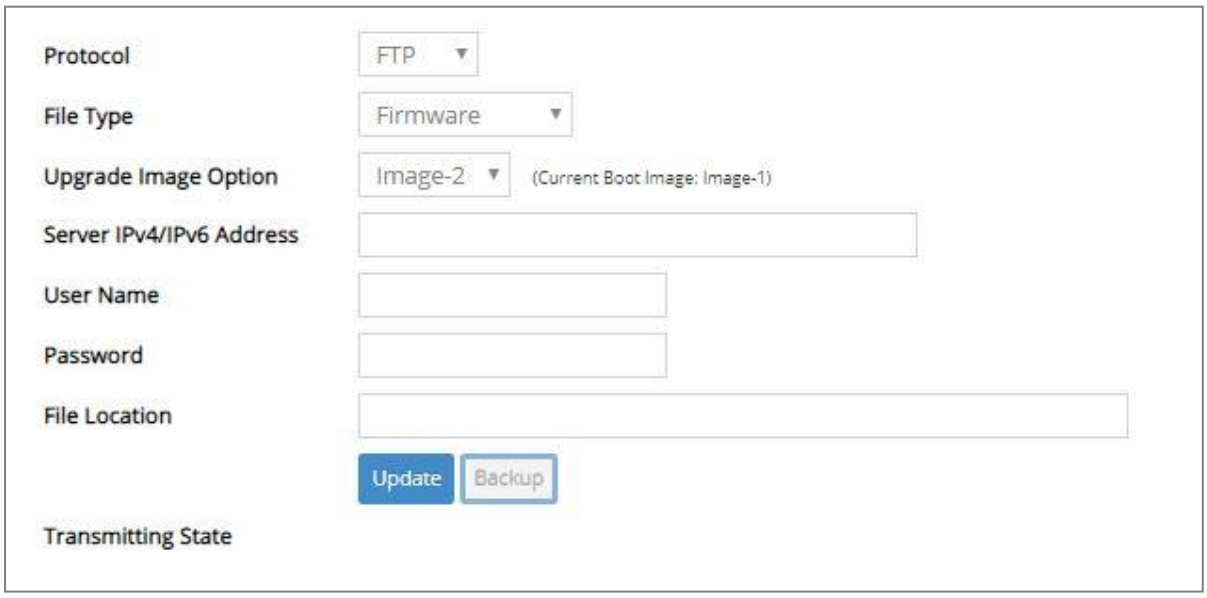
File Location: Enter the specific path and filename within the FTP/TFTP file server.

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.

4.10.5.4 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.

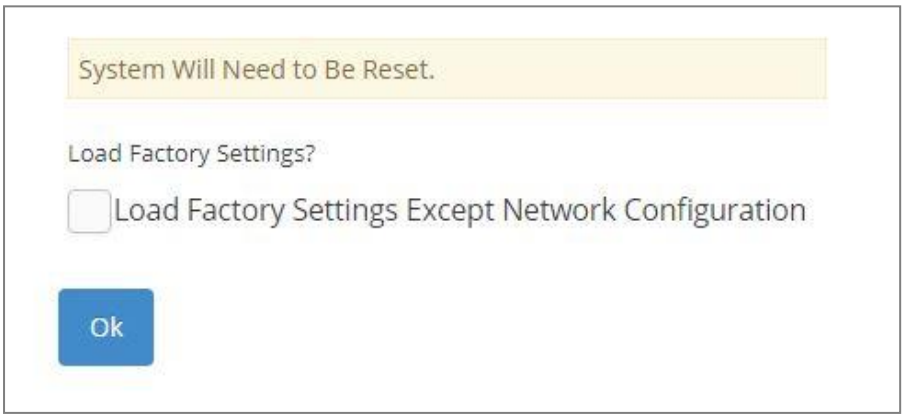
File Location: Enter the specific path and filename within the FTP/TFTP file server.

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.

4.10.6 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.



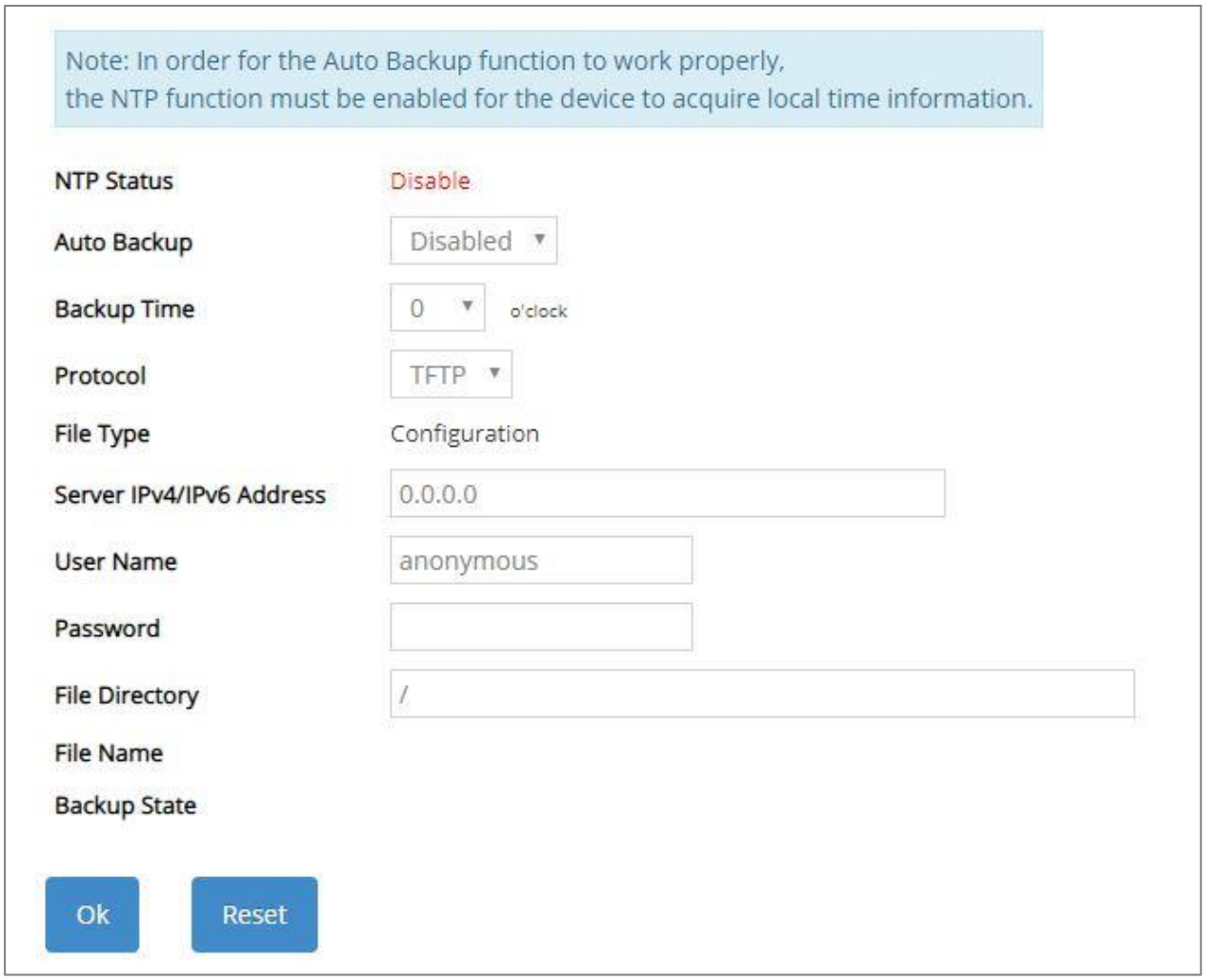
Load Factory Settings Except Network Configuration: It will set all the configurations of the Managed Switch back to the factory default settings. However, IP and Gateway addresses will not restore to the factory default. It is very useful when network administrators need to re-configure the system “REMOTELY” 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.

4.10.7 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.txt** , for example, 192.168.0.3_HES-5106SFP+_20190606.txt

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

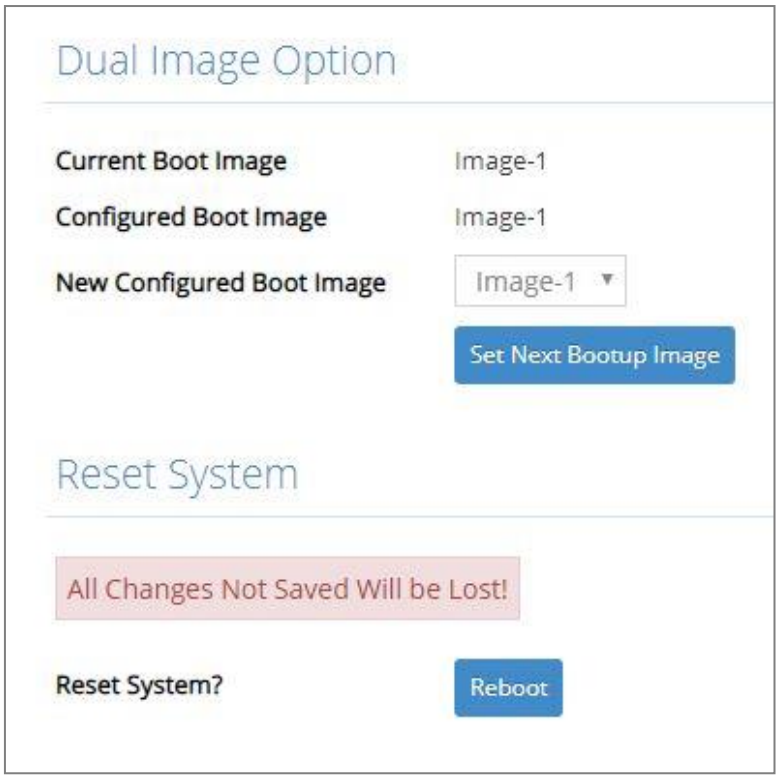
4.10.8 Save Configuration

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.

4.10.9 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

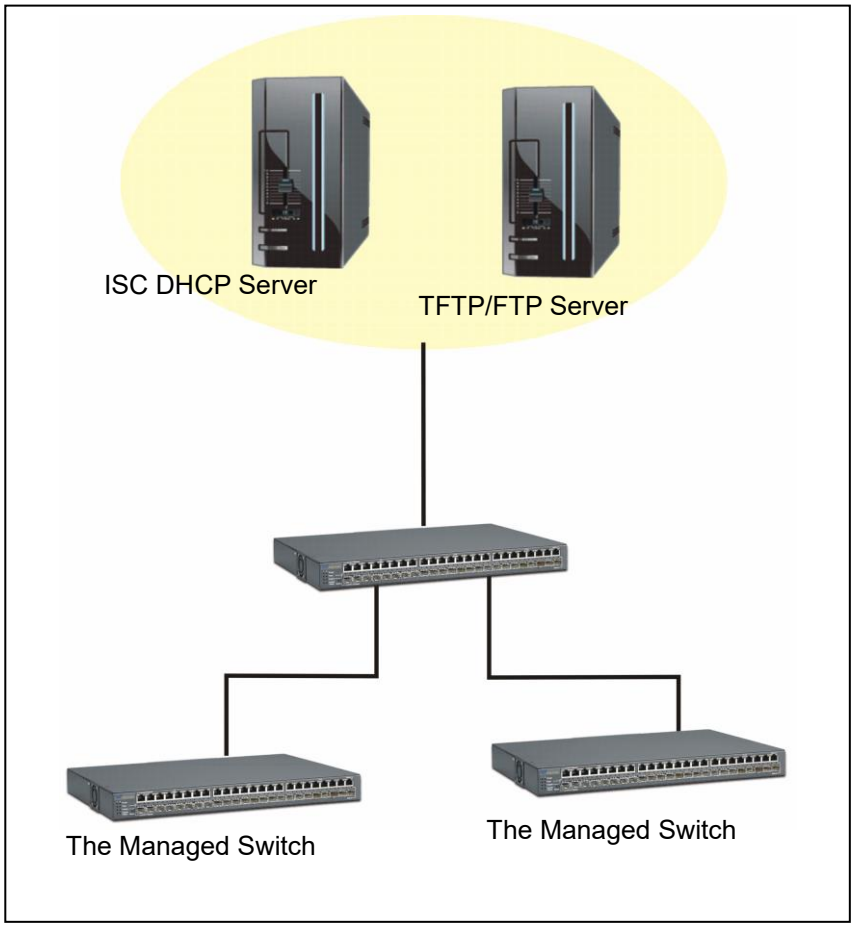
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the Managed Switch that you purchased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

