CONNECTION TECHNOLOGY SYSTEMS

FOS-3110 Series

10-port L2+ Managed Gigabit Fiber Switch

Network Management

User's Manual

Version 0.90

Revision History

Version	F/W	Date	Description
0.90	0.99.99	20171129	Fisrt release

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.

Table of Content

1. INTRODUCTION

Thank you for using the 8 100/1000Mbps SFP ports plus 2 10/100/1000Mbps combo uplink ports Managed Switch that is specifically designed for FTTx applications. The Managed Switch provides a built-in management module that enables users to configure and monitor the operational status both locally and remotely. This User's Manual will explain how to use command-line interface and Web Management to configure your Managed Switch. The readers of this manual should have knowledge about their network typologies and about basic networking concepts so as to make the best of this user's manual and maximize the Managed Switch's performance for your personalized networking environment.

1.1 Management Options

Switch management options available are listed below:

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

Local Console Management

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

Telnet Management

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

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.

SNMP Management

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

Web Management

Web Management is done over the network and can be accessed via a standard web browser, such as Microsoft Internet Explorer. Once the Managed switch is available on the network, you can login and monitor the status of it through a web browser remotely or locally. Local Console-type Web management, 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 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.

1.2 Management Software

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

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

Console Program

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

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

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

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

SNMP Management System

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

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

Web Browser Application

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

1.3 Management Preparations

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

Connecting the Managed Switch

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

1000Base-X / 100Base-FX SFP Port

The small form-factor pluggable (SFP) 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 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 slot for 3.3V mini GBIC module supports hot swappable SFP fiber transceiver. Before connecting the other switches, workstation or Media Converter, make sure both side of the SFP transfer are with the same media type, for example, 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX, and check the fiber-optic cable type matches the 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 RJ-45 Auto-MDI/MDIX Port

10/100/1000Base-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-5 UTP or STP cable may be used.

RS-232 RJ-45 Port

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

IP Addresses

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

IP addresses are made up of two parts:

- The first part (for example 192.168.n.n) refers to network address that identifies the network where the device resides. Network addresses are assigned by three allocation organizations. Depending on your location, each allocation organization assigns a globally unique network number to each network which intends to connect to the Internet.

- The second part (for example n.n.0.1) identifies the device within the network. Assigning unique device numbers is your responsibility. If you are unsure of the IP addresses allocated to you, consult with the allocation organization where your IP addresses were obtained.

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

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

MIB for Network Management Systems

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

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

2. Command Line Interface (CLI)

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

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

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

2.1 Using the Local Console

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

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

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

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

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

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

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

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

2.2 Remote Console Management - Telnet

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

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

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

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

Step 2. Run Telnet

Step 3. Log into the Switch CLI

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

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

2.3 Navigating CLI

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

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

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

2.3.1 General Commands

This section introduces you some general commands that you can use in User, Privileged, and Configuration modes, including “help”, “exit”, “history” and “logout”.

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

2.3.2 Quick Keys

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

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

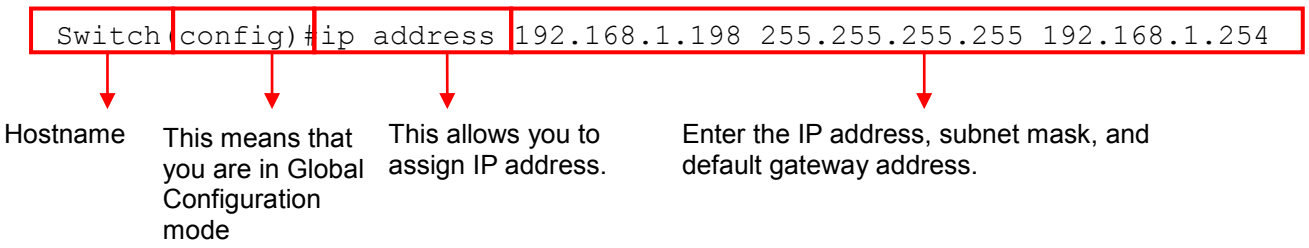
Unfinished command followed by ?	Enter an unfinished command or keyword and press “?” key to complete the command and get command syntax help.
	
	Example: List all available commands starting with the characters that you enter.
	
	`Switch#h?`
	`help  Show available commands`
	`history  Show history commands`

A space followed by ?	Enter a command and then press Spacebar followed by a “?” key to view the next parameter.
Up arrow	Use Up arrow key to scroll through the previous entered commands, beginning with the most recent key-in commands.
Down arrow	Use Down arrow key to scroll through the previous entered commands, beginning with the commands that are entered first.

2.3.3 Command Format

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

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



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

Symbols	**Brief Description**
>	Currently, the device is in User mode.
#	Currently, the device is in Privileged mode.
(config)#	Currently, the device is in Global Configuration mode.
Syntax	**Brief Description**
[ ]	Reference parameter.
[-s size] [-r repeat] [-t timeout]	These three parameters are used in ping command and are optional, which means that you can ignore these three parameters if they are unnecessary when executing ping command.
[A.B.C.D]	Brackets represent that this is a required field. Enter an IP address or gateway address.
[255.X.X.X]	Brackets represent that this is a required field. Enter the subnet mask.
[port]	Enter one port number. See Section 2.6.27 for detailed explanations.
[port_list]	Enter a range of port numbers or several discontinuous port numbers. See Section 2.6.27 for detailed explanations.
[forced_true | forced_false | auto]	There are three options that you can choose. Specify one of them.
[1-8191]	Specify a value between 1 and 8191.

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

	Example 2: specifying three values (separated by commas)
	
	`Switch(config)#qos 802.1p-map 1,3 0`
	
	`Switch(config)#qos dscp-map 10,13,15 3`
	
	Example 3: specifying a range of values (separated by a hyphen)
	
	`Switch(config)#qos 802.1p-map 1-3 0`
	
	`Switch(config)#qos dscp-map 10-15 3`

2.3.4 Login Username & Password

Default Login

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

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

Privileged Mode Password

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

Forgot Your Login Username & Password

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

2.4 User Mode

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

Command	Description
exit	Quit the User mode or close the terminal connection.
help	Display a list of available commands in User mode.
history	Display the command history.
logout	Logout from the Managed Switch.
ping	Test whether a specified network device or host is reachable or not.
traceroute	Trace the route to HOST
enable	Enter the Privileged mode.

2.4.1 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 times that packets are sent and received.

Command	Parameter	Description
Switch> ping [A.B.C.D | A:B:C:D:E:F:G:H] [-s size (1-65500)bytes] [-t timeout (1-99)secs]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IP/IPv6 address that you would like to ping.
	[-s size (1-65500)bytes]	Enter the packet size that would be sent. The allowable packet size is from 1 to 65500 bytes. (optional)
	[-t timeout (1-99) secs]	Enter the timeout value when the specified IP address is not reachable. (optional)
Example		
Switch> ping 8.8.8.8 Switch> ping 8.8.8.8 –s 128 –t 10 Switch> ping 2001:4860:4860::8888 Switch> ping 2001:4860:4860::8888 –s 128 –t 10		

2.4.2 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 max hops value for the number of hops that packets are sent and received.

Command	Parameter	Description
Switch> traceroute [A.B.C.D | A:B:C:D:E:F:G:H] [-h (1-100)hops]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IP/IPv6 address that you would like to ping.
	[-h (1-100)hops]	Specify max hops between the local host and the remote host
Example		
Switch> traceroute 8.8.8.8 Switch> traceroute 8.8.8.8 –h 30 Switch> ping 2001:4860:4860::8888 Switch> ping 2001:4860:4860::8888 –h 30		

2.5 Privileged Mode

The only place where you can enter the Privileged mode is in User mode. When you successfully enter 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.
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.

2.5.1 Copy-cfg Command

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

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

Command	Parameter	Description
Switch# copy-cfg from ftp [A.B.C.D | A:B:C:D:E:F:G:H] [file name] [user_name] [password]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IP/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 IP/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 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]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IP 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

[password]	[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 IP address of your TFTP server.
	[file name]	Enter the configuration file name that you want to backup.
	[running | default | startup]	Specify backup config to be running, default or startup
Example		
Switch# copy-cfg to ftp 192.168.1.198 HS_0600_file.conf running misadmin1 abcxyz Switch# copy-cfg to tftp 192.168.1.198 HS_0600_file.conf startup		

3. Restore the Managed Switch back to default settings.

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

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

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

2.5.2 Firmware Command

To upgrade firmware via TFTP or FTP server.

Command	Parameter	Description
Switch# firmware upgrade ftp [A.B.C.D | A:B:C:D:E:F:G:H] [file_name] [Image-1| Image-2] [user_name] [password]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IP address of your FTP server.
	[file name]	Enter the firmware file name that you want to upgrade.
	[Image-1| Image-2]	Choose image-1 or image-2 for the firmware to be upgraded to.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
Switch# firmware upgrade tftp [A.B.C.D | A:B:C:D:E:F:G:H] [file_name] [Image-1| Image-2]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IP address of your TFTP 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.
Example		
Switch# firmware upgrade ftp 192.168.1.198 HS_0600_file.bin Image-1 edgeswitch10 abcxyz		
Switch# firmware upgrade tftp 192.168.1.198 HS_0600_file.bin Image-2		

2.5.3 Ping Command

Command	Parameter	Description
Switch> ping [A.B.C.D | A:B:C:D:E:F:G:H] [-s size (1-65500)bytes] [-t timeout (1-99)secs]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IP/IPv6 address that you would like to ping.
	[-s size (1-65500)bytes]	Enter the packet size that would be sent. The allowable packet size is from 1 to 65500 bytes. (optional)
	[-t timeout (1-99) secs]	Enter the timeout value when the specified IP address is not reachable. (optional)
Example		
Switch> ping 8.8.8.8 Switch> ping 8.8.8.8 –s 128 –t 10 Switch> ping 2001:4860:4860::8888 Switch> ping 2001:4860:4860::8888 –s 128 –t 10		

2.5.4 Reload Command

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

Command / Example
Switch# reload

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

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

2.5.5 Traceroute Command

Command	Parameter	Description
Switch> traceroute [A.B.C.D | A:B:C:D:E:F:G:H] [-h (1-100)hops]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IP/IPv6 address that you would like to ping.
	[-h (1-100)hops]	Specify max hops between the local host and the remote host
Example		
Switch> traceroute 8.8.8.8 Switch> traceroute 8.8.8.8 –h 30 Switch> ping 2001:4860:4860::8888 Switch> ping 2001:4860:4860::8888 –h 30		

2.5.6 Write Command

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

Command / Example
Switch# write Save Config Succeeded!

2.5.7 Configure Command

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

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

2.5.8 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.

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-setting 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 “show switch-info command” section.

2.6 Configuration Mode

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

Command	Description
acl	Set up access control entries and lists.
archive	Manage archive configuration files
channel-group	Configure static link aggregation groups or enable LACP function.
dot1x	IEEE 802.1X/MAB global configuration commands
digital	Global Digital Input configuration commands
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
lldp	LLDP global configuration mode
loop-detection	Configure loop-detection to prevent loop between switch ports by locking them.
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.
spanning-tree	Set up RSTP status of each port and aggregated ports.
switch	Set up acceptable frame size and address learning, etc.
switch-info	Edit the system information.
syslog	Set up required configurations for Syslog server.
terminal	Set up Terminal functions
user	Create a new user account.
vlan	Set up VLAN mode and VLAN configuration.
no	Disable a command or reset it back to its default setting.
interface	Select a single interface or a range of interfaces.
show	Show a list of commands or show the current setting of each listed command.

2.6.1 Entering Interface Numbers

In the Global Configuration mode, you can configure a command that only applies to interfaces specified. For example, you can set up each interface’s VLAN assignment, speeds, or duplex modes. To configure, you must first enter the interface number. There are four ways to enter your interface numbers to signify the combination of different interfaces that apply a command or commands.

Commands	Description
Switch(config)# interface 1 Switch(config-if-1)#	Enter a single interface. Only interface 1 will apply commands entered.
Switch(config)# interface 1,3,5 Switch(config-if-1,3,5)#	Enter three discontinuous interfaces, separated by commas. Interface 1, 3, 5 will apply commands entered.