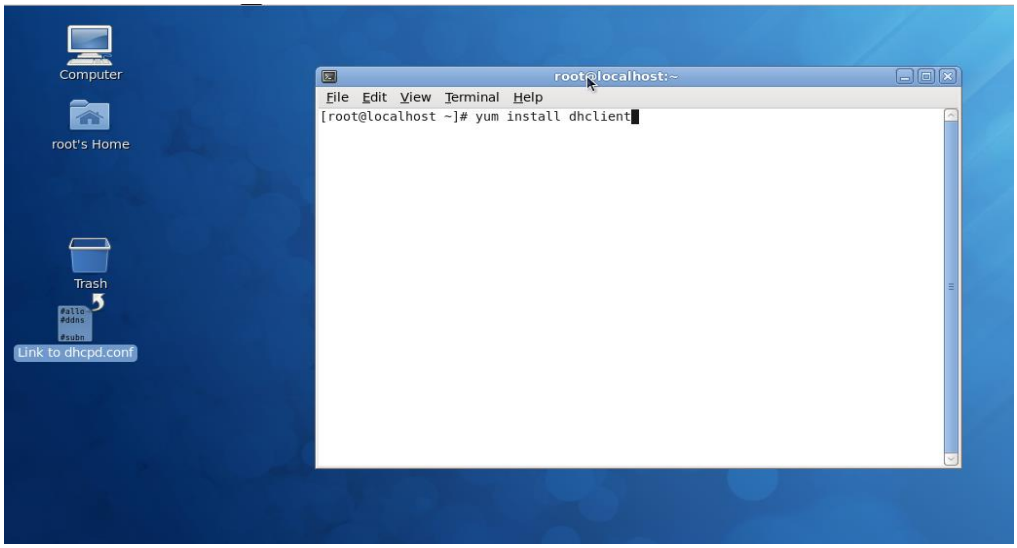
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Topology Example

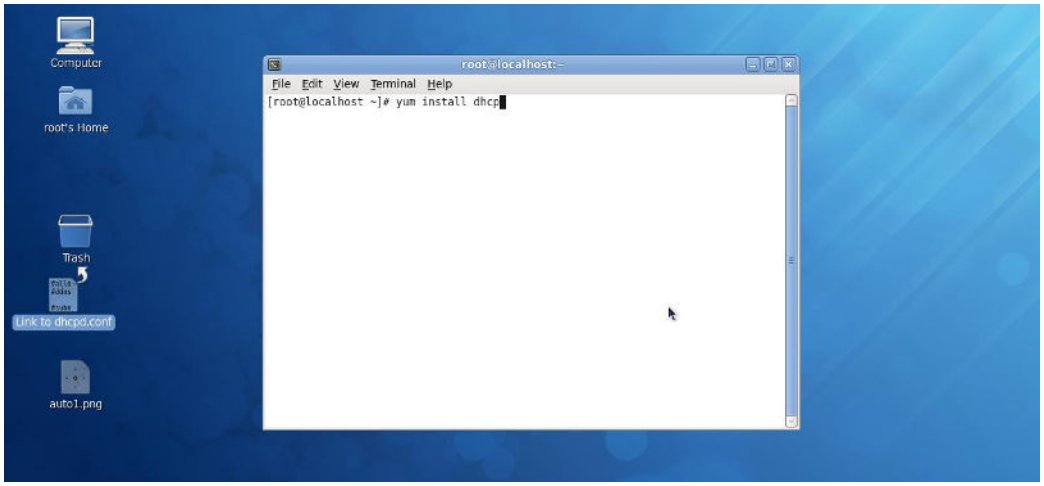
Step 2. Set up Auto Provision Server

- **Update DHCP Client**



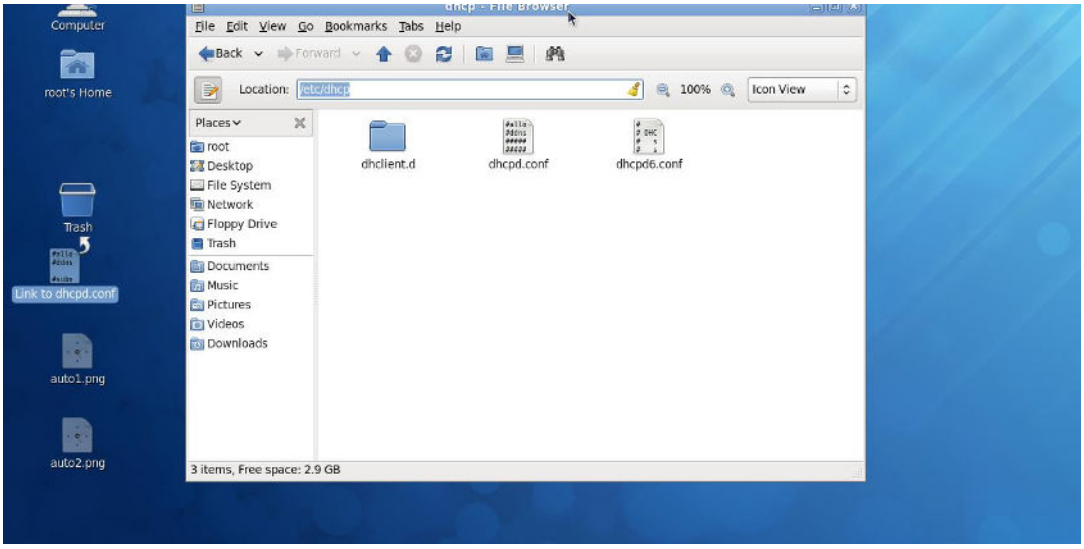
Linux Fedora 12 supports “yum” function by default. First of all, update DHCP client function by issuing “yum install dhclient” command.

- **Install DHCP Server**



Issue “yum install dhcp” command to install DHCP server.

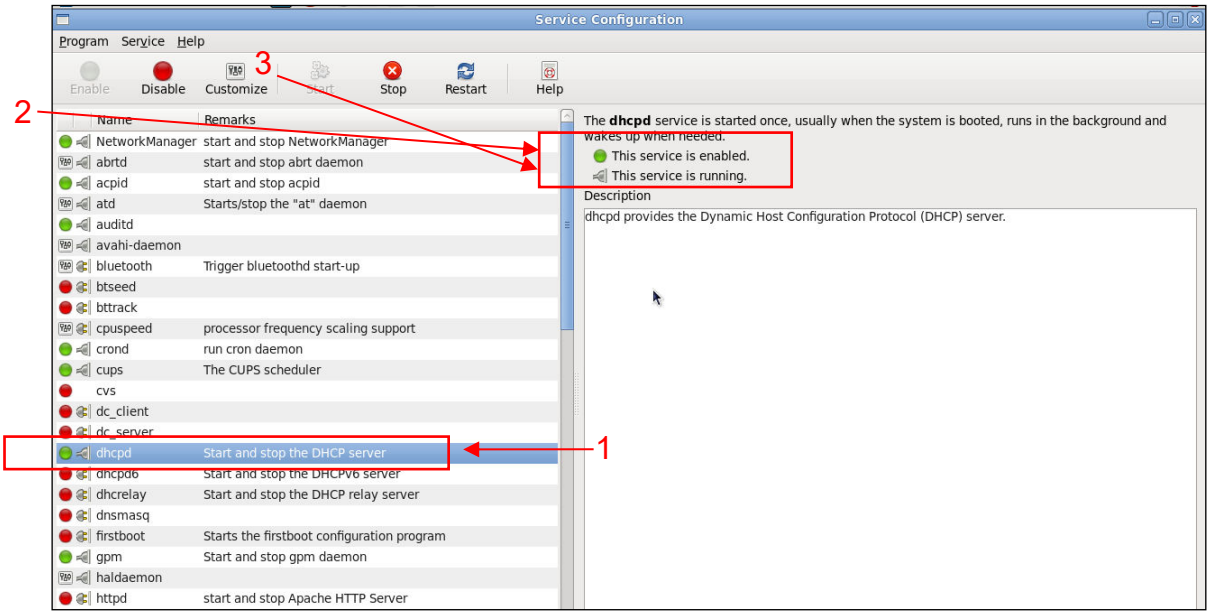
- **Copy dhcpd.conf to /etc/dhcp/ directory**



Copy dhcpd.conf file provided by the vendor to /etc/dhcp/ directory.

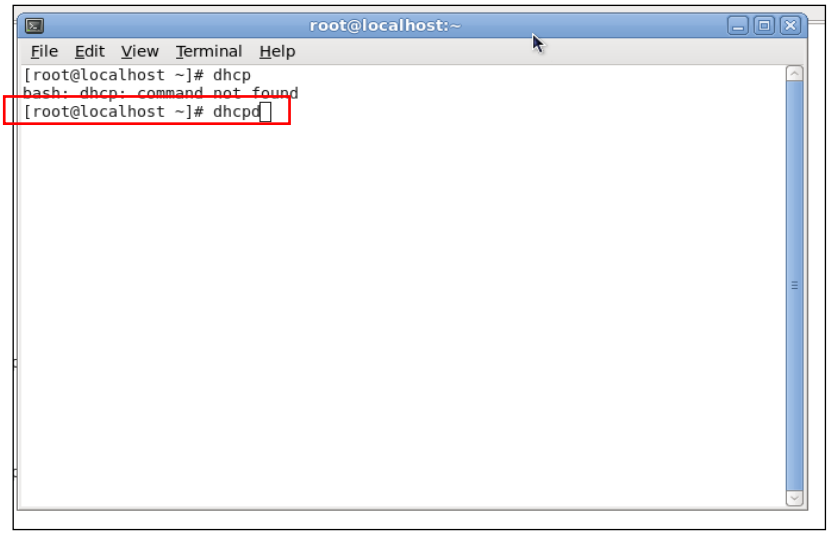
Please note that each vendor has their own way to define auto provisioning. Make sure to use the file provided by the vendor.

- **Enable and run DHCP service**



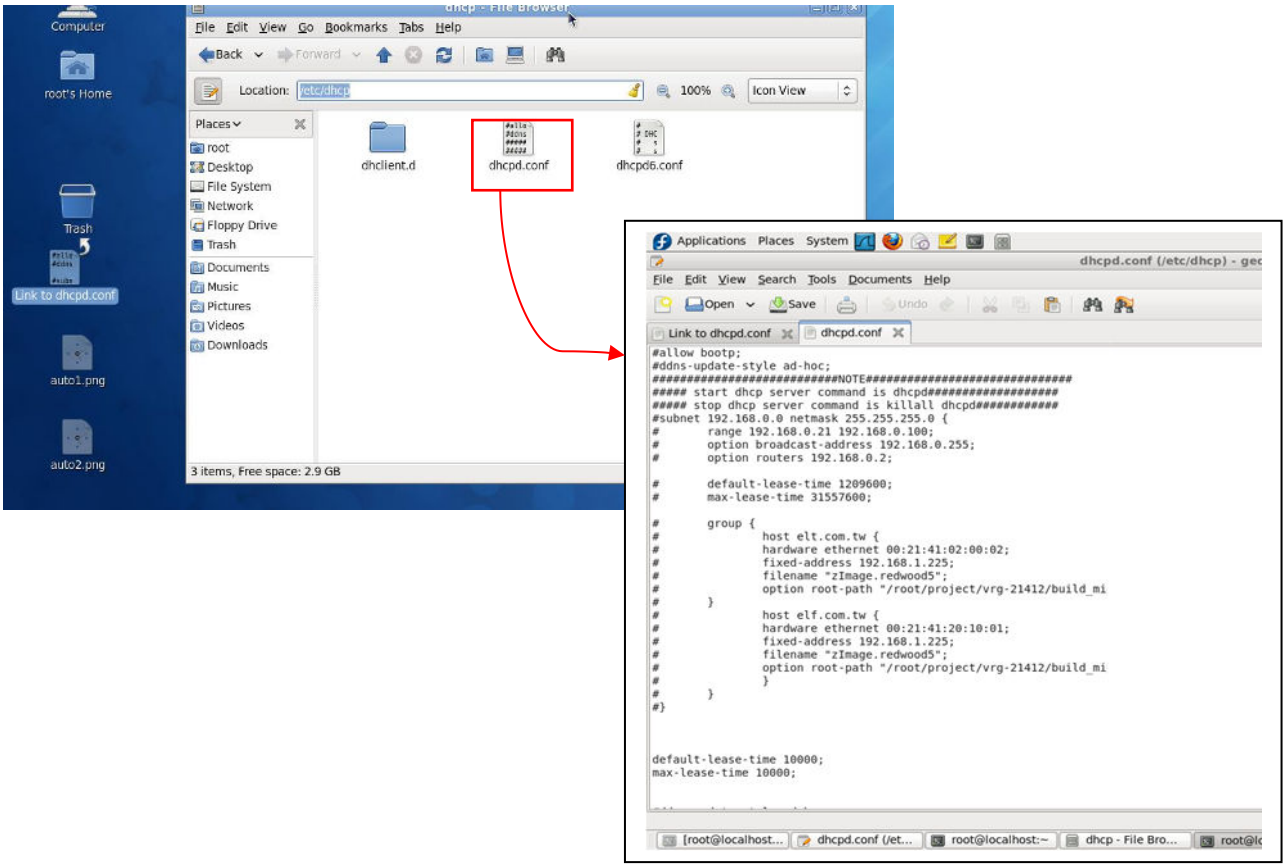
1. Choose dhcpd.
2. Enable DHCP service.
3. Start running DHCP service.

NOTE: *DHCP service can also be enabled by CLI. Issue "dhcpd" command to enable DHCP service.*



Step 3. Modify dhcpd.conf file

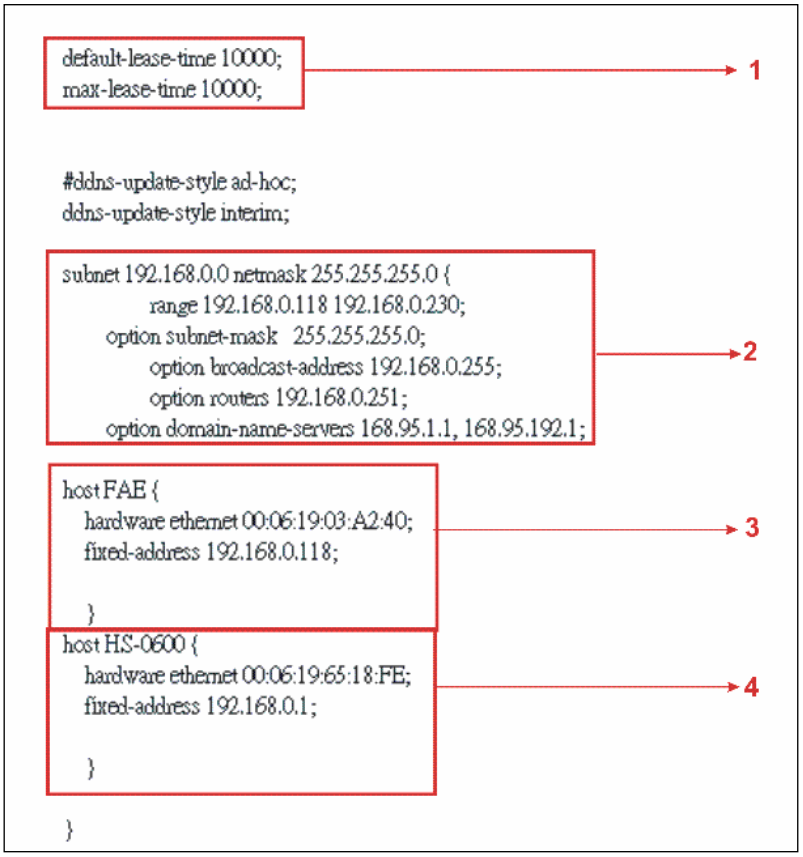
- **Open dhcpd.conf file in /etc/dhcp/ directory**



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.

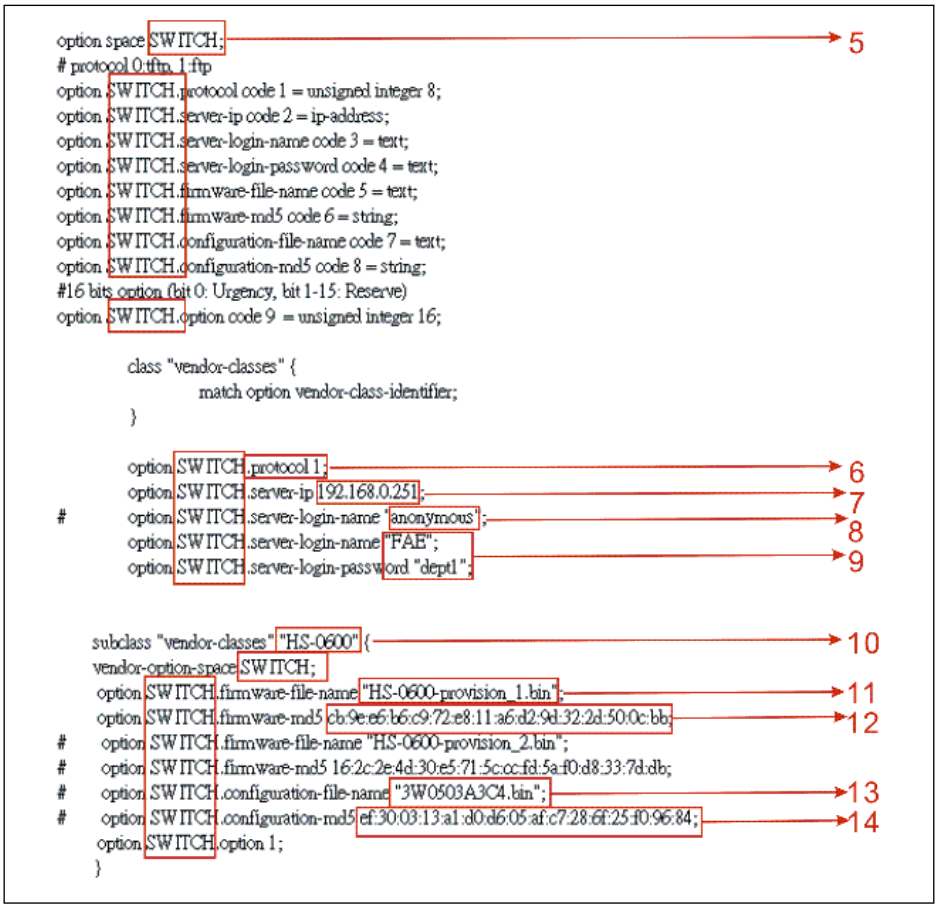
   Default lease time: If a client does not request a specific IP lease time, the server will assign a default lease time value.

   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.

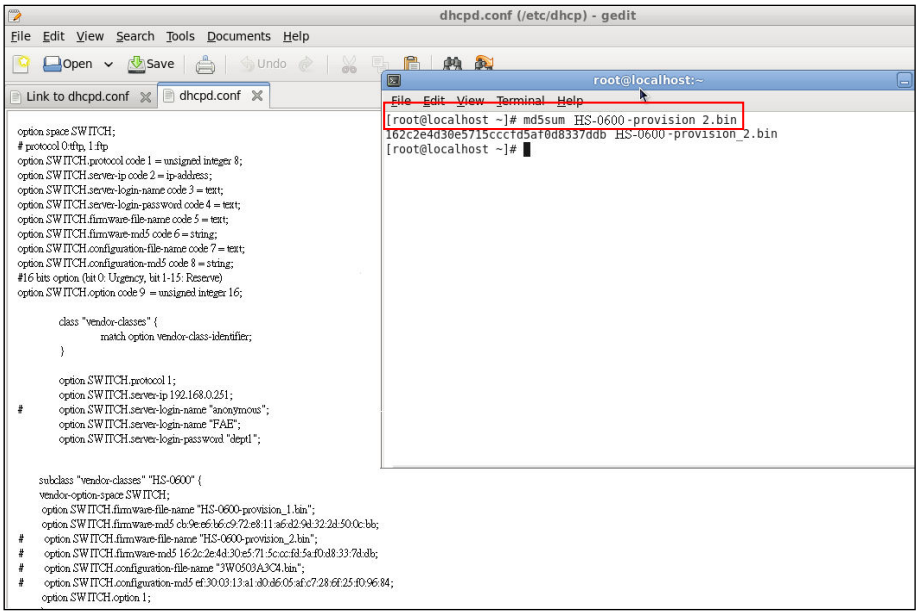
4. Map a host's MAC address to a fixed IP address. Use the same format to create multiple MAC-to-IP address bindings.



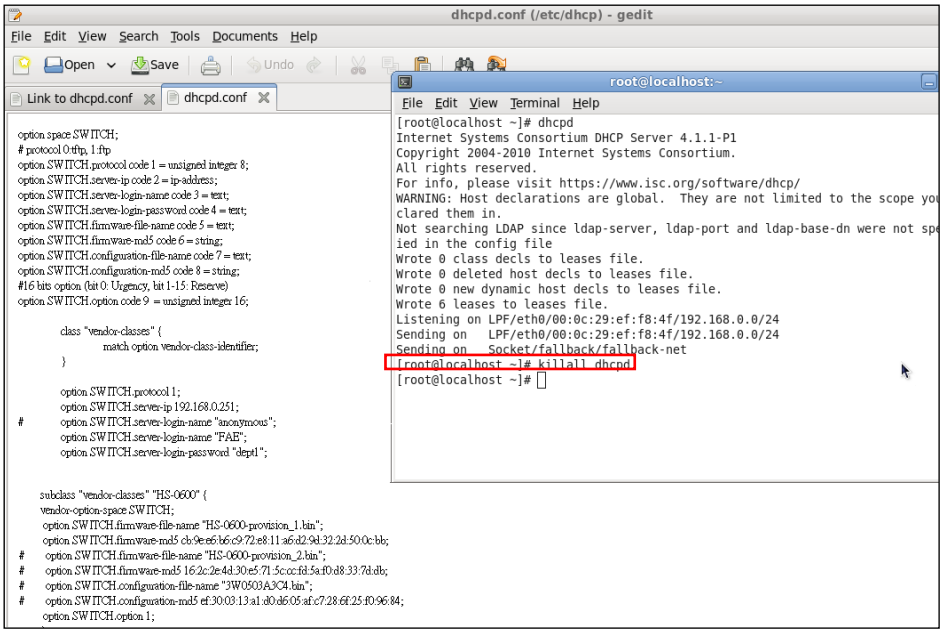
5. This value is configurable and can be defined by users.
6. Specify the protocol used (Protocol 1: FTP; Protocol 0: TFTP).
7. Specify the FTP or TFTP IP address.
8. Login TFTP server anonymously (TFTP does not require a login name and password).
9. Specify FTP Server login name and password.
10. Specify 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.