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

2.6.2 No Command

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

2.6.3 Show Command

The “show” command is very important for network administrators to get information about the device, receive outputs to verify a command’s configurations or troubleshoot a network configuration error. It can be used in Privileged or Configuration mode. The following describes different uses of “show” command.

1. Display system information

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

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

System Object ID: Display the predefined System OID.

System Contact: Display the contact information for this Managed Switch. Use “switch-info system-contact [sys_contact]” command to edit this field.

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

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

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

Model Name: Display the product’s model name.

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

Current Boot Image: The image that is currently using.

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

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

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

M/B Version: Display the main board version.

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

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

Up Time: Display the up time since last restarting.

Local Time: Display the local time of the system

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-setting 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 “show switch-info command” section

2.6.4 ACL Command

Command	Parameter	Description
Switch(config)# acl [1-192]	[1-192]	The total number of ACL rule can be created is 192. 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-RULE)# action [deny | copy(mirror) | permit | redirect]	[deny | copy(mirror) | permit | redirect]	Specify action to the ACL-matched packet.
Switch(config-acl-RULE)# action-port [port]	[port]	Specify copy(mirror)-to/redirect-to port (1~10).
Switch(config-acl-RULE)# apply		To have the specified rule taken effect.
Switch(config-acl-RULE)# destination-ipv4 any		Specify destination IPv4 address as “ANY”.
Switch(config-acl-RULE)# destination-ipv4 address [A.B.C.D] [255.X.X.X]	[A.B.C.D]	Specify destination IPv4 address.
	[255.X.X.X]	Specify destination IPv4 mask.
Switch(config-acl-RULE)# destination-ipv6 any		Specify destination IPv6 address as “ANY”.
Switch(config-acl-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-RULE)# destination-l4-port any		Specify destination Layer4 port as “ANY”.
Switch(config-acl-RULE)# destination-l4-port [1-65535] [0xWXYZ]	[1-65535]	Specify destination Layer4 port.
	[0xWXYZ]	Specify destination Layer4 mask. (Range:0x0000~FFFF)
Switch(config-acl-RULE)# destination-mac any		Specify destination MAC as “ANY”.
Switch(config-acl-RULE)# destination-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-RULE)# ethertype [any | 0xWXYZ]	[any | 0xWXYZ]	Specify Ethertype (Range: 0x0000 ~FFFF) or “ANY”.
Switch(config-acl-RULE)# ingress-port [any | port-list]	[any | port-list]	Specify ingress port(s) or “ANY”.
Switch(config-acl-RULE)# protocol [any | 0xWX]	[any | 0xWX]	Specify IPv4 protocol and IPv6 next header (Range: 0x00~FF) or “ANY”.
Switch(config-acl-RULE)# rate-limit [0,16-1048560]	[16-1048560]	Specify rate limitation from 16 to 1048560 kbps (0:Disable)

Switch(config-acl-RULE)# source-ipv4 any		Specify source IPv4 address as “ANY”.
Switch(config-acl-RULE)# source-ipv4 address [A.B.C.D] [255.X.X.X]	[A.B.C.D]	Specify source IPv4 address.
	[255.X.X.X]	Specify source IPv4 mask.
Switch(config-acl-RULE)# source-ipv6 any		Specify source IPv6 address as “ANY”.
Switch(config-acl-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-RULE)# source-l4-port any		Specify source Layer4 port as “ANY”.
Switch(config-acl-RULE)# source-l4-port [1-65535] [0xWXYZ]	[1-65535]	Specify source Layer4 port.
	[0xWXYZ]	Specify source Layer4 mask. (Range:0x0000~FFFF)
Switch(config-acl-RULE)# source-mac any		Specify source MAC as “ANY”.
Switch(config-acl-RULE)# source-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-RULE)# tos [any | 0xWX]	[any | 0xWX]	Specify IPv4 TOS and IPv6 traffic class (Range: 0x00~FF) or “ANY”.
Switch(config-acl-RULE)# vid [any | 1-4094]	[any | 1-4094]	Specify 802.1q VLAN ID (Range: 1~4094) or “ANY”.
No command		
Switch(config)# no acl [1-192]	[1-192]	Remove the specified ACL rule.
Switch(config-acl-RULE)# no action		Reset action back to the default (permit).
Switch(config-acl-RULE)# no action-port		Reset copy(mirror)-to/redirect-to the default port (Port 1).
Switch(config-acl-RULE)# no destination-ipv4		Reset destination IPv4 address back to the default (ANY).
Switch(config-acl-RULE)# no destination-ipv6		Reset destination IPv6 address back to the default (ANY).
Switch(config-acl-RULE)# no destination-l4-port		Reset destination Layer4 port back to the default (ANY).
Switch(config-acl-RULE)# no destination-mac		Reset destination MAC back to the default (ANY).
Switch(config-acl-RULE)# no ingress-port		Reset ingress port(s) back to the default (ANY).
Switch(config-acl-RULE)# no ethertype		Reset Ethertype back to the default (ANY).

Switch(config-acl-RULE)# no protocol		Reset IPv4 protocol and IPv6 next header back to the default “ANY”.
Switch(config-acl-RULE)# no rate-limit		Disable rate limitation.
Switch(config-acl-RULE)# no source-ipv4		Reset source IPv4 address back to the default (ANY).
Switch(config-acl-RULE)# no source-ipv6		Reset source IPv6 address back to the default (ANY).
Switch(config-acl-RULE)# no source-l4-port		Reset source Layer4 port back to the default (ANY).
Switch(config-acl-RULE)# no source-mac		Reset source MAC back to the default (ANY).
Switch(config-acl-RULE)# no tos		Reset IPv4 TOS and IPv6 traffic class back to the default (ANY).
Switch(config-acl-RULE)# no vid		Reset 802.1q VLAN ID back to the default (ANY).
Show command		**Description**
Switch(config)# show acl		Display the valid ACL(s).
Switch(config)# show acl [1-192]	[1-192]	Display the specified ACL rule configuration.
Switch(config-acl-RULE)# show		Display the specified ACL rule configuration.

2.6.5 Archive Command

Command	Parameter	Description
Switch(config)# archive auto-backup		Enable the auto-backup configuration files function.
Switch(config)# archive auto-backup path ftp [A.B.C.D | 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 IP/ IPv6 address of the FTP server.
	[file_directory]	Specify the file directory of the FTP server to save the start-up configuration files.
	[user_name]	Specify the user name to login the FTP server.
	[password]	Specify the password for FTP server's authentication.
Switch(config)# archive auto-backup path tftp [A.B.C.D | A:B:C:D:E:F:G:H] [file_directory]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the IP/ IPv6 address of the TFTP server.
	[file_directory]	Specify the file directory of the TFTP server to save the start-up configuration files.
Switch(config)# archive auto-backup time [0-23]	[0-23]	Specify the time to begin the automatic backup of the start-up configuration files everyday.
No command		
Switch(config)# no archive auto-backup		Disable the auto-backup function.
Switch(config)# no archive auto-backup path		Remove TFTP / FTP server settings.
Switch(config)# no archive auto-backup time		Reset the Auto-backup time back to the default (0 o'clock).
Show command		**Description**
Switch# show archive auto-backup		Display the auto-backup configuration.
Switch(config)# show archive auto-backup		Display the auto-backup configuration.

2.6.6 Channel-group Command

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

Command	Parameter	Description
Switch(config)# channel-group trunking [group_name]	[group_name]	Specify a name for this link aggregation group.
Switch(config)# interface [port_list] Switch(config-if-PORT-PORT)# channel-group trunking [group_name]	[port_list] [group_name]	Use “interface” command to configure a group of ports’ link aggregation link membership. Assign the selected ports to the specified link aggregation group.
Switch(config)# channel-group distribution-rule destination-ip		Load-balancing depending on destination IP address.
Switch(config)# channel-group distribution-rule source-ip		Load-balancing depending on source IP address.
Switch(config)# channel-group distribution-rule destination-L4-port		Load-balancing depending on destination L4 port.
Switch(config)# channel-group distribution-rule source-L4-port		Load-balancing depending on source L4 port.
Switch(config)# channel-group distribution-rule destination-mac		Load-balancing depending on destination MAC address.
Switch(config)# channel-group distribution-rule source-mac		Load-balancing depending on source MAC address.
No command		
Switch(config)# no channel-group trunking [group_name]	[group_name]	Delete a link aggregation group.
Switch(config)# interface [port_list] Switch(config-if-PORT-PORT)# no channel-group trunking	[port_list]	Remove the selected ports from a link aggregation group.
Switch(config)# no channel-group distribution-rule destination-ip		Disable load-balancing based on destination IP address.
Switch(config)# no channel-group distribution-rule source-ip		Disable load-balancing based on source IP address.
Switch(config)# no channel-group distribution-rule destination-L4-port		Disable load-balancing based on destination L4 port.
Switch(config)# no channel-group distribution-rule source-L4-port		Disable load-balancing based on source L4 port.
Switch(config)# no channel-group type destination-mac		Disable load-balancing based on destination MAC address.
Switch(config)# no channel-group type source-mac		Disable load-balancing based on destination MAC address.

Show command		
Switch(config)# show channel-group trunking		Show or verify link aggregation settings.
Switch(config)# show channel-group trunking [group_name]	[group_name]	Show or verify a specific link aggregation group's settings including aggregated port numbers and load-balancing status.

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

	Command	Purpose
STEP1	configure **Example:** FOS-3110# config FOS-3110(config)#	**Enter the global configuration mode.**
STEP2 *(Optional)*	channel-group distribution-rule source-ip **Example:** FOS-3110(config)# channel-group distribution-rule source-ip OK !	**Enable Source IP Address in Distribution Rule.**
STEP3 *(Optional)*	channel-group distribution-rule destination-ip **Example:** FOS-3110(config)# channel-group distribution-rule destination-ip OK !	**Enable Destination IP Address in Distribution Rule.**
STEP4 *(Optional)*	channel-group distribution-rule source-L4-port **Example:** FOS-3110(config)# channel-group distribution-rule source-L4-port OK !	**Enable Source L4 Port in Distribution Rule.**
STEP5 *(Optional)*	channel-group distribution-rule destination-L4-port **Example:** FOS-3110(config)# channel-group distribution-rule destination-L4-port OK !	**Enable Destination L4 Port in Distribution Rule.**
STEP6 *(Optional)*	channel-group distribution-rule source-mac **Example:** FOS-3110(config)# channel-group distribution-rule source-mac OK !	**Enable Source Mac Address in Distribution Rule.**
STEP7 *(Optional)*	channel-group distribution-rule destination-mac **Example:** **FOS-3110(config)# channel-group distribution-rule destination-mac** **OK !**	**Enable Destination Mac Address in Distribution Rule.**
STEP8	channel-group trunking *group_name* **Example:** FOS-3110(config)# channel-group trunking CTSGROUP OK !	**In this example, it configures the name of the Trunking Group as "CTSGROUP".**

STEP9	interface *port_list* **Example:** FOS-3110(config)# interface 1,3 FOS-3110(config-if-1,3)#	**Speciy the interface that you would like to set to Trunking Group.**
STEP10	channel–group trunking *group_name* **Example:** FOS-3110(config-if-1,3)# channel-group trunking CTSGROUP OK !	**In this example, it configures Port 1 and Port 3 as the link membership of "CTSGROUP"Trunking Group**
STEP11	exit **Example:** FOS-3110(config-if-1,3)# exit FOS-3110(config)#	**Return to the global configuration mode.**
STEP12	exit **Example:** FOS-3110(config)# exit FOS-3110#	**Return to the Privileged mode.**
STEP13	write **Example:** FOS-3110# write Save Config Succeeded! OK !	**Save the running configuration into the startup configuration.**