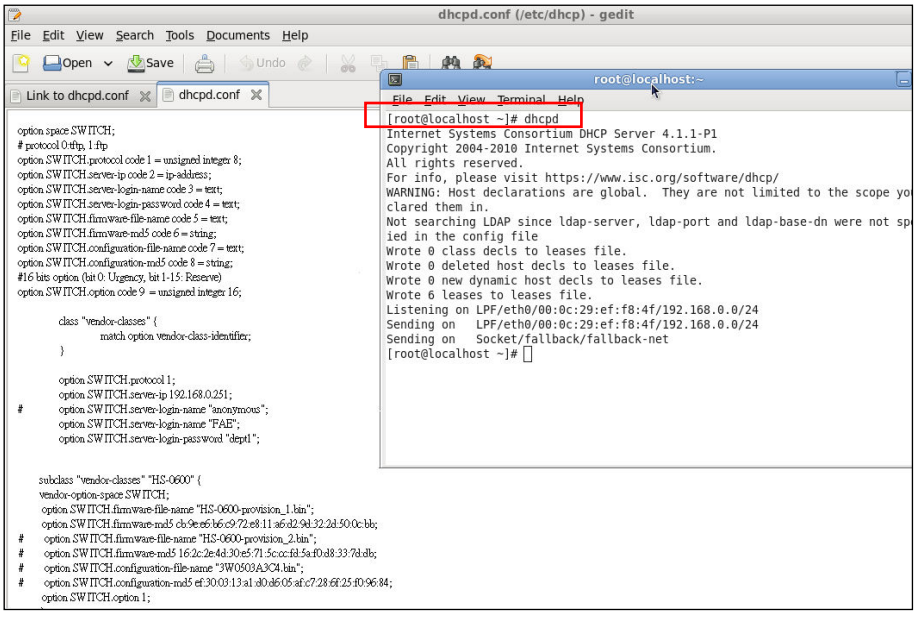
NOTE 1: *The text beginning with a pound sign (#) will be ignored by the DHCP server. For example, in the figure shown above, firmware-file-name "HS-0600-provision_2.bin" and firmware-md5 (line 5 & 6 from the bottom) will be ignored. If you want DHCP server to process these two lines, remove pound signs 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.

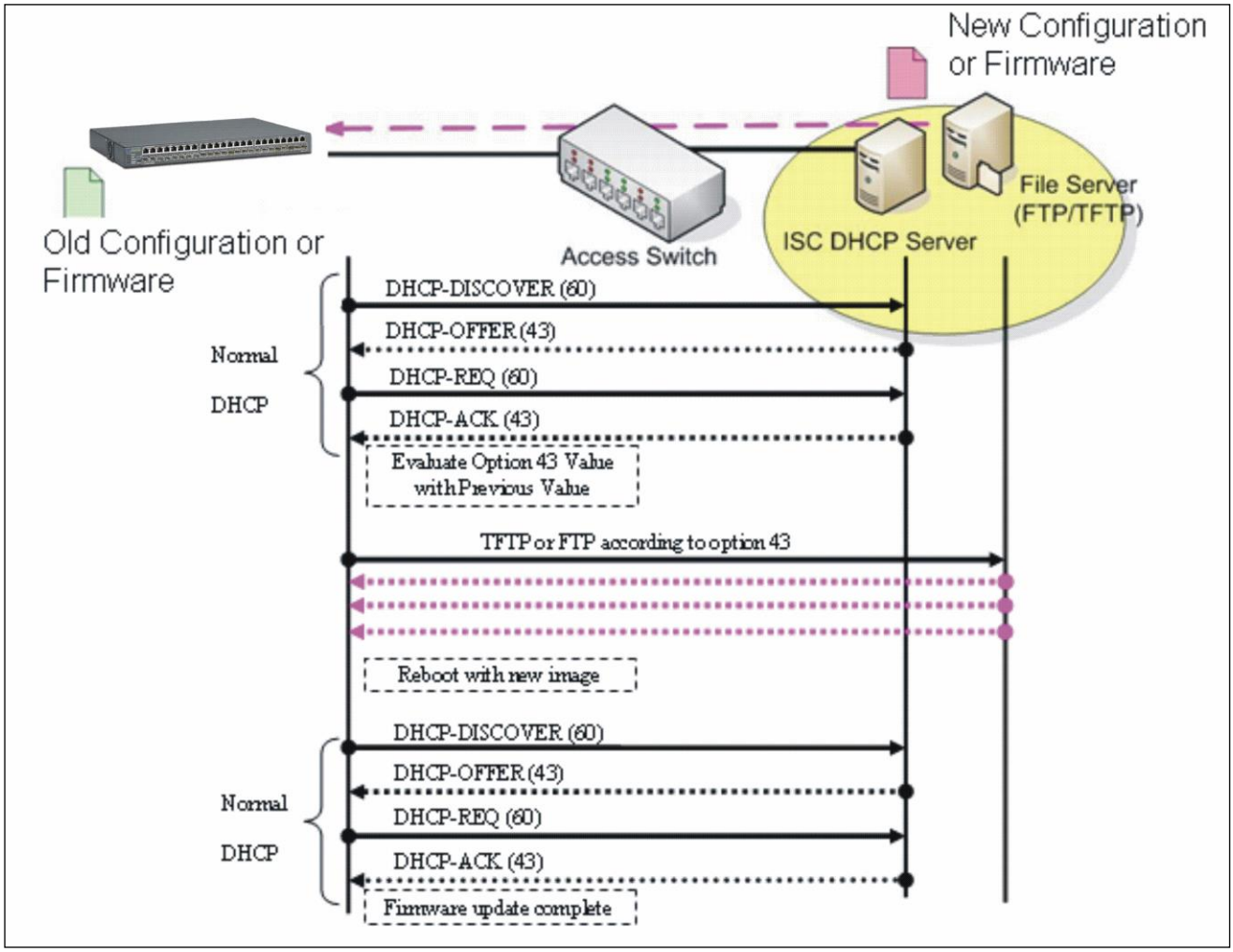
Step 5. Place a copy of Firmware and Configuration File in TFTP/FTP

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

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.

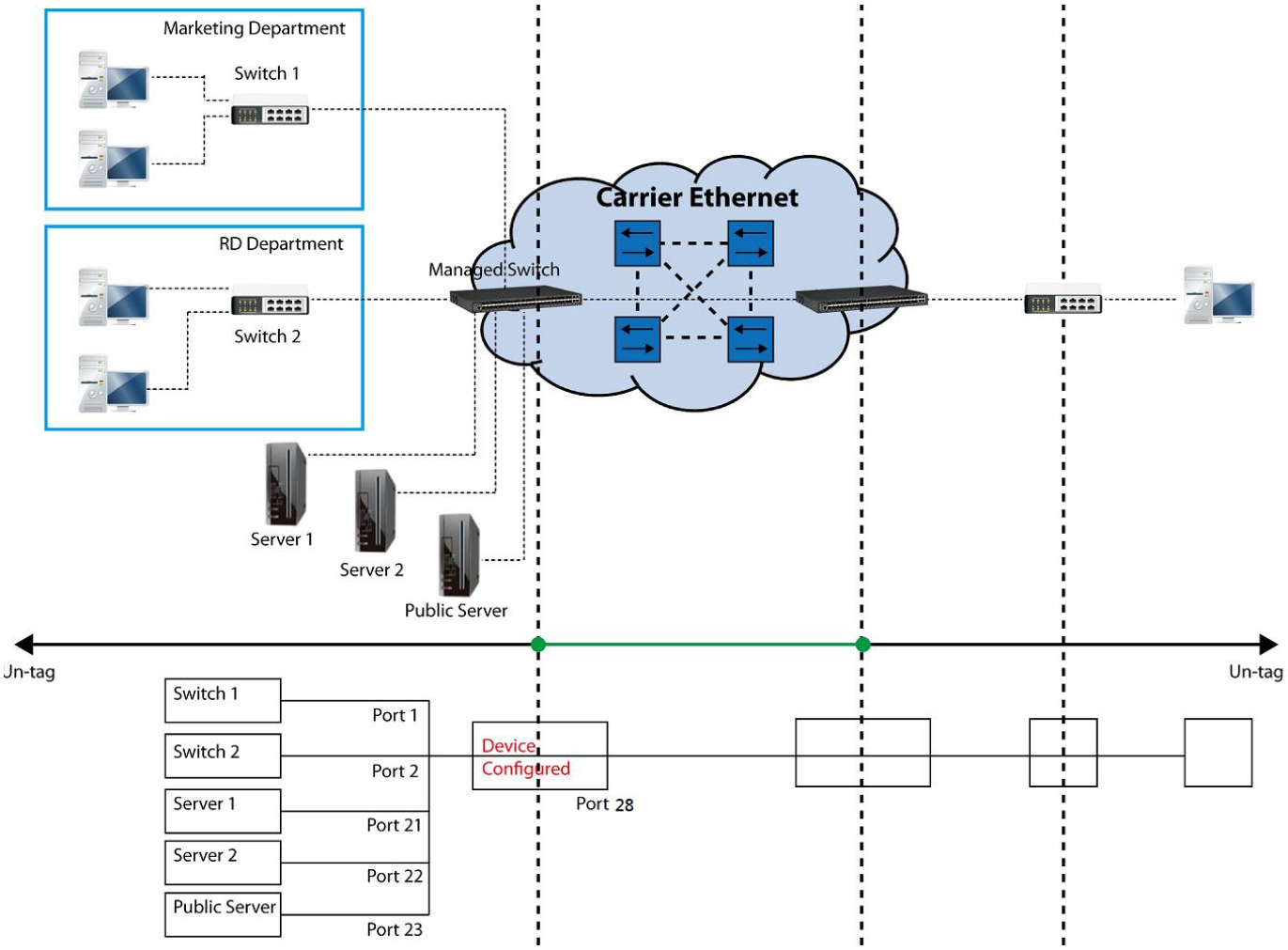
While this application note can not cover all of the real-life applications that are possible on this Managed Switch, it does provide the most common applications largely deployed in most situations. In particular, this application note provides a couple of network examples to help users implement Port-Based 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 !`

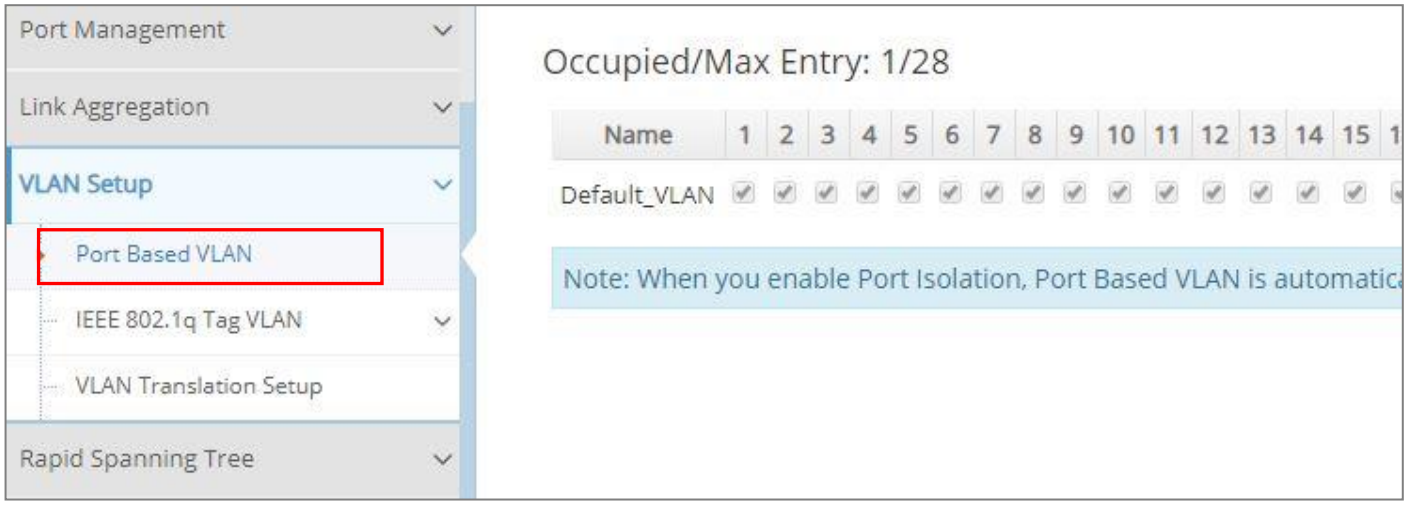
5. Return to Global Configuration mode, and select port 2, 22, 23 and 28 to configure.	`Switch(config-if-1,21,23,28)# exit`
	`Switch(config)# interface 2,22,23,28`
	`Switch(config-if-2,22,23,28)#`

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.