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

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

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

	Command	Purpose
STEP1	configure **Example:** FOS-3110# config FOS-3110(config)#	**Enter the global configuration mode.**
STEP2 *(Optional)*	channel–group distribution–rule source–ip **Example:** FOS-3110(config)# channel-group distribution-rule source-ip OK !	**Enable Source IP Address in Distribution Rule.**
STEP3 *(Optional)*	channel–group distribution–rule destination–ip **Example:** FOS-3110(config)# channel-group distribution-rule destination-ip OK !	**Enable Destination IP Address in Distribution Rule.**
STEP4 *(Optional)*	channel–group distribution–rule source–L4–port **Example:** FOS-3110(config)# channel-group distribution-rule source-L4-port OK !	**Enable Source L4 Port in Distribution Rule.**
STEP5 *(Optional)*	channel–group distribution–rule destination–L4–port **Example:** FOS-3110(config)# channel-group distribution-rule destination-L4-port OK !	**Enable Destination L4 Port in Distribution Rule.**
STEP6 *(Optional)*	channel–group distribution–rule source–mac **Example:** FOS-3110(config)# channel-group distribution-rule source-mac OK !	**Enable Source Mac Address in Distribution Rule.**
STEP7 *(Optional)*	channel–group distribution–rule destination–mac **Example:** **FOS-3110(config)# channel-group distribution-rule destination-mac** **OK !**	**Enable Destination Mac Address in Distribution Rule.**
STEP8	interface *port_list* **Example:** FOS-3110(config)# interface 5-7 FOS-3110(config-if-5-7)#	**Speciy the interfaces that you would like to set to LACP Group.**
STEP9	channel–group lacp **Example:** FOS-3110(config-if-5-7)# channel-group lacp OK !	**Enable Port 5~Port 7 to LACP Port.**

STEP10	channel–group lacp role active [no channel–group lacp role] **Example 1:** FOS-3110(config-if-5-7)# channel-group lacp role active OK ! **Example 2:** FOS-3110(config-if-5-7)# no channel-group lacp role OK !	**In the Example 1, it configures LACP Port 5~7 as "Active" in LACP Role.** **In the Example 2, it configures LACP Port 5~7 as "Passive" in LACP Role.** **.**
STEP11	channel–group lacp key *LACP_key* [no channel–group lacp key] **Example 1:** FOS-3110(config-if-5-7)# channel-group lacp key 10 OK ! **Example 2:** FOS-3110(config-if-5-7)# no channel-group lacp key OK !	**In the Example 1, it configures a key value "10" as the LACP Key of LACP Port 5~7.** **In the Example 2, it configures a key value "0" (default value) as the LACP Key of LACP Port 5~7.**
STEP12	exit **Example:** FOS-3110(config-if-5-7)# exit FOS-3110(config)#	**Return to the global configuration mode.**
STEP13	exit **Example:** FOS-3110(config)# exit FOS-3110#	**Return to the Privileged mode.**
STEP14	write **Example:** FOS-3110# write Save Config Succeeded!	**Save the running configuration into the startup configuration.**

2.6.7 Dot1x Command

Command	Parameter	Description
Switch(config)# dot1x		Enable IEEE 802.1X/MAB function. When enabled, the Managed Switch acts as a proxy between the 802.1X-enabled client and the authentication server. In other words, the Managed Switch requests identifying information from the client, verifies that information with the authentication server, and relays the response to the client.
Switch(config)# dot1x radius-assigned vlan		Enable radius-assigned vlan of the system.
Switch(config)# dot1x reauthentication		Enable auto re-authentication function of the system.
Switch(config)# dot1x secret [shared_secret]	[shared_secret]	Specify a shared secret of up to 30 characters. This is the identification word or number assigned to each RADIUS authentication server with which the client shares a secret.
Switch(config)# dot1x server [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the RADIUS authentication server IP/ IPv6 address.
No command		
Switch(config)# no dot1x		Disable IEEE 802.1X/MAB function.
Switch(config)# no dot1x radius-assigned vlan		Disable radius-assigned vlan of the system.
Switch(config)# no dot1x reauthentication		Disable auto re-authentication function of the system.
Switch(config)# no dot1x secret		Remove the configured shared secret.
Switch(config)# no dot1x server		Remove the configured RADIUS authentication server IP/IPv6 address.
Show command		
Switch(config)# show dot1x		Show 802.1X/MAB system configuration
Switch(config)# show dot1x interface		Show each interface's 802.1X/MAB configuration.
Switch(config)# show dot1x interface [port_list]	[port_list]	Show the selected interfaces' 802.1X/MAB configuration.
Switch(config)# show dot1x statistics		Show each port's 802.1X/MAB statistics.
Switch(config)# show dot1x statistics [port_list]	[port_list]	Show the selected interfaces' 802.1X/MAB statistics.
Switch(config)# show dot1x status		Show all ports' 802.1X/MAB status.
Switch(config)# show dot1x status [port_list]	[port_list]	Show the selected interfaces' 802.1X/MAB status.

Examples of Dot1x command	
Switch(config)# dot1x	Enable IEEE 802.1X/MAB function.
Switch(config)# dot1x reauthentication	Enable auto re-authentication function of the system.
Switch(config)# dot1x secret agagabcxyz	Set up the shared secret to “agagabcxyz”
Switch(config)# dot1x server 192.168.1.10	Set up the RADIUS authentication server IP address to 192.168.1.10.

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

Dot1x & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4.
Switch(config-if-PORT-PORT)# dot1x mab		Enable MAB authentication bypass.
Switch(config-if-PORT-PORT)# dot1x max-req [1-10]	[1-10]	Configure EAP-request/identity retry times from switch to client before restarting the authentication process.
Switch(config-if-PORT-PORT)# dot1x port-control [auto | authorized | unauthorized]		Specify the 802.1X/MAB port type “auto”, “authorized” or “unauthorized” to the selected ports. **“auto”:** This requires 802.1X-aware clients to be authorized by the authentication server. Accesses from clients that are not dot1x aware will be denied. **“authorized”:** This forces the Managed Switch to grant access to all clients, both 802.1X-aware and 802.1x-unaware. No authentication exchange is required. By default, all ports are set to “authorized”. **“unauthorized”:** This forces the Managed Switch to deny access to all clients, neither 802.1X-aware nor 802.1X-unaware.
Switch(config-if-PORT-PORT)# dot1x radius-assigned vlan		Enable radius-assigned vlan of the specified port.
Switch(config-if-PORT-PORT)# dot1x reauthenticate		Re-authenticate the selected interfaces right now.
Switch(config-if-PORT-PORT)# dot1x reauthentication		Enable the selected ports’ auto re-authentication function.
Switch(config-if-PORT-PORT)# dot1x timeout eap-timeout [1-255]	[1-255]	Specify EAP authentication timeout value in seconds. The Managed Switch will wait for a period of time for the response from the authentication server to an authentication request before it times out. The allowable

		value is between 1 and 255 seconds.
Switch(config-if-PORT-PORT)# dot1x timeout reauth-period [1-65535]	[1-65535]	Specify a period of authentication time that a client authenticates with the authentication server. The allowable value is between 1 and 65535 seconds.
No command		
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1, 3 or 2-4.
Switch(config-if-PORT-PORT)# no dot1x mab		Disable MAB authentication bypass.
Switch(config-if-PORT-PORT)# no dot1x max-req		Reset EAP-request/identity retry times back to the default. (2 times)
Switch(config-if-PORT-PORT)# no dot1x port-control		Reset the selected interfaces' 802.1X/MAB port type to the default (authorized state).
Switch(config-if-PORT-PORT)# no dot1x radius-assigned vlan		Disable radius-assigned vlan of the specified port.
Switch(config-if-PORT-PORT)# no dot1x reauthentication		Disable the selected ports' auto re-authentication function.
Switch(config-if-PORT-PORT)# no dot1x timeout reauth-period		Reset EAP re-authentication period back to the default. (3600 seconds).
Switch(config)# no dot1x timeout eap-timeout		Reset EAP authentication timeout value back to the default. (30 seconds).
Show command		
Switch(config)# show dot1x		Show 802.1X/MAB system configuration.
Switch(config)# show dot1x interface		Show each interface's 802.1x settings including port status and authentication status.
Switch(config)# show dot1x interface [port_list]	[port_list]	Show the selected interfaces' 802.1x settings including port status and authentication status.
Switch(config)# show dot1x statistics		Show 802.1x statistics.
Switch(config)# show dot1x statistics [port_list]	[port_list]	Show the selected interfaces' statistics.
Switch(config)# show dot1x status		Show 802.1x status.
Switch(config)# show dot1x status [port_list]	[port_list]	Show the selected interfaces' 802.1x status.
Examples of Dot1x & interface command		
Switch(config)# interface 1-3		Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-1-3)# dot1x port-control auto		Set the selected ports to "auto" state.
Switch(config-if-1-3)# dot1x reauthenticate		Re-authenticate the selected interfaces immediately.

2.6.8 Digital Input Command

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

2.6.9 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 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 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 DHCP relay function.

IP DHCP Snooping Command	Parameter	Description
Switch(config)# ip dhcp snooping		Enable DHCP/DHCPv6 snooping function.
Switch(config)# ip dhcp snooping dhcp-server [port_list]	[port_list]	Specify DHCP/DHCPv6 server trust port.
Switch(config)# ip dhcp snooping dhcp-server-ip		Globally enable DHCP/DHCPv6 server trust IP/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 DHCP/DHCPv6 server trust IP/IPv6 address number.
	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify DHCP/ DHCPv6 server trust IP/ IPv6 address.
Switch(config)# ip dhcp snooping initiated [0-9999]	[0-9999]	Specify the DHCP/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 DHCP/DHCPv6 snooping Leased Time when packets' expired. (Range:180~259200 Seconds).
Switch(config)# ip dhcp snooping option		Enable DHCP Option 82 / DHCPv6 Option 37 relay agent.

Switch(config)# ip dhcp snooping remote		Enable DHCP Option 82 / DHCPv6 Option 37 Manual Remote Id.
Switch(config)# ip dhcp snooping remote formatted		Enable the Formatted Option 82 / DHCPv6 Option 37 Remote Id.
Switch(config)# ip dhcp snooping remote id [remote_id]	[remote_id]	You can configure the DHCP Option 82 / DHCPv6 Option 37 remote ID to be a string of up to 63 chaaracters. The default remote ID is the switch MAC address.
No command		
Switch(config)# no ip dhcp snooping		Disable DHCP/DHCPv6 snooping function.
Switch(config)# no ip dhcp snooping dhcp-server		Remove DHCP/DHCPv6 server trust ports.
Switch(config)# no ip dhcp snooping dhcp-server-ip		Globally disable DHCP/DHCPv6 server trust IP/IPv6 address.
Switch(config)# no ip dhcp snooping dhcp-server-ip [1-4] ip-address		Remove DHCP/DHCPv6 server trust IP/IPv6 address from the specified trust IP/IPv6 address number.
Switch(config)# no ip dhcp snooping initiated		Reset the initiated time value back to the default setting. (4 seconds)
Switch(config)# no ip dhcp snooping leased		Reset the leased time value back to the default setting.(86400 seconds)
Switch(config)# no ip dhcp snooping option		Disable DHCP Option 82 / DHCPv6 Option 37 relay agent.
Switch(config)# no ip dhcp snooping remote		Disable DHCP Option 82 / DHCPv6 Option 37 Manual Remote Id.
Switch(config)# no ip dhcp snooping remote id		Clear Remote ID description.
Switch(config)# no ip dhcp snooping formatted		Disable the Formatted Option 82 / DHCPv6 Option 37 Remote Id.
Show command		
Switch(config)# show ip dhcp snooping		Show DHCP/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 ports' 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 current		Show DHCP snooping opt82 Remote ID.
Switch(config)# show ip dhcp snooping status		Show DHCP/DHCPv6 snooping status.

Examples of IP DHCP Snooping	
Switch(config)# ip dhcp snooping	Enable DHCP snooping function.
Switch(config)# ip dhcp snooping dhcp-server [port_list]	Configure DHCP server ports.
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 "123"

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

DHCP & 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' DHCP Option 82 / DHCPv6 Option 37 Manual Circuit Id.
Switch(config-if-PORT-PORT)# ip dhcp snooping circuit formatted		Enable Formatted 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. 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' DHCP Option 82 / DHCPv6 Option 37 relay agent.
Switch(config-if-PORT-PORT)# ip dhcp snooping trust		Enable the selected interfaces as DHCP Option 82 / DHCPv6 Option 37 trust ports.
Switch(config-if-PORT-PORT)# ip dhcp snooping server-trust		Enable the selected interfaces as DHCP/DHCPv6 server trust ports. **Note : A port / ports can not be configured as option 82 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' DHCP Option 82 / DHCPv6 Option 37 Manual Circuit Id.
Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit formatted		Disable Formatted Option 82 / DHCPv6 Option 37 Circuit Id for the selected interfaces.

Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit id		Clear DHCP Option 82 / DHCPv6 Option 37 Circuit Id.
Switch(config-if-PORT-PORT)# no ip dhcp snooping option		Disable the selected interfaces' DHCP Option 82 / DHCPv6 Option 37 relay agent.
Switch(config-if-PORT-PORT)# no ip dhcp snooping trust		Reset the selected interfaces back to non-DHCP 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-DHCP/DHCPv6 server trust ports.
Show command		
Switch(config)# show ip dhcp snooping		Show each port's DHCP Snooping Option 82 and trust port settings.
Switch(config)# show ip dhcp snooping interface [port_list]		Show the specified ports' DHCP Snooping trust port settings.
Examples of DHCP & 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		Set up the selected interfaces to DHCP Option 82 / DHCPv6 Option 37 relay agent.
Switch(config-if-1-3)# ip dhcp snooping trust		Set up the selected interfaces to DHCP Option 82 / DHCPv6 Option 37 trust ports.

4. Enable or disable IGMP/MLD snooping globally.

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

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

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

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

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

Command / Example	Parameter	Description
Switch(config)# ip igmp snooping		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. Set forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic will flood when enabled. However, the traffic will forward to router-ports only when disabled.
Switch(config)# ip igmp snooping immediate-leave		Enable immediate leave function.
Switch(config)# ip igmp snooping max-response-time [1-255] (1/10secs)	[1-255] (1/10secs)	Specify the 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 mcast-router [port_list]	[port_list]	Specify multicast router ports.
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 the flooding function. Traffic will forward to router-ports only when disabled.
Switch(config)# no ip igmp snooping immediate-leave		Disable immediate leave function.
Switch(config)# no ip igmp snooping max-response-time		Reset maximum response time back to the default. (125 seconds)
Switch(config)# no ip igmp snooping mcast-router [port_list]	[port_list]	Remove the selected ports from the router port list.
Switch(config)# no ip igmp snooping query-interval		Reset Query interval value back to the default. (100 seconds)
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.

5. 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-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 [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.

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

IGMP & Interface Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# ip igmp filter		Enable IGMP filter 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 max-groups [1-512]	[1-512]	Specify the maximum groups number of multicast streams to the selected ports.
Switch(config-if-PORT-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.
	[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 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-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 this static multicast IP
	[1-4094]	Specify a VLAN ID.
	[1-4094]	Remvoe the specified VLAN ID.
Show command		
Switch(config)# show ip igmp filter interface [port_list]	[port_list]	Show the specified ports' IGMP filtering configuration.
Switch(config)# show ip igmp static-multicast-ip		Show the static multicast IP table.
Switch(config)#show ip igmp snooping groups		Show IGMP snooping groups table.
Examples of IGMP & Interface		
Switch(config)# interface1-3		Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-1-3)# ip igmp filter		Enable IGMP Filter on port 1 to port 3.
Switch(config-if-1-3)# ip igmp filter profile Silverprofile		Assign the selected ports to the specified profile "Silverprofile".
Switch(config-if-1-3)# ip igmp max-groups 400		Set the maximum number of multicast streams to 400.
Switch(config-if-1-3)# ip igmp static-multicast-ip 224.10.0.5 vlan 50		Create a static multicast IP to VLAN entry.

7. Set Up IP Source Binding Function

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

2.6.10 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 in the auto mode.
Switch(config)# ipv6 address dhcp force		Configure DHCPv6 function in the forced mode.
Switch(config)# ipv6 address dhcp rapid-commit		Allow the two-message exchange for address assignment.
"ipv6 address dhcp" commands are functional only when autoconfiguration is enabled.		
Switch(config)# ipv6 address global [A:B:C:D:E:F:G:H/10~128]	[A:B:C:D:E:F:G:H/10~128]	Specify switch IPv6 global address and prefix-length.
[A:B:C:D:E:F:G:H]	[A:B:C:D:E:F:G:H]	Specify switch IPv6 default gateway IP address.
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 switch IPv6 link-local address and prefix-length.
Switch(config)# ipv6 enable		Enable IPv6 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 processing.
Show command		
Switch(config)# show ipv6 address		Display IPv6 configuraiton and the current IPv6 status of the Managed Switch.
Examples of IPv6 command		
Switch(config)# ipv6 address autoconfig		Enable Ipv6 autoconfiguration.
Switch(config)# ipv6 address dhcp auto		Enable DHCPv6 auto mode.

2.6.11 LLDP Command

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

LLDP command	Parameter	Description
Switch(config)# lldp hold-time [1-3600]	[1-3600]	Specify the amount of time in seconds. A receiving device will keep the information sent by your device for a period of time you specify here before discarding it. The allowable hold-time value is between 1 and 3600 seconds.
Switch(config)# lldp interval [1-180]	[1-180]	Specify the time interval for updated LLDP packets to be sent. The allowable interval value is between 1 and 180 seconds.
Switch(config)# lldp packets [1-16]	[1-16]	Specify the amount of packets that are sent in each discover. The allowable packet value is between 1 and 16 packets.
Switch(config)# lldp tlv-select capability		Enable Capability attribute to be sent.
Switch(config)# lldp tlv-select management-address		Enable Management Address attribute to be sent.
Switch(config)# lldp tlv-select port-description		Enable Port Description attribute to be sent.
Switch(config)# lldp tlv-select system-description		Enable System Description attribute to be sent.
Switch(config)# lldp tlv-select system-name		Enable System Name attribute to be sent.
No command		
Switch(config)# no lldp hold-time		Reset the hold-time value back to the default. (120 seconds)
Switch(config)# no lldp interval		Reset the time interval value of sending updated LLDP packets back to the default.(5 seconds)
Switch(config)# no lldp packets		Reset the amount of packets that are sent in each discover back to the default.(1 packet)
Switch(config)# no lldp tlv-select capability		Disable Capability attribute to be sent.
Switch(config)# no lldp tlv-select management-address		Disable Management Address attribute to be sent.
Switch(config)# no lldp tlv-select port-description		Disable Port Description attribute to be sent.
Switch(config)# no lldp tlv-select system-description		Disable System Description attribute to be sent.
Switch(config)# no lldp tlv-select system-name		Disable System Name attribute to be sent.

Show command	
Switch(config)# show lldp	Show LLDP settings.
Switch(config)# show lldp interface	Show each interface's LLDP configuraiton.
Switch(config)# show lldp interface [port_list]	Show the selected interfaces' LLDP configuration.
Switch(config)# show lldp status	Show the current LLDP status.
Examples of LLDP command	**Description**
Switch(config)# lldp hold-time 60	Set the hold-time value to 60 seconds.
Switch(config)# lldp interval 10	Set the updated LLDP packets to be sent in very 10 seconds.
Switch(config)# lldp packets 2	Set the number of packets to be sent in each discovery to 2.
Switch(config)# lldp tlv-select capability	Enable Capability attribute to be sent.
Switch(config)# lldp tlv-select management-address	Enable Management Address attribute to be sent.
Switch(config)# lldp tlv-select port-description	Enable Port Description attribute to be sent.
Switch(config)# lldp tlv-select system-description	Enable System Description to be sent.
Switch(config)# lldp tlv-select system-name	Enable System Name to be sent.

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

LLDP & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# lldp		Enable LLDP on the selected interfaces.
No command		
Switch(config-if-PORT-PORT)# no lldp		Disable LLDP on the selected interfaces.

2.6.12 Loop Detection Command

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

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

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

When the system does not 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 3 actions

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

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

Command	Parameter	Description
Switch(config)# loop-detection		Enable Loop Detection function.
Switch(config)# loop-detection all-vlan		Check All VLAN box to enable loop detection on all trunk-VLAN-vids configured in VLAN Command (See Section 2.6.26). ***NOTE:*** *When All VLAN checkbox is checked, it invalidates the configured "Specific VLAN".*
Switch(config)# loop-detection interval [1-180]	[0-180]	This is the time interval (in seconds) that the device will periodically send loop detection packets to detect the presence of looped network. The valid range is from 1 to 180 seconds. The default setting is 1 seconds.
Switch(config)# loop-detection unlock-interval [1-1440]	[1-1440]	This is the time interval for the system to detect the existence of loop condition. System un-blocks the looped port if it does not receive any loop-detection packet during the configured unlock-interval. The unlock-interval can be set from 1 to 1440 minutes. The default setting is 1440 minutes. ***NOTE:***

		1. Be aware that Looped port unlock-interval converted into seconds should be greater than or equal to Detection Interval seconds multiplied by 10. The '10' is a magic number which is for the system to claims the loop detection disappears when the system does not receive the loop-detection packet from itself at least 10 times. In general, it can be summarized by a formula below: ***60* "Looped port unlock-interval" ≧ 10* "Detection Interval"*** *2. When a port is detected as a looped port, the system keeps the looped port in blocking status until loop situation is gone. In other words, the system stops forwarding all the traffic via the looped port. However, the system will process the loop-detection packet received on the looped port.*
Switch(config)# loop-detection vlan-id [1-4094]	[1-4094]	Enable loop detection on specified VLAN. Up to 4 sets of VLAN ID can be assigned. ***NOTE:*** *The configured "Specific VLAN" takes effect when All VLAN check-box is unchecked.*
No command		
Switch(config)# no loop-detection		Disable Loop Detection function.
Switch(config)# no loop-detection all-vlan		Disable loop detection on all trunk-VLAN-vids.
Switch(config)# no loop-detection interval		Reset Loop Detection time interval to the default.
Switch(config)# no loop-detection unlock-interval		Reset Loop Detection unlock time interval to the default.
Switch(config)# no loop-detection vlan-id [1-4094]	[1-4094]	Disable loop detection on a specified VLAN.
Show command		
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 60		Set the Loop Detection time interval to 60 seconds.
Switch(config)# loop-detection unlock-interval 120		Set the Loop Detection unlock time interval to 120 minutes.
Switch(config)# loop-detection vlan-id 100		Enable the Loop Detection on VLAN ID 100.

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

Dot1x & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# loop-detection		Enable Loop Detection function on the specified ports.
No command		
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# no loop-detection		Disable Loop Detection function on the specified ports.

2.6.13 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 [0-172800s]	[0-172800s]	Enter the aging time for MAC addresses in seconds. 0= never aging out.
No command		
Switch(config)# no mac address-table aging-time		Reset MAC address table aging time to the default. (300 seconds).
Show command		
Switch(config)# show mac address-table		Show MAC addresses learned by the Managed Switch
Switch(config)# show mac address-table all		Show all of MAC table information
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]	[port_list]	Show MAC addresses learned by the specified port.
Switch(config)# show mac address-table mac [mac-addr]	[mac-addr]	Show the MAC status of specified MAC address.
Switch(config)# show mac address-table vlan [vlan_id]	[vlan_id]	Show the MAC status of specified VLAN ID.
Switch(config)# show mac learning		Show MAC learning setting of each interface.
Switch(config)# show mac static-mac		Show static MAC address table.
Switch(config)#show mac aging-time		Show 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-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 VLAN entry.
	[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 learning function.
No command		
Switch(config-if-PORT-PORT)# no mac address-table static-mac [xx:xx:xx:xx:xx:xx] vlan [1-4094]	[xx:xx:xx:xx:xx:xx]	Remove the specified MAC address from the MAC address table.
	[1-4094]	Remove the VLAN to which the specified MAC belongs.
Switch(config-if-PORT-PORT)# no mac learning		Disable MAC learning function of the specified ports.

2.6.14 Management Command

Command	Parameter	Description
Switch(config)# management console		Enable console interface.
Switch(config)# management console fail-retry [1-10]	[1-10]	Configure the retry times if the console login fails. The allowable value is 1~10 (times).
Switch(config)# management console block-time [1-120]	[1-120]	Configure the coslole block time of the Managed Switch if the console login retry times are more than the console fail-retry value you set up. The allowable value 1-120 (minutes).
Switch(config)# management console timeout [1-1440]	[1-1440]	To disconnect the Managed Switch when console management is inactive for a certain period of time. The allowable value is from 1 to 1440 (seconds).
Switch(config)# management console timeout [1-1440] min	[1-1440]	To disconnect the Managed Switch when console management is inactive for a certain period of time. The allowable value is from 1 to 1440 (minutes).
Switch(config)# management ssh		Enable SSH management. To manage the Managed Switch via SSH.
Switch(config)# management telnet		Enable Telnet Management. To manage the Managed Switch via Telnet.
Switch(config)# management telnet port [1-65535]	[1-65535]	When telnet is enabled, you can set up the port number that allows telnet access. The default port number is set to 23. However, you can also identify a port number between 1 and 65535.
Switch(config)# management web		Enable Web Management. To manage the Managed Switch via Web management.
Switch(config)# management web timeout [1-1440]	[1-1440]	To disconnect the Managed Switch when web management is inactive for a certain period of time. The allowable value is from 1 to 1440(minutes).
No command		
Switch(config)# no management console		Disable console interface.