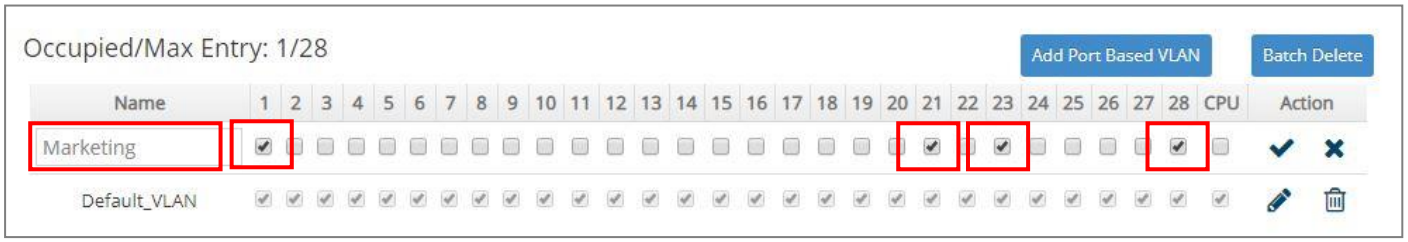
Web Management Configuration:

1. **Select “Port Based VLAN” option in VLAN Setup menu.**
   VLAN Setup > Port Based VLAN



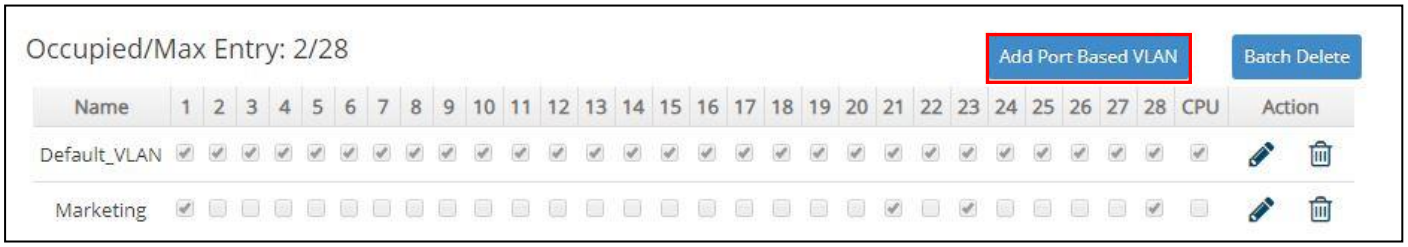
2. **Click “Add Port Based VLAN” to add a new Port-Based VLAN**
   VLAN Setup>Port Based VLAN>Add Port Based VLAN

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

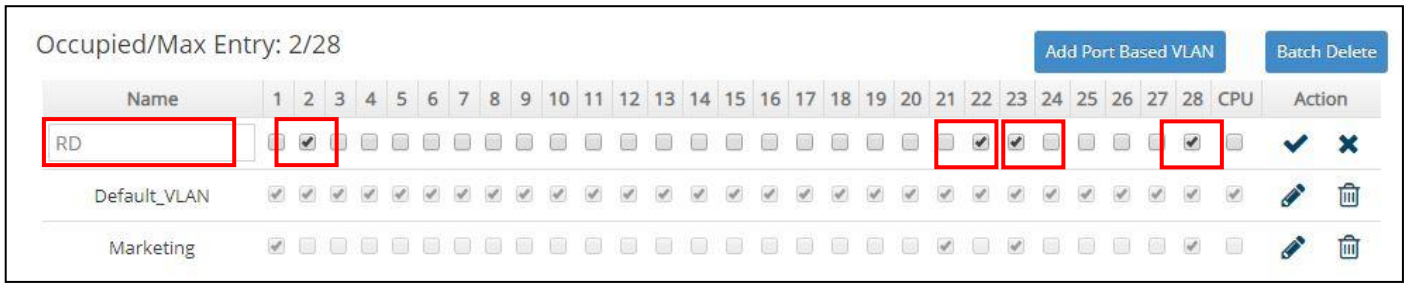


Click ✔ to apply the new settings when completing.

4. **Click “Add Port Based VLAN” again to add a new Port-Based VLAN.**
   VLAN Setup>Port Based VLAN> Add Port Based VLAN

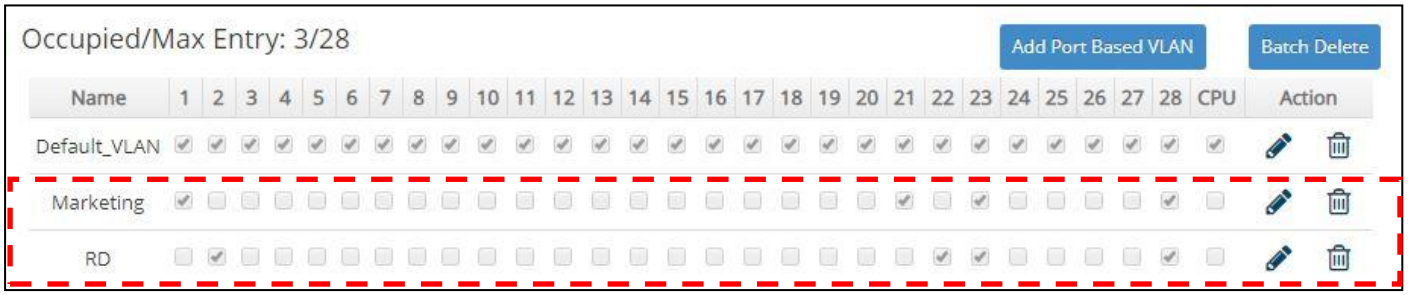


5. **Add Port 2, 22, 23 and 28 in a group and name it to “RD”.**
   VLAN Setup>Port Based VLAN>Add Port Based VLAN



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.

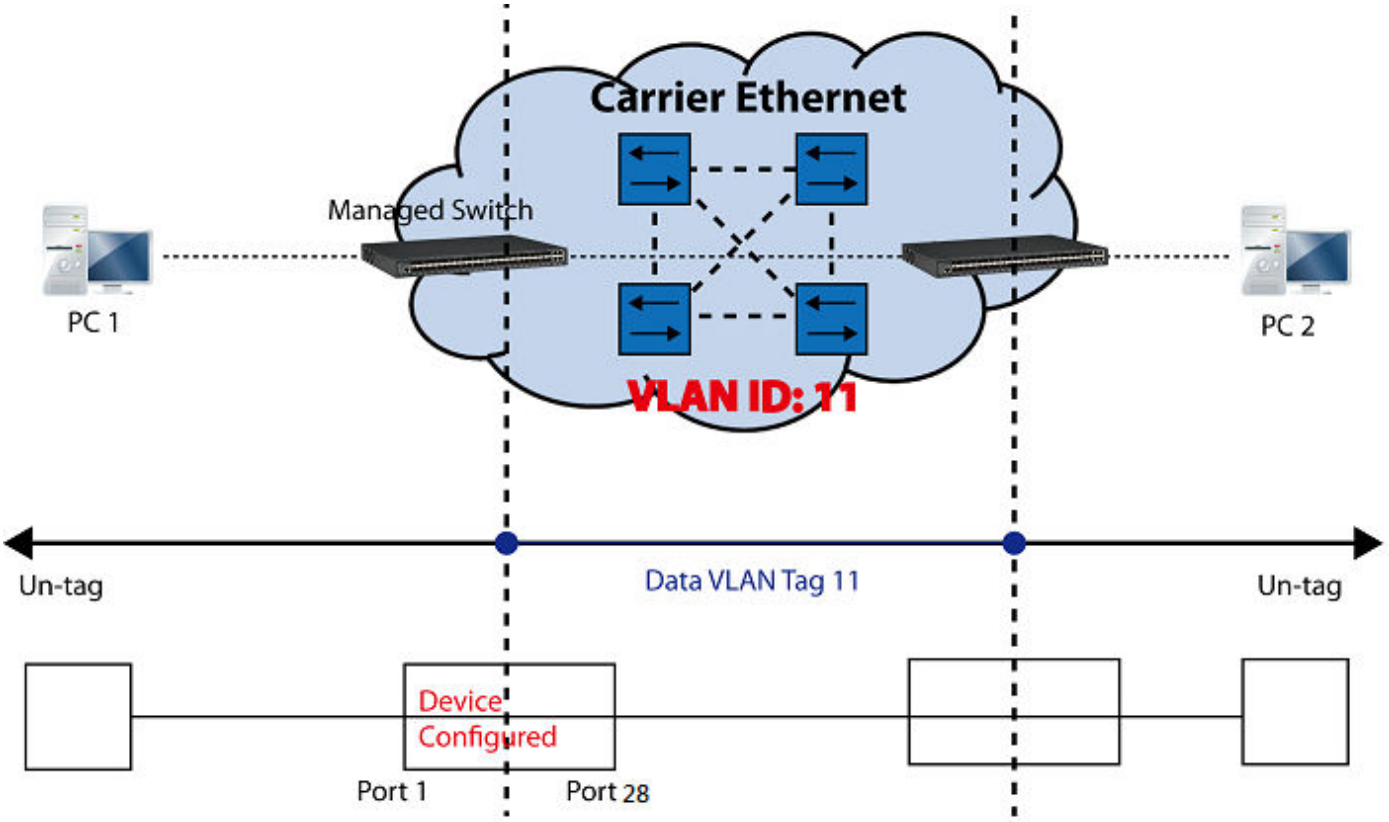
3. A tagged packet with any permissible VID arrives at Port 1
Tagged packets received on the Managed Switch will be forwarded out tagged. Therefore, in this example, the Managed Switch will look at the Port-Based forwarding table for Port 1 and forward tagged packets to member port 21, 23, and 28.