Switch(config)# no management console fail-retry	Reset console fail-retry times back to the default (3 times).
Switch(config)# no management console block-time	Reset console block-time back to the default (20 minutes).
Switch(config)# no management console timeout	Reset console timeout back to the default (300 seconds).
Switch(config)# no management ssh	Disable SSH management.
Switch(config)# no management telnet	Disable Telnet management.
Switch(config)# no management telnet port	Reset Telnet port back to the default. The default port number is 23.
Switch(config)# no management web	Disable Web management.
Switch(config)# no management web timeout	Reset web timeout value back to the default (20 minutes).
Show command	
Switch(config)# show management	Show the current management configuration of the Managed Switch.
Examples of Management command	
Switch(config)# management console timeout 300	The console management will timeout (logout automatically) when it is inactive for 300 seconds.
Switch(config)# management telnet	Enable Telnet management.
Switch(config)# management telnet port 23	Set Telnet port to port 23.
Switch(config)# management web	Enable Web management.

2.6.15 Mirror Command

Command	Parameter	Description
Switch(config)# mirror destination [port]	[port]	Specify the preferred target port (1~10) for port mirroring.
Switch(config)# mirror source [port_list]	[port_list]	Specify a source port number or several source port numbers for port mirroring. ***NOTE:*** The port selected as the target port cannot be the source port.
No command		
Switch(config)# no mirror destination		Disable port mirroring function or disable mirroring target port.
Switch(config)# no mirror source		Disable mirroring source ports.
Show command		
Switch(config)# show mirror		Show the current port mirroring configuration.
Example of Mirror command		
Switch(config)# mirror destination 8		The selected source ports' data will mirror to port 8.
Switch(config)# mirror source 1-7		Port 1 to 7's data will mirror to the target port.

2.6.16 NTP Command

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 IP/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 IP/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 IP/IPv6 address.
Switch(config)# no ntp server2		Delete the primary time server IP/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(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 IP address to 192.180.0.12.
Switch(config)# ntp server2 192.180.0.13		Set the secondary NTP time server IP address to 192.180.0.13.
Switch(config)# ntp syn-interval 4		Set the synchronization interval to 4 hours.
Switch(config)# ntp time-zone 3		Set the time zone to GMT-8:00 Vancouver.

2.6.17 QoS Command

1. Set up Qos

QoS command	Parameter	Description
Switch(config)# qos [802.1p | dscp]	[802.1p | dscp]	Specify QoS mode.
Switch(config)# qos dscp-map [0-63] [0-7]	[0-63]	Specify a DSCP bit value.
	[0-7]	Specify a queue value.
Switch(config)# qos management-priority [0-7]	[0-7]	Specify management default 802.1p bit.
Switch(config)# qos queuing-mode [weight]	[weight]	Specify QoS queuing mode as weight mode.
Switch(config)# qos queue-weighted [1:2:4:8:16:32:64:127]	[1:2:4:8:16:32:64 :127]	Specify the queue weighted.
Switch(config)# qos remarking dscp		Globally enable DSCP bit remarking.
Switch(config)# qos remarking dscp-map [1-8]	[1-8]	Specify the DSCP and priority mapping ID.
Switch(config)# qos remarking 802.1p		Globally enable 802.1p bit remarking.
Switch(config)# qos remarking 802.1p-map [1-8]	[1-8]	Specify the 802.1p and priority mapping ID.
Switch(config)# qos 802.1p-map	[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.
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 bit 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)# 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)# no qos 802.1p-map [0-7]	[0-7]	Reset the specified 802.1p bit value back to the default queue value Q(0).

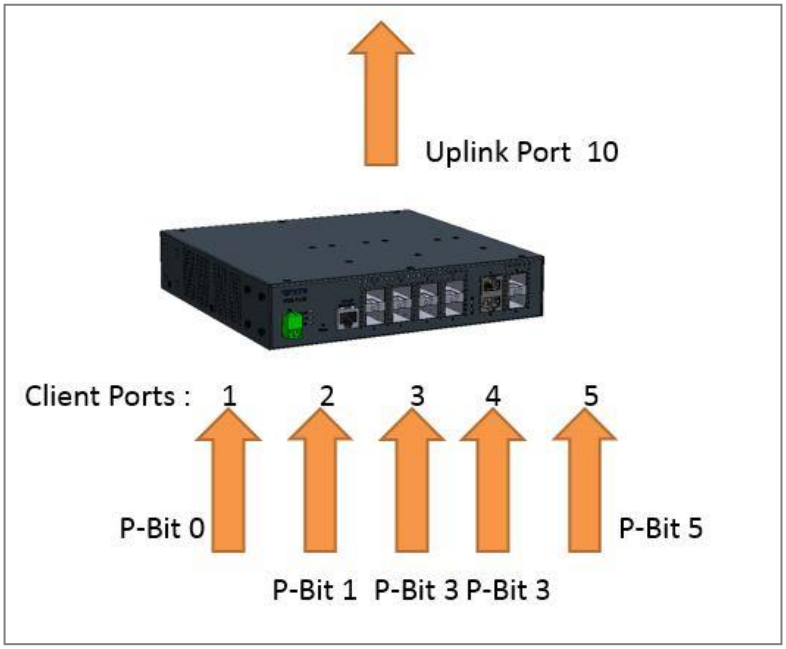
Show command		
Switch(config)# show qos		Show QoS configuration.
Switch(config)# show qos interface		Show QoS interface overall information.
Switch(config)# show qos interface [port-list]	[port-list]	Show the selected QoS interface information.
Switch(config)# show qos remarking		Show QoS remarking information.

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

For QoS configuration via CLI, we take a FOS-3110 Managed Switch for example to let the users have a clear understanding of these QoS commands.

Under this network environment, FOS-3110 will be configured as Table 2-1. Port 1-5 are client ports and Port 10 is the uplink port of the device. Client ports will receive the data traffic with different VLAN P-bit value. Port 3, Port 4 and Port 5 are also limited to specified bandwidth in the different rate limit in ingress and egress.



QoS Mode: 802.1p; Egress Mode: Weight; Port 10: Uplink Port. Queue-Weighted: 1(Q0):2(Q1):3(Q2):4(Q3):5(Q4):6(Q5):7(Q6):8(Q7)					
802.1p Priority Map	**P-Bit**	**Queue Mapping**	**Ingress Rate**	**Egress Rate**	**Remark**
Port 1	0	Q0	Default	Default	The rest of P-Bits are default value.
Port 2	1	Q1	Default	Default	
Port 3	3	Q2	10000	10000	
Port 4	3	Q2	10000	10000	
Port 5	5	Q3	1G	1G	

Table 2-1

Below is the complete CLI commands applied to FOS-3110 Managed Switch.

	Command	**Purpose**
STEP1	configure **Example:** FOS-3110# config FOS-3110(config)#	**Enter the global configuration mode.**
STEP2	qos 802.1p **Example:** FOS-3110(config)# qos 802.1p OK !	**In this example, it configures the QoS Mode to 802.1p.**

STEP3	qos queuing-mode weight **Example:** FOS-3110(config)# qos queuing-mode weight **OK !**	**In this example, it configures Configure Egress Mode as "Weight".**
STEP4	qos queue-weighted *weighted* **Example:** FOS-3110(config)# qos queue-weighted 1:2:3:4:5:6:7:8 OK !	**In this example, it configures the Queue Weighted to : 2(Q0):4(Q1):6(Q2):8(Q3): 10(Q4):12(Q5):14(Q6):16(Q7)..**
STEP5	qos 802.1p-map *802.1p_list queue_value* **Example:** FOS-3148(config)# qos 802.1p-map 0 0 FOS-3148(config)# qos 802.1p-map 1 1 FOS-3148(config)# qos 802.1p-map 3 2 FOS-3148(config)# qos 802.1p-map 5 3	**In this example, it configures the P-Bit 0 with Queue Mapping to Q0, the P-Bits 1 with Queue Mapping to Q1, the P-Bits 3 with Queue Mapping to Q2, and the P-Bit 5 with Queue Mapping to Q3**
STEP6	interface *port_list* **Example:** FOS-3110(config)# interface 3, 4 FOS-3110(config-if-3,4)#	**Specify the Port 3 and Port 4 that you would like to configure QoS Rate limit.**
STEP7	qos rate-limit ingress *limit_rate(kbps)* **Example:** FOS-3110(config-if-3,4)# qos rate-limit ingress 10000 OK !	**In this example, it configures Port 3 and Port 4 with 1G Ingress Rate.**
STEP8	qos rate-limit egress *limit_rate(kbps)* **Example:** FOS-3110(config-if-3,4)# qos rate-limit egress 10000 OK !	**In this example, it configures Port 3 and Port 4 with 1G Egress Rate.**
STEP9	exit **Example:** FOS-3110(config-if-3,4)# exit FOS-3110(config)#	**Return to the global configuration mode.**
STEP10	interface *port_list* **Example:** FOS-3110(config)# interface 5 FOS-3110(config-if-5)#	**Specify the Port 5 that you would like to configure QoS Rate limit.**
STEP11	qos rate-limit ingress *limit_rate(kbps)* **Example:** FOS-3110(config-if-5)# qos rate-limit ingress 1000000 OK !	**In this example, it configures Port 5 with 100G Ingress Rate.**

STEP12	qos rate-limit egress *limit_rate(kbps)* **Example:** FOS-3110(config-if-5)# qos rate-limit egress 1000000 OK !	**In this example, it configures Port 5 with 100G Engress Rate.**
STEP13	exit **Example:** FOS-3110(config-if-5)# exit FOS-3110(config)#	**Return to the global configuration mode.**
STEP14	write **Example:** FOS-3110# write Save Config Succeeded!	**Save the running configuration into the startup configuration.**

After completing the QoS settings for your FOS-3110 switches, you can issue the commands listed below for checking your configuration

Example 1,

FOS-3110(config)# show qos

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

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

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

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


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

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

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

Example 2,

FOS-3110(config)# show vlan interface

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

Example 3,

FOS-3110(config)# show qos interface

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

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

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

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

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

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

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

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

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

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

Port                   : 6
Ingress Rate Limiter : disable
Egress Rate Limiter  : disable

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

Port                   : 7
Ingress Rate Limiter : disable
Egress Rate Limiter  : disable

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

Port                    : 8
Ingress Rate Limiter : disable
Egress Rate Limiter  : disable

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

Port                    : 9
Ingress Rate Limiter : disable
Egress Rate Limiter  : disable

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

Port                    : 10
Ingress Rate Limiter : disable
Egress Rate Limiter  : disable
```

2.6.18 Security Command

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

Enable or disable broadcast/unknown multicast/unknown unicast storm control.

Security command	Parameter	Description
Switch(config)# security mac-limit		Globally enable the MAC Limit function on the switch. This is to set number of threshold whthin which MAC address can be learned. After it reaches threshold, any other incoming MAC address would be dropped until the recovery mechanism activates.
Switch(config-if-PORT-PORT)# security mac-limit		Enable MAC Limit function of the selected port(s).
Switch(config-if-PORT-PORT)# security mac-limit maximum [0-1024]	[0-1024]	Specify the number of MAC address that can be learned. “0” indicates there is no limit on specified ports. The valid range of number that can be configured is 0~1024.
Switch(config)# security port-isolation		Enable port isolation function. If port isolation is set to enabled, the ports cannot communicate with each other.
Switch(config)# security port-isolation up-link-port [port_list]	[port_list]	Specify the port(s) as uplinks that are allowed to communicate with other ports.
Switch(config)# 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)# security storm-protection 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)# security storm-protection 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)# no security mac-limit		Globally disable MAC Limit function on the switch.
Switch(config)# no security port-isolation		Disable port isolation function.
Switch(config)# no security port-isolation up-link-port [port_list]	[port_list]	Disable the specified port(s) as non-up-link-port.
Switch(config)# no security storm-protection broadcast		Disable broadcast storm control.
Switch(config)# no security storm-protection multicast		Disable multicast storm control.
Switch(config)# no security storm-protection unicast		Disable unicast storm control.
Switch(config-if-PORT-PORT)# no security mac-limit		Disable MAC Limit function of the selected port(s).
Switch(config-if-PORT-PORT)# no security mac-limit maximum		Reset the MAC Limit back to the default "0". "0" indicates there is no limit on specified ports.
Show command		
Switch(config)# show security mac-limit		Show the current MAC Limit configuration of all ports.
Switch(config)# show security mac-limit [port_list]	[port_list]	Show the current MAC Limit configuration of specified ports.
Switch(config)# show security port-isolation		Show the current port isolation configuration.
Switch(config)# show security storm-protection		Show the current storm control configurations.

Examples of Security command	
Switch(config)# security storm-protection broadcast 256k	Set the maximum broadcast packets per second (pps) to 256k. Any broadcast packets exceeding this specified threshold will then be dropped.
Switch(config)# security storm-protection multicast 128k	Set the maximum unknown multicast packets per second (pps) to 128k. Any unknown multicast packets exceeding this specified threshold will then be dropped.
Switch(config)# security storm-protection unicast 32k	Set the maximum unknown unicast packets per second (pps) to 32k. Any unknown unicast packets exceeding the specified threshold will then be dropped.

2.6.19 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 server function globally.
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 function.
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 trap destination you would like to modify.
Switch(config-trap-ID)# active		Enable the specified SNMP trap destination.
Switch(config-trap-ID)# community [community]	[community]	Enter the description for the secified 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 IP/IPv6 address for the secified trap destination.
No command		
Switch(config)# no snmp-server trap-destination [1-3]	[1-3]	Reset the specified 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 trap destination.
Switch(config-trap-ID)# no destination		Delete SNMP server IP/IPv6 address for the specified 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 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 do the modification.
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 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 | digital | port-link | power-down | warm-start | console-port-link]	[all | auth-fail | auto-backup | cold-start | cpu-load | digital | port-link | power-down | warm-start | console-port-link]	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, digital input is alarmed, cpu is overload, power failure occurs and console port link up/down . **auth-fail:** A trap will be sent when any unauthorized user attempts to login. **auto-backup:** A trap will be sent when the auto backup succeeds or fails. **cold-start:** A trap will be sent when the Managed Switch boots up. **cpu-load:** A trap will be sent when the CPU is overloaded. **Digital:** A trap will be sent when the alarm occurs. **port-link:** A trap will be sent when the link is up or down. **power-down:** A trap will be sent when the Managed Switch’s power is down. **warm-start:** A trap will be sent when the Managed Switch restarts. **console-port-link:** A trap will be sent when when console port link up/link down trap.

No command		
Switch(config)# no snmp-server trap-type [all | auth-fail | auto-backup | cold-start | cpu-load | digital | port-link | power-down | warm-start | console-port-link]	[all | auth-fail | battery-mode | case-fan | cold-start | port-link | power-down | 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 2.6.25)

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]		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 as below indicates which security mechanism is used when handling an SNMP packet.

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

2.6.20 Spanning-tree Command

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

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

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

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

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

tree delay-time [4-30]		seconds. The allowable value is between 4 and 30 seconds.
Switch(config)# spanning-tree hello-time [1-10]	[1-10]	Specify the hello interval value in seconds. The allowable value is between 1 and 10 seconds.
Switch(config)# spanning-tree max-age [6-200]	[6-200]	Specify the maximum age time value in seconds. The allowable value is between 6 and 200.
Switch(config)# spanning-tree priority [0-15]	[0-15]	Specify a priority value on a per switch basis. The allowable value is between 0 and 15. **0=0, 1=4096, 2=8192, 3=12288, 4=16384, 5=20480, 6=24576, 7=28672, 8=32768, 9=36864, 10=40960, 11=45056,12=49152, 13=53248, 14=57344, 15=61440**
Switch(config)# spanning-tree version [compatible | normal]	[compatible | normal]	Set up RSTP version. **"compatible"** means that the Managed Switch is compatible with STP. **"normal"** means that the Managed Switch uses RSTP.
No command		
Switch(config)# no spanning-tree aggregated-port		Disable STP on aggregated ports.
Switch(config)# no spanning-tree aggregated-port cost		Reset aggregated ports' cost back to the factory default.
Switch(config)# no spanning-tree aggregated-port priority		Reset aggregated ports' priority back to the factory default.
Switch(config)# no spanning-tree aggregated-port edge		Disable aggregated ports' edge ports status.
Switch(config)# no spanning-tree aggregated-port p2p		Reset aggregated ports back to non-point to point ports (forced_ false).
Switch(config)# no spanning-tree delay-time		Reset the Forward Delay time back to the factory default.
Switch(config)# no spanning-tree hello-time		Reset the Hello Time back to the factory default.
Switch(config)# no spanning-tree max-age		Reset the Maximum Age back to the factory default.
Show command		
Switch(config)# show spanning-tree		Show or verify RSTP settings on the per switch basis.
Switch(config)# show spanning-tree aggregated-port		Show or verify RSTP settings on aggregated ports.
Switch(config)# show spanning-tree interface		Show each interface's RSTP information, including port state, path cost, priority, edge port state, and p2p port state.
Switch(config)# show spanning-tree interface [port_list]	[port_list]	Show the selected interfaces' RSTP information, including port state, path cost, priority, edge port state, and p2p port state.

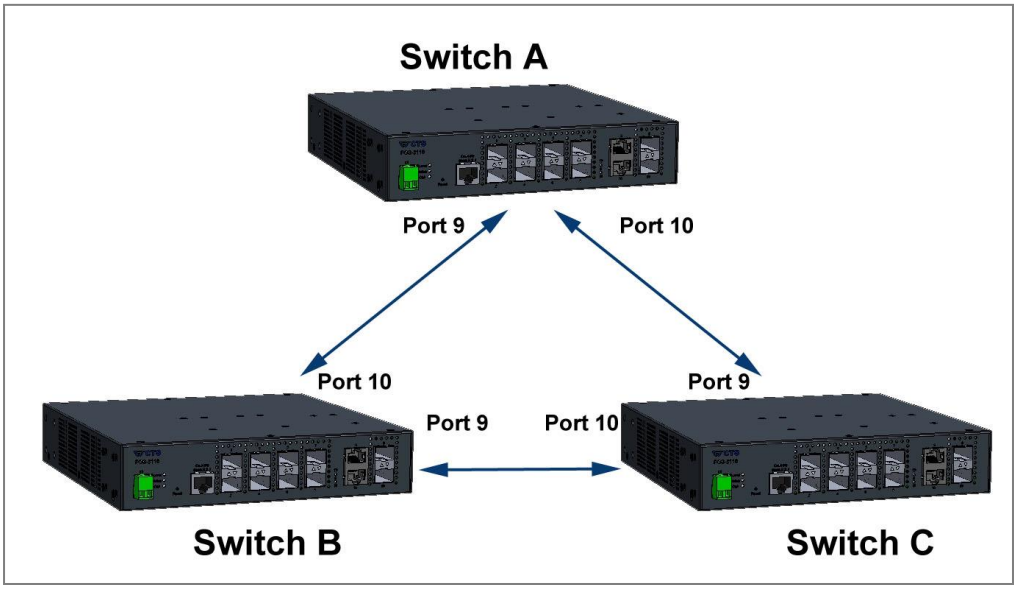
Switch(config)# show spanning-tree statistic		Show each interface and each link aggregation group's statistics information, including the total RSTP packets received, RSTP packets transmitted, STP packets received, STP packets transmitted, TCN (Topology Change Notification) packets received, TCN packets transmited, illegal packets received, and unknown packets received.
Switch(config)# show spanning-tree statistic [port_list | llag]	[port_list | llag]	Show the selected interfaces or link aggregation groups' statistics information, including the total RSTP packets received, RSTP packets transmitted, STP packets received, STP packets transmitted, TCN (Topology Change Notification) packets received, TCN packets transmited, illegal packets received, and unknown packets received.
Switch(config)# show spanning-tree status		Show the current RSTP port status.
Switch(config)# show spanning-tree status [port_list | llag]	[port_list | llag]	Show the selected interfaces or link aggregation groups' status.
Switch(config)# show spanning-tree overview		Show the current root-related information.
Spanning-tree command Example		**Description**
Switch(config)# spanning-tree aggregated-port		Enable Spanning Tree on aggregated ports.
Switch(config)# spanning-tree aggregated-port cost 100		Set the aggregated ports' cost to 100.
Switch(config)# spanning-tree aggregated-port priority 0		Set the aggregated ports' priority to 0
Switch(config)# spanning-tree aggregated-port edge		Set the aggregated ports to edge ports.
Switch(config)# spanning-tree aggregated-port p2p forced_true		Set the aggregated ports to P2P ports.
Switch(config)# spanning-tree delay-time 20		Set the Forward Delay time value to 10 seconds.
Switch(config)# spanning-tree hello-time 2		Set the Hello Time value to 2 seconds.
Switch(config)# spanning-tree max-age 15		Set the Maximum Age value to 15 seconds.

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

Spanning tree & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# spanning-tree		Enable spanning-tree protocol on the selected interfaces.
Switch(config-if-PORT-PORT)# spanning-tree cost [0-200000000]	[0-200000000]	Specify the path cost value on the selected interfaces.
Switch(config-if-PORT-PORT)# spanning-tree priority [0-15]	[0-15]	Specify priority value on the selected interfaces. **0=0, 1=16, 2=32, 3=48, 4=64** **5=80, 6=96, 7=112, 8=128** **9=144, 10=160, 11=176,12=192** **13=208, 14=224, 15=240**
Switch(config-if-PORT-PORT)# spanning-tree edge		Set the selected interfaces to edge ports.
Switch(config-if-PORT-PORT)# spanning-tree p2p [forced_true| forced_fasle | auto]	[forced_true | forced_fasle | auto]	Set the selected interfaces to non-point to point ports (forced_false) or allow the Managed Switch to detect point to point status automatically (auto). By default, physical ports are set to point to point ports (forced_true).
No command		
Switch(config-if-PORT-PORT)# no spanning-tree		Disable spanning-tree protocol on the selected interfaces.
Switch(config-if-PORT-PORT)# no spanning-tree cost		Reset the cost value back to the default.
Switch(config-if-PORT-PORT)# no spanning-tree priority		Reset the priority value back to the default.
Switch(config-if-PORT-PORT)# no spanning-tree edge		Reset the selected interfaces back to non-edge ports.
Switch(config-if-PORT-PORT)# no spanning-tree p2p		Reset the selected interfaces back to point to point ports (forced_ true).
Show command		
Switch(config)# show spanning-tree		Show or verify RSTP settings on the per switch basis.
Switch(config)# show spanning-tree interface		Show each interface's RSTP information, including port state, path cost, priority, edge port state, and p2p port state.
Switch(config)# show spanning-tree interface [port_list]	[port_list]	Show the selected interfaces' RSTP information, including port state, path cost, priority, edge port state, and p2p port state.
Switch(config)# show spanning-tree statistic		Show each interface and each link aggregation group's statistics

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

For RSTP configuration via CLI, we take the following ring network topology composed of 3 sets of FOS-3110 Managed Switches, including Switch A, Switch B and Switch C for example to let the users have a clear understanding of these RSTP commands. Under this network environment, Switch A, Switch B and Switch C will be configured as Table 2-2, and the “Root Switch” will automatically be determined by this network.



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

Table 2-2

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

	Command	Purpose
STEP1	configure **Example:** FOS-3110# config FOS-3110(config)#	**Enter the global configuration mode.**
STEP2	spanning-tree priority *system_priority* **Example:** FOS-3110(config)# spanning-tree priority 1 OK !	**In this example, it configures the System Priority of Switch A as “1”. It means the value of the real priority is 4096.**
STEP3	spanning-tree max-age *max_age_time* **Example:** **FOS-3110(config)# spanning-tree max-age 6** **OK !**	**In this example, it configures the Max. Age Time of Switch A as “6”.**
STEP4	spanning-tree hello-time *hello_interval* **Example:** FOS-3110(config)# spanning-tree hello-time 1 OK !	**In this example, it configures the Hello Time of Switch A as “1”.**

STEP5	spanning-tree delay-time *forward_delay_time* **Example:** FOS-3110(config)# spanning-tree delay-time 4 OK !	**In this example, it configures the Forward Delay Time of Switch A as 4.**
STEP6	spanning-tree version *stp_version* **Example:** FOS-3110(config)# spanning-tree version normal OK !	**In this example, it configures the STP Version of Switch A as "Normal".**
STEP7	interface *port_list* **Example:** FOS-3110(config)# interface 9-10 FOS-3110(config-if-9,10)#	**Specify the Port 9 and Port 10 that you would like to configure to RSTP.**
STEP8	spanning-tree **Example:** FOS-3110(config-if-9,10)# spanning-tree OK !	**Enable spanning tree protocol**
STEP9	spanning-tree cost *path_cost* **Example:** FOS-3110(config-if-9,10)# spanning-tree cost 0 OK !	**In this example, it configure the port path cost for Port 9 and Port 10 as 0.**
STEP10	spanning-tree priority *bridge_priority* **Example:** FOS-3110(config-if-9,10)# spanning-tree priority 0 OK !	**In this example, it configure the port priority for Port 9 and Port 10 as 0. It means the value of the real priority is "0".**
STEP11	spanning-tree edge **Example:** FOS-3110(config-if-9,10)# no spanning-tree edge OK !	**In this example, it configure Port 9 and Port 10 as the non-edge ports.**
STEP12	spanning-tree p2p *type* **Example:** FOS-3110(config-if-9,10)# spanning-tree p2p forced_true OK !	**In this example, it configures the type of Port 9 and Port 10 as point to point ports.**
STEP13	exit **Example:** FOS-3110(config-if-9,10)# exit FOS-3110(config)#	**Return to the global configuration mode.**
STEP14	exit **Example:** FOS-3110(config)# exit FOS-3110#	**Return to the Privileged mode.**
STEP15	write **Example:** FOS-3110# write Save Config Succeeded!	**Save the running configuration into the startup configuration.**

After completing the RSTP Switch settings for your FOS-3110 switches, you can issue the commands listed below for checking your configuration

Example 1,

FOS-3110(config)# show spanning-tree

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

FOS-3110(config)#
```