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)#`

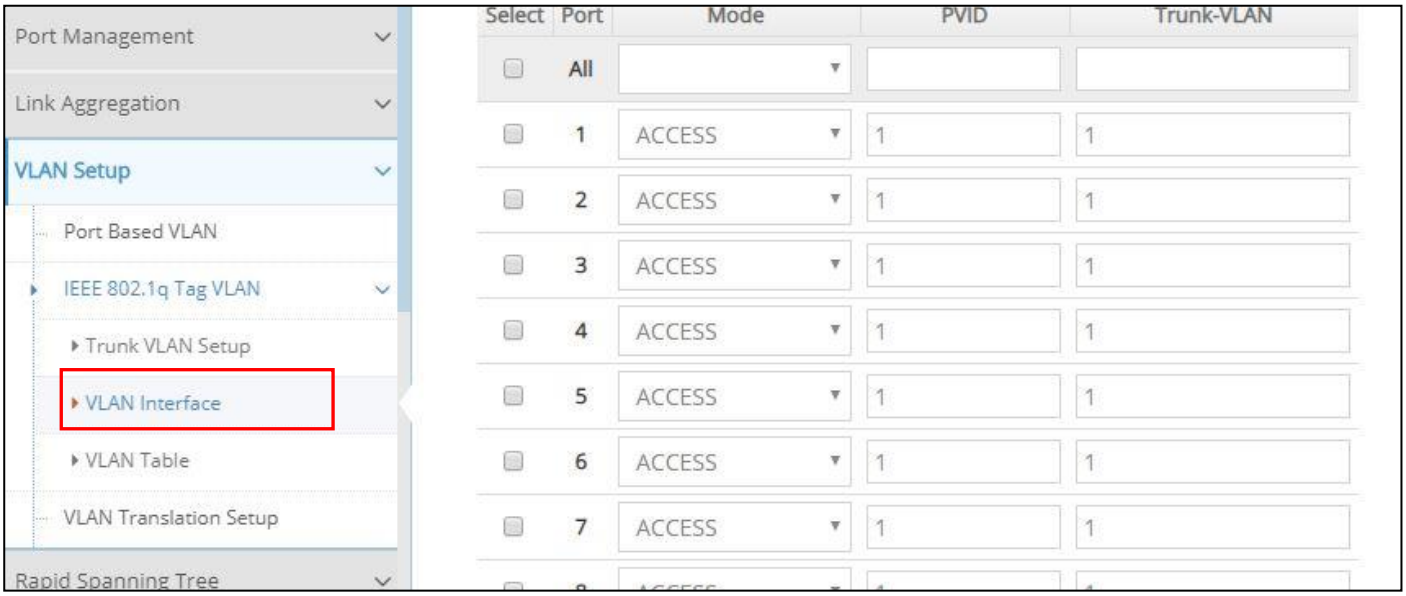
2. Create VLAN 11 and assign Port 1 and Port 28 to VLAN 11.	`Switch(config)# interface 1,28`
	`Switch(config-if-1,28)# vlan dot1q-vlan trunk-vlan 11`
	`OK !`
	`Switch(config-if-1,28)# exit`

3. Name VLAN 11 as “DataVLAN”.	`Switch(config)# vlan dot1q-vlan 11`
	`Switch(config-vlan-11)# name DataVLAN`
	`OK !`
	`Switch(config-vlan-11)# exit`

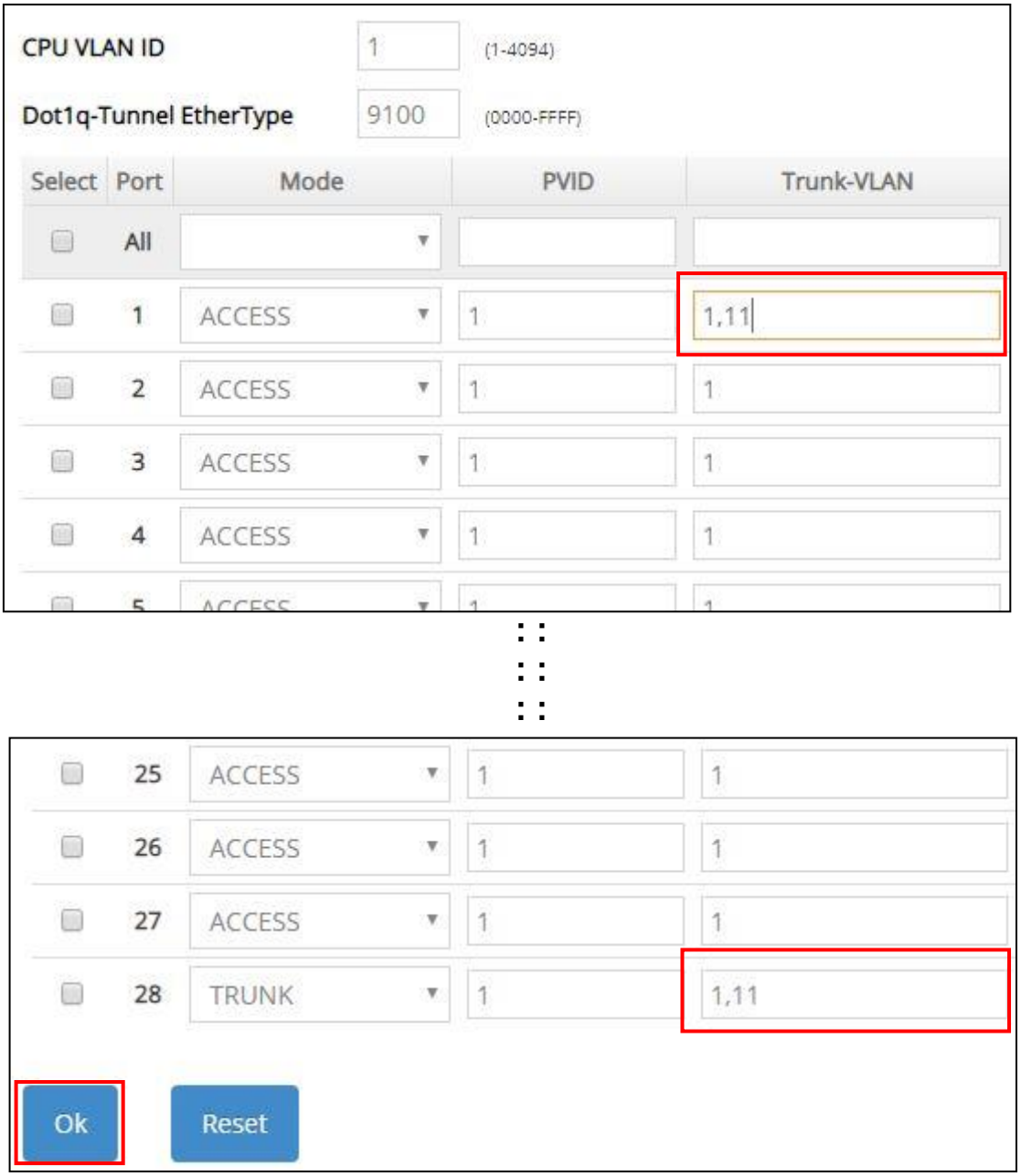
4. Set Port 28 to trunk mode.	Switch(config)# interface 28 Switch(config-if-28)# vlan dot1q-vlan mode trunk OK ! Switch(config-if-28)# exit
5. Change Port 1's Access VLAN ID into "11".	Switch(config)# interface 1 Switch(config-if-1)# vlan dot1q-vlan pvid 11 OK ! Switch(config-if-1)# exit
6. Show currently 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

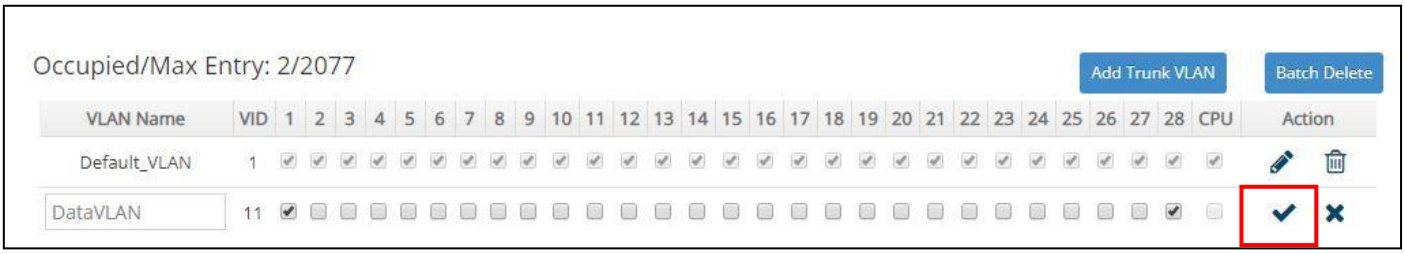


2. **Create a new Data VLAN 11 that includes Port 1 and Port 28 as members.**
   VLAN Setup>IEEE 802.1q Tag VLAN>VLAN Interface



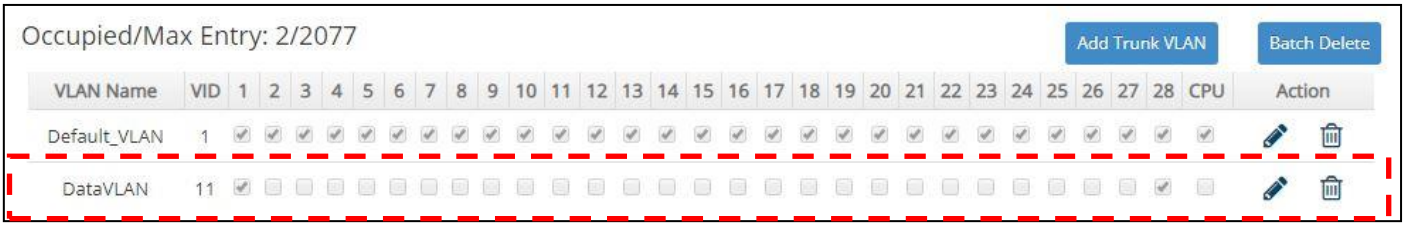
Click **OK** to apply the new settings when completing..