Example 2,

FOS-3110(config)# show spanning-tree aggregated-port

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

FOS-3110(config)#
```

Example 3,

FOS-3110(config)# show spanning-tree interface

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

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

9      enable     0           0           disable    forced-true
10     enable     0           0           disable    forced-true
FOS-3110(config)#
```

Example 4,

FOS-3110(config)# show spanning-tree overview

```
================================================================================
RSTP overview
================================================================================

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

FOS-3110(config)#
```

Example 5,

FOS-3110(config)# show spanning-tree statistic

```
==========================================================================
RSTP Port Statistics
==========================================================================
Port   Rx RSTP   Tx RSTP   Rx STP   Tx STP   Rx TCN   Tx TCN   Rx Ill.   Rx Unk
------ ---------- ---------- ---------- ---------- ---------- ---------- ---------
1        0          0          0          0          0          0          0          0
2        0          0          0          0          0          0          0          0
3        0          0          0          0          0          0          0          0
4        0          0          0          0          0          0          0          0
5        0          0          0          0          0          0          0          0
6        0          0          0          0          0          0          0          0
7        0          0          0          0          0          0          0          0
8        0          0          0          0          0          0          0          0

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

9        0          0          0          0          0          0          0          0
10       0          0          0          0          0          0          0          0

LLAG1  0          0          0          0          0          0          0          0
LLAG2  0          0          0          0          0          0          0          0
LLAG3  0          0          0          0          0          0          0          0
LLAG4  0          0          0          0          0          0          0          0
LLAG5  0          0          0          0          0          0          0          0


FOS-3110(config)#
```

Example 6,

FOS-3110(config)# show spanning-tree status

```
==========================================================================
RSTP Port Status
==========================================================================
                    Edge   P2p                                  Port
Port    PathCost    Port   Port   Protocol   Role           State
------ ---------- ------- ------ ---------- ---------- ----------
1          0          no     yes    RSTP       Non-STP    Non-STP
2          0          no     yes    RSTP       Non-STP    Non-STP
3          0          no     yes    RSTP       Non-STP    Non-STP
4          0          no     yes    RSTP       Non-STP    Non-STP
5          0          no     yes    RSTP       Non-STP    Non-STP
6          0          no     yes    RSTP       Non-STP    Non-STP
7          0          no     yes    RSTP       Non-STP    Non-STP
8          0          no     yes    RSTP       Non-STP    Non-STP
```

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

9       2000000  no   yes   RSTP    Disable      Disable
10      20000    no   yes   RSTP    Designated   Forwarding