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

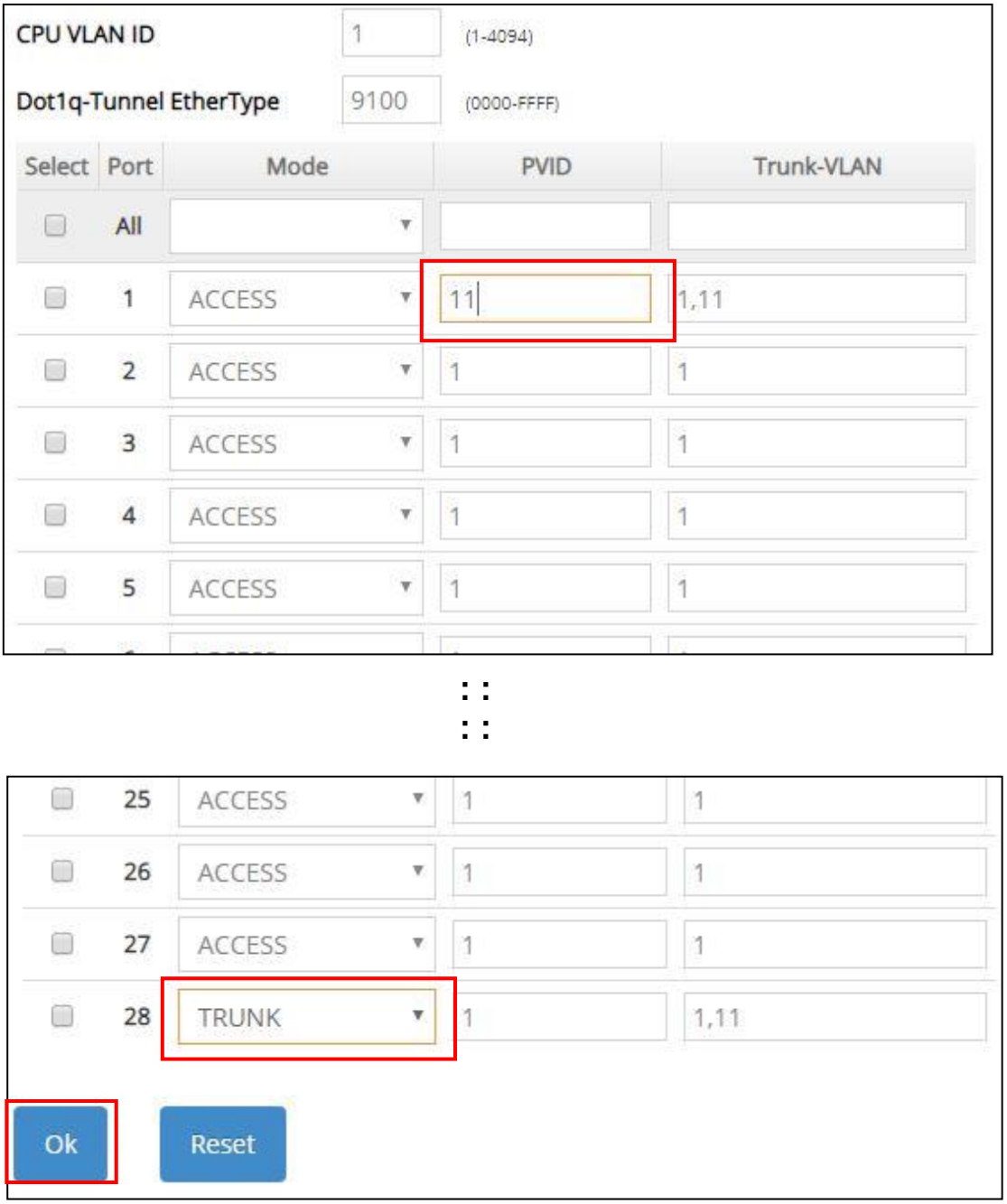


Click ✔ to apply the new settings when completing.

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.

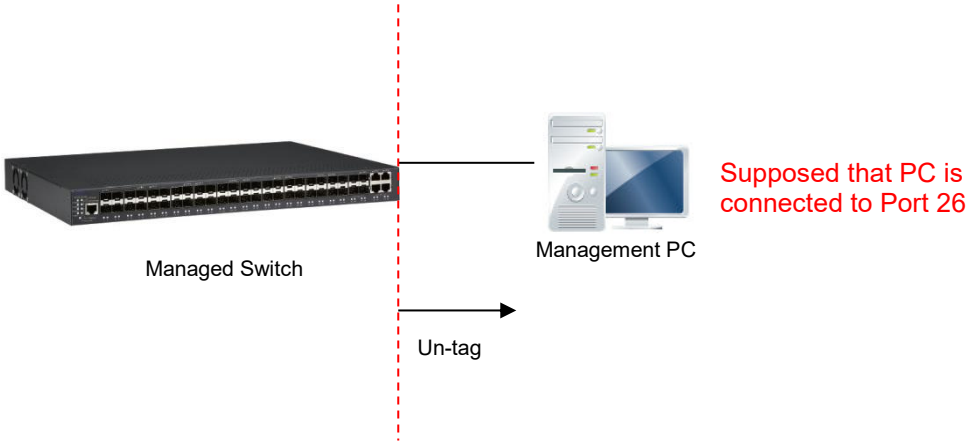
III. Management VLAN

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.



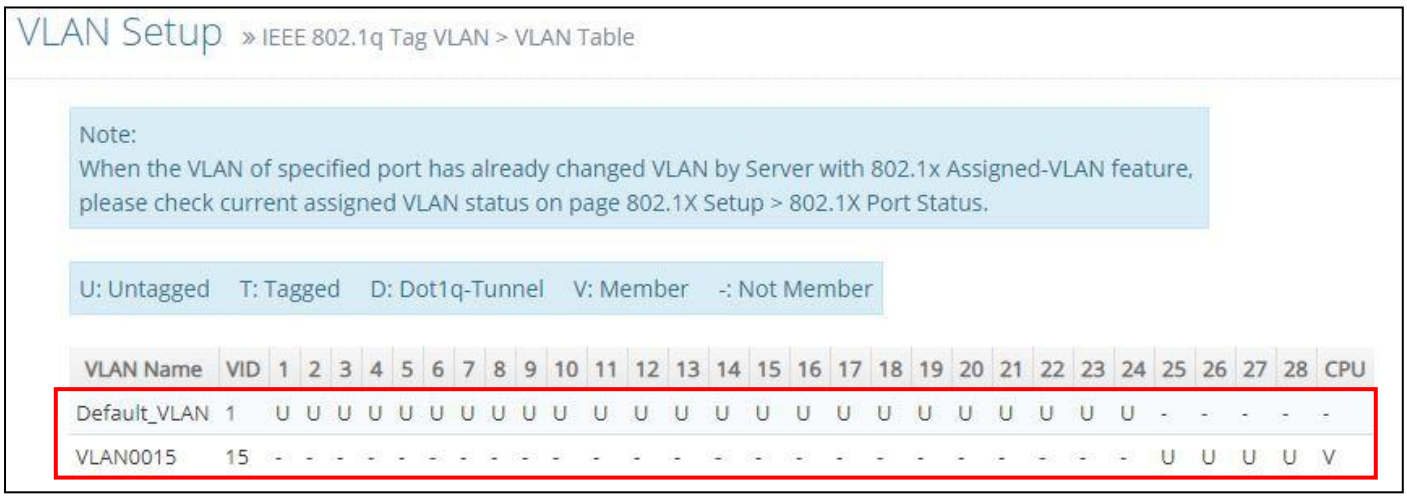
Management VLAN Network Diagram

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****.*

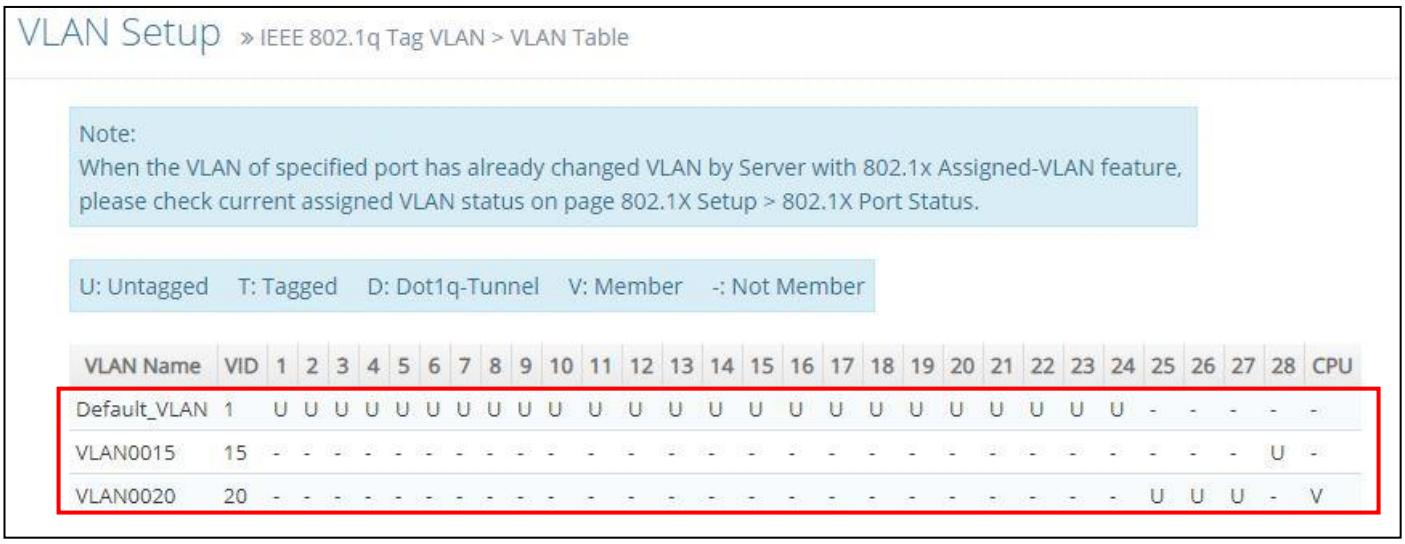


2. Now, change the Management VLAN 15 into VLAN 20 and includes Port 25, 26 and 27 under Access mode (It's necessary to include Port 26 to prevent the disconnection.)

VLAN Setup>IEEE 802.1q Tag VLAN>VLAN Interface

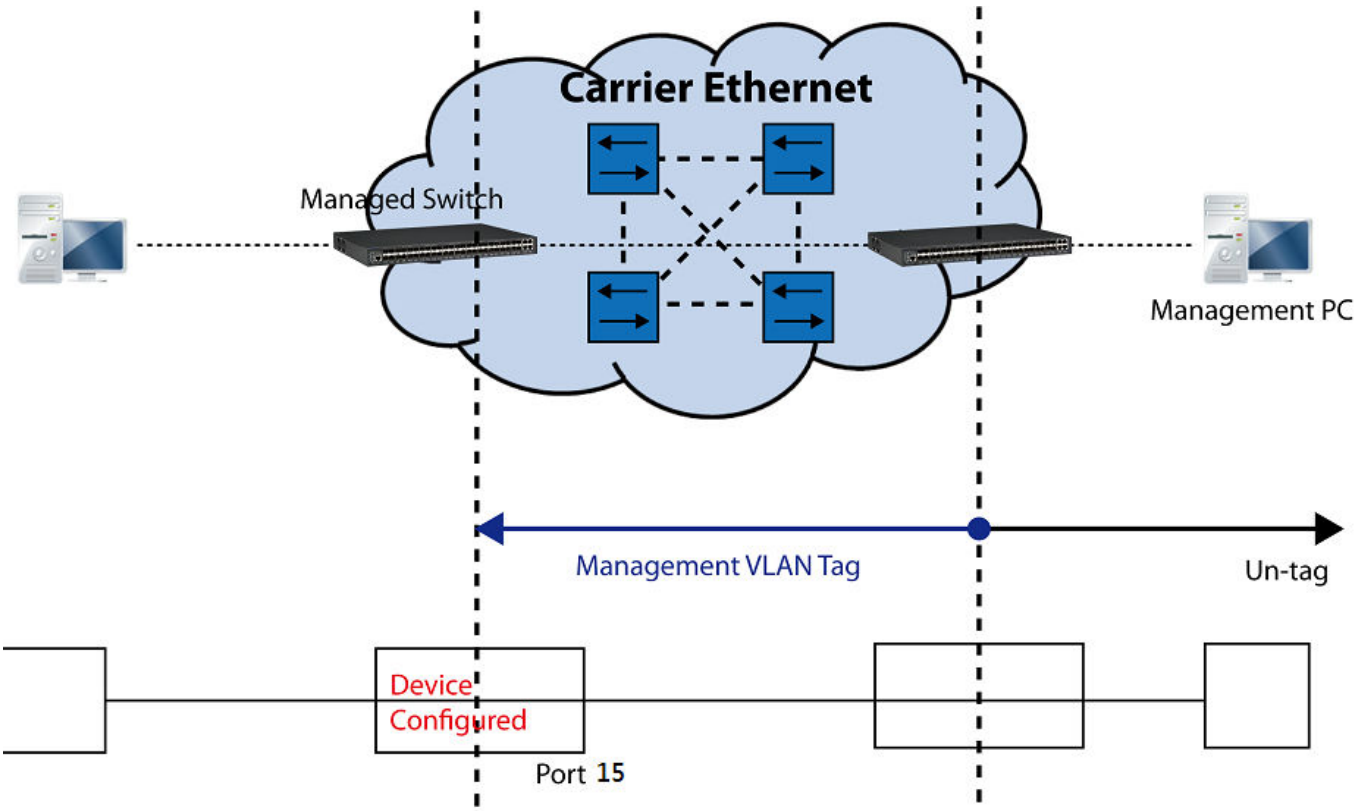
Click **OK** to apply the new settings when completing..

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.



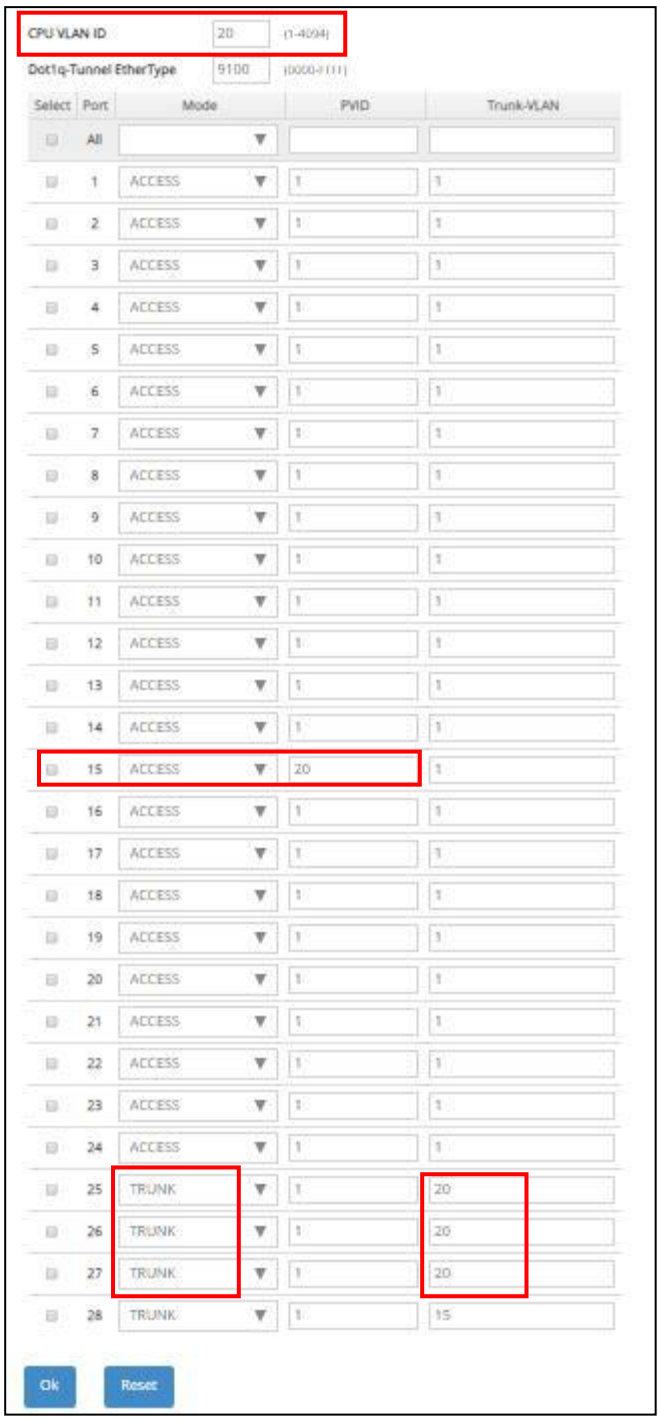
Management VLAN Network Diagram

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.

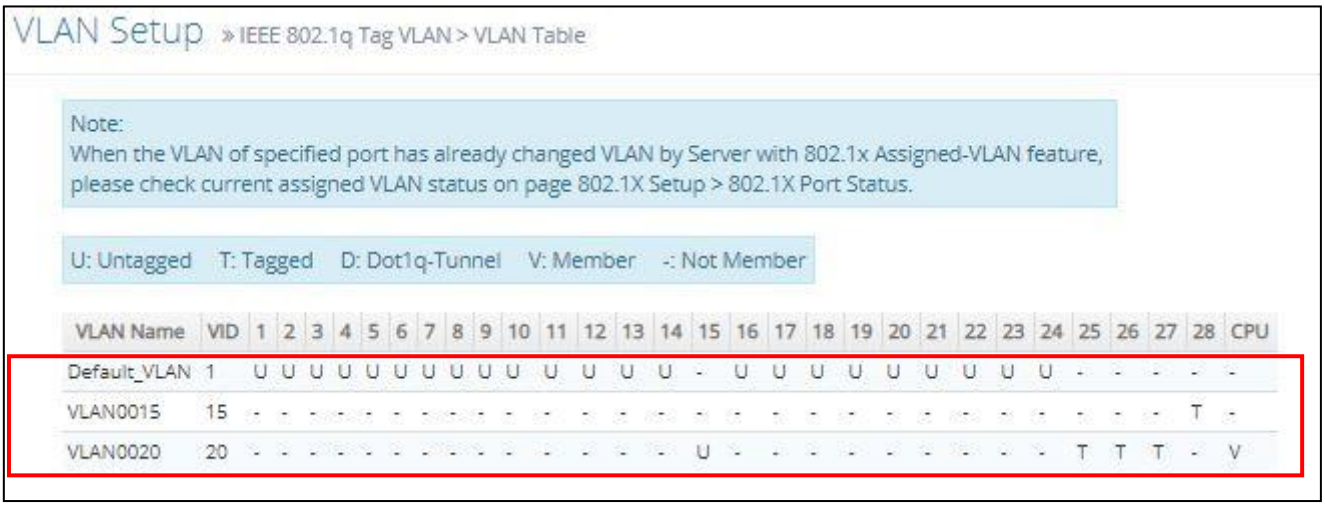


Click **OK** to apply the new settings when completing.

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):

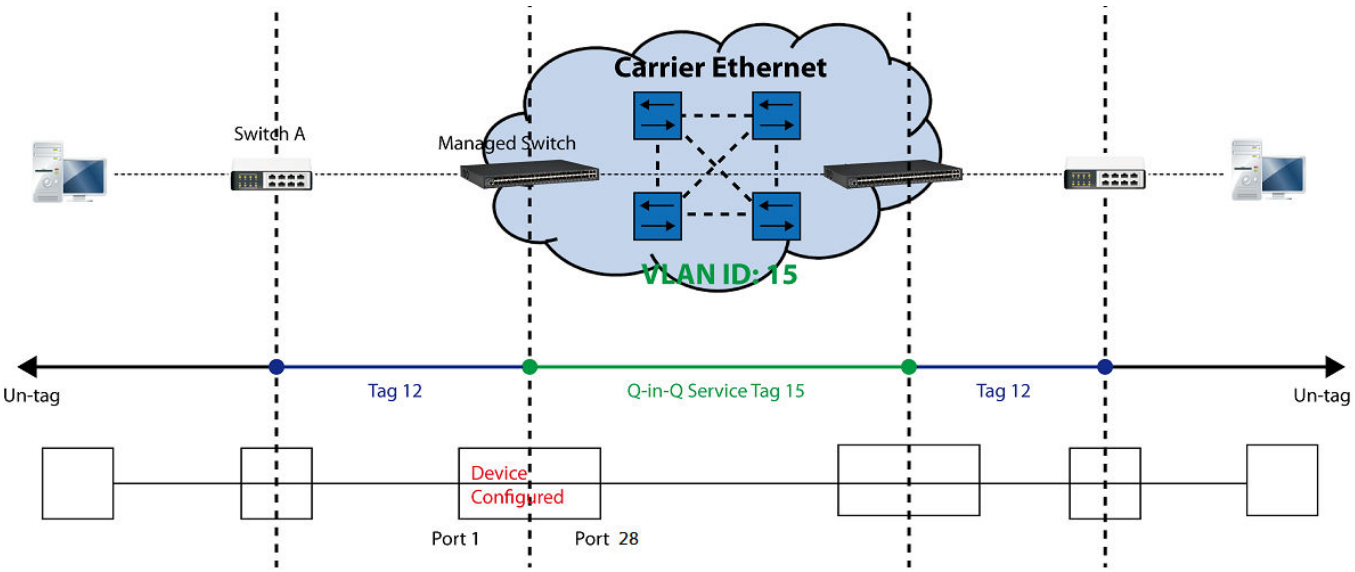
This part is to demonstrate how to change Management VLAN 15 into VLAN 20 on specified ports under Trunk mode. Supposed that we have the existing Management VLAN 15 on Port 25,26,27,28 and CPU, we can create new Management VLAN 20 as required. Here, we supposed that the Management PC is remotely connected 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`

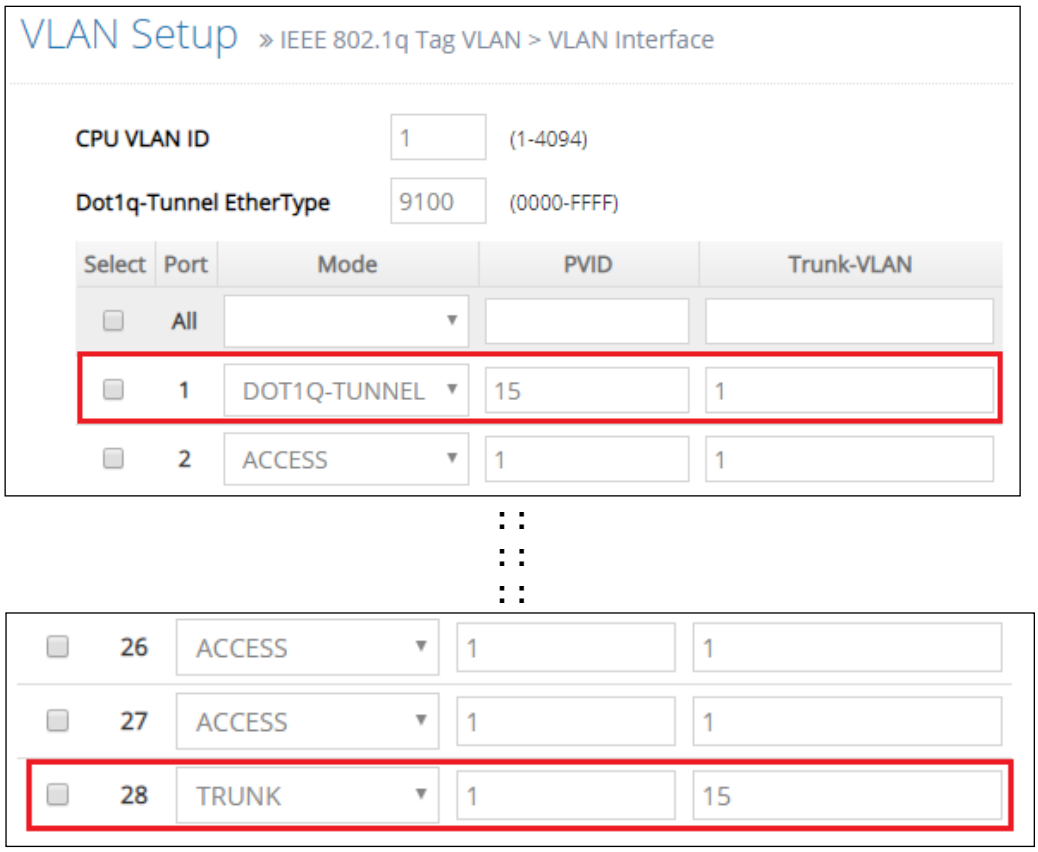
4. Show currently configured dot1q VLAN membership.	`Switch(config)# show vlan interface`
	`==========`
	`IEEE 802.1q Tag VLAN Interface`
	`==========`
	`CPU VLAN ID : 1`
	`Dot1q-Tunnel EtherType : 0x9100`
	
	`Port P-Bit Port VLAN Mode PVID Trunk-vlan`
	`---- ----- ---------- ---- ----------`
	`1 0 dot1q 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.

This page is intentionally left blank.