LLAG1   0        no   no    RSTP    Non-STP      Non-STP
LLAG2   0        no   no    RSTP    Non-STP      Non-STP
LLAG3   0        no   no    RSTP    Non-STP      Non-STP
LLAG4   0        no   no    RSTP    Non-STP      Non-STP
LLAG5   0        no   no    RSTP    Non-STP      Non-STP
```

2.6.21 Switch Command

Switch command	Parameter	Description
Switch(config)# switch bpdu 00-0F [permit]	[permit]	Permit packets from the address ranging from 0180C2000000 to 0180C200000F.
Switch(config)# switch bpdu 20-2F [permit]	[permit]	Permit packets from the address ranging from 0180C2000020 to 0180C200002F.
Switch(config)# switch bpdu 10 [permit]	[permit]	Permit packets from the address 0180C2000010.
Switch(config)# switch mtu [1518-9600]	[1518-9600] bytes	Specify the maximum frame size in bytes. The allowable MTU value is between 1518 and 9600 bytes.
Switch(config)# switch statistics polling port [1-10]	[1-10]	Specify the number of ports for data acquisition in each polling.
Switch(config)# switch statistics polling interval [1-600]	[1-600] (1/10secs)	Specify the time interval between each polling.
No command		
Switch(config)# no switch bpdu 00-0F		Undo permit packets from the address ranging from 0180C2000000 to 0180C200000F.
Switch(config)# no switch bpdu 20-2F		Undo permit packets from the address ranging from 0180C2000020 to 0180C200002F.
Switch(config)# no switch bpdu 10		Undo permit packets from the address 0180C2000010.
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. (5 ports)
Switch(config)# no switch statistics polling interval		Reset the time interval between each polling back to the default. (50 in 1/10 seconds)
Show command		
Switch(config)# show switch bpdu		Show the current BPDU configuration.
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 bpdu 00-0F permit	Permit packets from the address ranging from 0180C2000000 to 0180C200000F.
Switch(config)# switch bpdu 20-2F permit	Permit packets from the address ranging from 0180C2000020 to 0180C200002F.
Switch(config)# switch bpdu 10 permit	Permit packets from the address 0180C2000010.
Switch(config)# switch mtu 9600	Set the maximum transmission unit to 9600 bytes.

2.6.22 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 dhcp-vendor-id [dhcp_vendor_id]	[dhcp_vendor_id]	Enter a DHCP vendor ID, up to 55 alphanumeric characters, for this Managed Switch.
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 dhcp-vendor-id		Reset the entered DHCP vendor ID information 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.
Switch(config)# no switch-info host-name		Reset the hostname 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.
Examples of Switch-info	
Switch(config)# switch-info company-name telecomxyz	Set the company name to “telecomxyz”.
Switch(config)# switch-info system-contact info@company.com	Set the system contact field to “info@compnay.com”.
Switch(config)# switch-info system-location 13thfloor	Set the system location field to “13thfloor”.
Switch(config)# switch-info system-name backbone1	Set the system name field to “backbone1”.
Switch(config)# switch-info host-name edgeswitch10	Change the Managed Switch’s hostname into “edgeswitch10”.

2.6.23 Syslog Command

Syslog command	Parameter	Description
Switch(config)# syslog		Enable the system log function.
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 IP/IPv6address.
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 IP/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 IP/IPv6 address.
No command		
Switch(config)# no syslog		Disable System log function.
Switch(config)# no syslog logging-type terminal-history		Disable Terminal-history log function.
Switch(config)# no syslog server1		Delete the primary system log server IP address.
Switch(config)# no syslog server2		Delete the secondary system log server IP address.
Switch(config)# no syslog server3		Delete the third system log server IP address.
Show command		
Switch(config)# show syslog		Show the current system log configuration.

Switch(config)# show log	Show event logs currently stored in the Managed Switch. These event logs will be saved to the system log server that you specify.
Syslog command example	
Switch(config)# syslog	Enable System log function.
Switch(config)# syslog server1 192.180.2.1	Set the primary system log server IP address to 192.168.2.1.
Switch(config)# syslog server2 192.168.2.2	Set the secondary system log server IP address to 192.168.2.2.
Switch(config)# syslog server3 192.168.2.3	Set the third system log server IP address to 192.168.2.3.

2.6.24 Terminal Length Command

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 terminal length back to the default (20).
Show Command		
Switch(config)# show terminal		Show the current configuration of terminal length.

2.6.25 User Command

1. Create a new login account.

User command	Parameter	Description
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 [user_name]	[user_name]	Create/modify a user account. The authorized user login name is up to 20 alphanumeric characters. Only 5 login accounts can be registered in this device at the same time.
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 password-encryption		Disable MD5(Message-Digest Algorithm).
Switch(config)#no user name [user_name]	[user_name]	Delete the specified account.

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 password		Remove the configured password for the specified user account.
Switch(config-user-NAME)# no level		Reset the access privilege level back to the default (Read Only).
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 IP/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 IP/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 IP/IPv6 address of the primary RADIUS server.
Switch(config)# no user radius server2		Delete the IP/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 to 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.

3. Configure TACACS server settings.

User command	Parameter	Description
Switch(config)# user tacacs		Enable TACACS authentication.
Switch(config)# user tacacs tacacs-port [49, 1025-65535]	[49, 1025-65535]	Specify TACACS server port number. The default setting is at 49 port.
Switch(config)# user tacacs 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 TACACS server is not reachable.
Switch(config)# user tacacs secret [secret]	[secret]	Specify a secret, up to 30 alphanumeric characters, for TACACS server. This secret key is used to validate communications between TACACS servers.
Switch(config)# user tacacs 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 TACACS server IP/IPv6 address.
Switch(config)# user tacacs 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 TACACS server IP/IPv6 address.
No command		
Switch(config)# no user tacacs		Disable TACACS authentication.
Switch(config)# no user tacacs tacacs-port		Reset the tacacs port setting back to the default.(49 port)
Switch(config)# no user tacacs retry-time		Reset the retry time setting back to the default.
Switch(config)# no user tacacs secret		Remove the configured secret value.
Switch(config)# no user tacacs server1		Delete the IP/IPv6 address of the primary TACACS server.
Switch(config)# no user tacacs server2		Delete the IP/IPv6 address of the secondary TACACS server.
Show command		
Switch(config)#show user tacacs		Show the current TACACS configuration.

2.6.26 VLAN Command

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

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

2.6.26.1 Port-Based VLAN

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

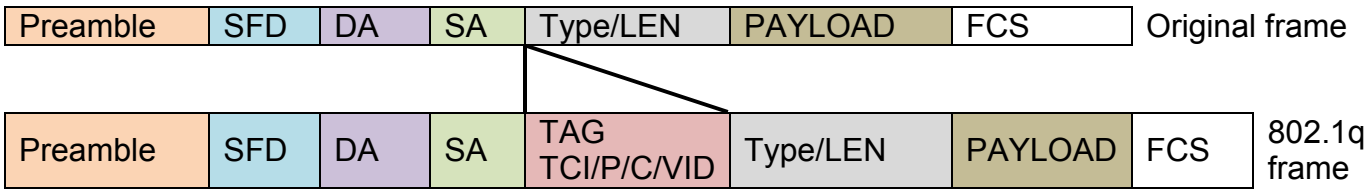
Since source addresses of the packets are listed in MAC address table of specific VLAN (except broadcast/multicast packets), in every VLAN the traffic between two ports will be two-way without restrictions.

2.6.26.2 802.1Q 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.

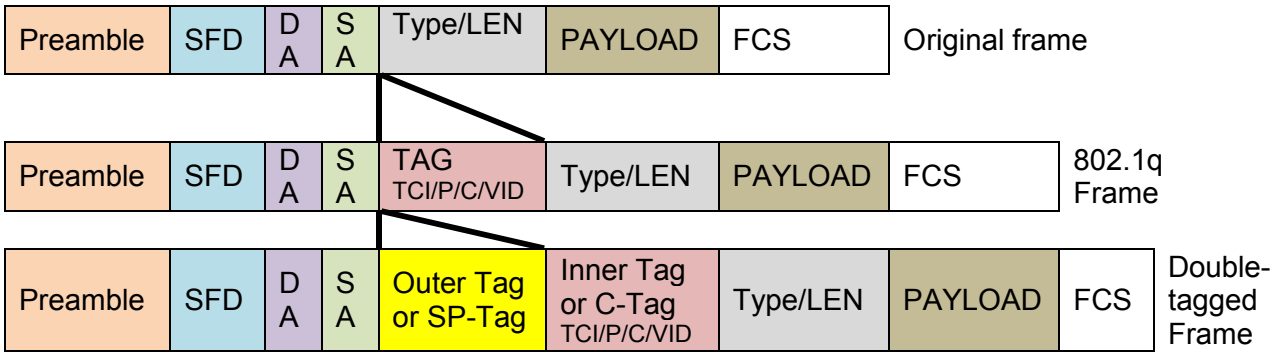
- Customer traffic tagged in the normal way with appropriate VLAN IDs comes from an IEEE 802.1Q trunk port on the customer device and into a tunnel port on the service-provider edge switch. The link between the customer device and the edge switch is asymmetric because one end is configured as an IEEE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

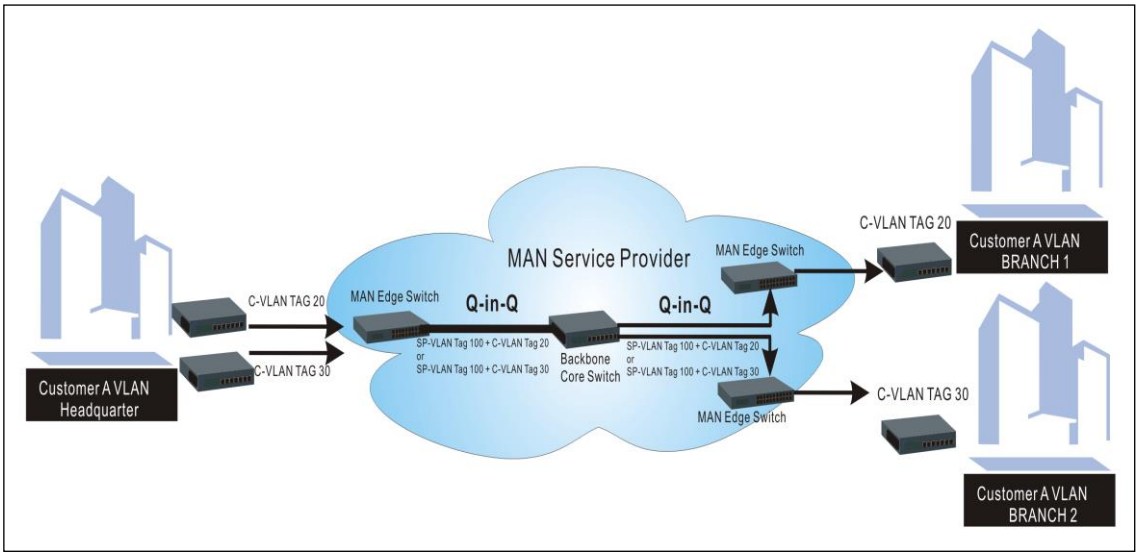
2.6.26.3 Introduction to Q-in-Q (DOT1Q-Tunnel)

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-basedVLAN settings.**

VLAN & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
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 port. (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 access-vlan		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 back to the default setting (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.

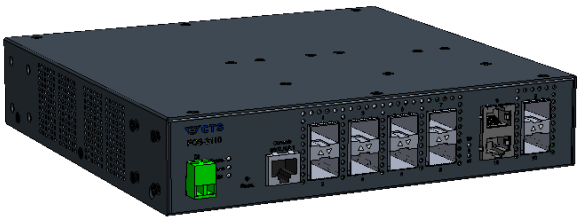
VLAN dot1q command	Parameter	Description
Switch(config)# vlan dot1q-vlan [1-4094]	[1-4094]	Enter a VLAN ID number to create a new 802.1q VLAN or modify an existing 802.1q VLAN.
Switch(config-vlan-ID)# name [vlan_name]	[vlan_name]	Specify a descriptive name for the created VLAN ID, maximun 15 characters.
Switch(config)# vlan isolation up-link-port [port_list]	[port_list]	To assign uplink ports which will form a port-based VLAN group with all other downlink ports separately so as to isolate downlink ports from each other except from uplink ports.
Switch(config)# vlan isolation		Enable the port isolation function. If the port isolation is set to “Enabled”, the ports cannot communicate with each other.
Switch(config)# vlan management-vlan [1-4094] management-port [port_list] mode [trunk | access]	[1-4094]	Enter the management VLAN ID.
	[port_list]	Specify the management port number.
	[trunk | access]	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.
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 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 dot1q-tunnel ethertype		Reset outer VLAN's ethertype back to the default setting (9100).
Switch(config)# no vlan isolation up-link-port [port_list]		Remove the specified up link port for port VLAN isolation.
Switch(config)# no vlan isolation		Disable port isolation mode.
Show command		
Switch(config)# show vlan dot1q-vlan tag-vlan		Show IEEE 802.1q tag VLAN table
Switch(config-vlan-ID)# show		Show the membership status of this VLAN ID

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

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 FOS-3110 Managed Switch via CLI as the Table 2-3 listed.



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

Table 2-3

1. Create 802.1q VLAN IDs.

FOS-3110(config)# interface 1-2	Enter port 1 to port 2's interface mode.
FOS-3110(config-if-1,2)# vlan dot1q-vlan trunk-vlan 10, 20	Set port 1 to port 2's Trunk-VLAN ID (VID) to 10 and 20.
FOS-3110(config-if-1,2)# vlan dot1q-vlan mode trunk	Set the selected ports to Trunk Mode (tagged).
FOS-3110(config-if-1,2)#exit	Exit current ports interface mode

FOS-3110 (config)# interface 3-4	Enter port 3 to 4's interface mode.
FOS-3110(config-if-3,4)# vlan dot1q-vlan access-vlan 50	Set port 3 to port 4's Access-VLAN ID (PVID) to 50.
FOS-3110(config-if-3,4)# vlan dot1q-vlan trunk-vlan 30,40	Set port 3 to port 4's Trunk-VLAN ID (VID) to 30 and 40.
FOS-3110(config-if-3,4)# vlan dot1q-vlan mode trunk native	Set the selected ports to Trunk-native Mode (tagged and untagged).
FOS-3110(config-if-3,4)#exit	Exit current ports interface mode
FOS-3110 (config)# interface 5-6	Enter port 5 to port 6's interface mode.
FOS-3110(config-if-5,6)# vlan dot1q-vlan access-vlan 60	Set port 5 to port 6's Access-VLAN ID (PVID) to 60.
FOS-3110(config-if-5,6)# vlan dot1q-vlan mode access	Set the selected ports to Access Mode (untagged).
FOS-3110(config-if-5,6)#exit	Exit current ports interface mode
FOS-3110(config)# interface 7-8	Enter port 7 to port 8's interface mode.
FOS-3110(config-if-7,8)# vlan dot1q-vlan access-vlan 70	Set port 7 to port 8's Access-VLAN ID (PVID) to 70.
FOS-3110(config-if-7,8)# vlan dot1q-vlan mode access	Set the selected ports to Access Mode (untagged).
FOS-3110(config-if-7,8)#exit	Exit current ports interface mode

2. Modify 802.1q VLAN IDs' names.

FOS-3110(config)# vlan dot1q-vlan 10	Enter VLAN 10.
FOS-3110 (config-vlan-10)# name Sales	Specify "Sales" as the name for VLAN 10.
FOS-3110 (config-vlan-10)# exit	Exit VLAN 10.
FOS-3110(config)# vlan dot1q-vlan 20	Enter VLAN 20.
FOS-3110(config-vlan-20)# name Sales	Specify "Sales" as the name for VLAN 20.
FOS-3110(config-vlan-20)# exit	Exit VLAN 20.
FOS-3110(config)# vlan dot1q-vlan 30	Enter VLAN 30.
FOS-3110(config-vlan-30)# name RD	Specify "RD" as the name for VLAN 30.
FOS-3110(config-vlan-30)# exit	Exit VLAN 30.
FOS-3110(config)# vlan dot1q-vlan 40	Enter VLAN 40.
FOS-3110(config-vlan-40)# name RD	Specify "RD" as the name for VLAN 40.
FOS-3110(config-vlan-40)# exit	Exit VLAN 40.
FOS-3110(config)# vlan dot1q-vlan 50	Enter VLAN 50.
FOS-3110(config-vlan-50)# name RD	Specify "RD" as the name for VLAN 50.
FOS-3110(config-vlan-50)# exit	Exit VLAN 50.
FOS-3110(config)# vlan dot1q-vlan 60	Enter VLAN 60.
FOS-3110(config-vlan-60)# name SQA	Specify "SQA" as the name for VLAN 60.
FOS-3110(config-vlan-60)# exit	Exit VLAN 60.
FOS-3110 (config)# vlan dot1q-vlan 70	Enter VLAN 70.
FOS-3110 (config-vlan-70)# name PME	Specify "PME" as the name for VLAN 70.
FOS-3110 (config-vlan-70)# exit	Exit VLAN 70.

Example 2,

We will configure two sets of FOS-3110 Managed Switch(including #1 FOS-3110 and #2 FOS-3110) via CLI as theTable 2-4 listed.

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

Table 2-4

Below is the complete CLI commands applied to #1 FOS-3110. Also issue the same commands to #2 FOS-3110.

	Command	Purpose
STEP1	configure **Example:** FOS-3110# config FOS-3110(config)#	**Enter the global configuration mode.**
STEP2	vlan dot1q-tunnel ethertype *0xWXYZ* **Example:** FOS-3110(config)# vlan dot1q-tunnel ethertype 9100 OK !	**In this example, it configures the dot1q-tunnel ethertype value as "9100"**
STEP3	interface *port_list* **Example:** FOS-3110(config)# interface 1 FOS-3110 (config-if-1)#	**Specify Port 1 that you would like to configure it as dot1q-tunnel port.**
STEP4	vlan dot1q-vlan access-vlan *vlan_id* **Example:** FOS-3110(config-if-1)# vlan dot1q-vlan access-vlan 10 OK !	**In this example, it configures Access-VLAN ID "10" to Port 1.**
STEP5	vlan dot1q-vlan mode *dot1q-tunnel* **Example:** **FOS-3110** (config-if-1)# vlan dot1q-vlan mode dot1q-tunnel OK !	**Configure Port 1's VLAN mode as "dot1q-tunnel" mode.**
STEP6	exit **Example:** FOS-3110 (config-if-1)# exit FOS-3110 (config)#	**Return to the global configuration mode.**
STEP7	interface *port_list* **Example:** FOS-3110(config)# interface 2 FOS-3110(config-if-2)#	**Specify Port 2 that you would like to configure it as Trunk port.**

STEP8	vlan dot1q–vlan trunk–vlan *vlan_id* **Example:** FOS-3110(config-if-2)# vlan dot1q-vlan trunk-vlan 10 OK !	**In this example, it configures Trunk-VLAN ID "10" to Port 2.**
STEP9	v lan dot1q–vlan mode *trunk* **Example:** FOS-3110(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:** FOS-3110(config-if-2)# no vlan dot1q-vlan trunk-vlan 1 OK !	**Remove the Trunk-VLAN ID "1" from Port 2.**
STEP10	exit **Example:** FOS-3110 (config-if-2)# exit FOS-3110 (config)#	**Return to the global configuration mode.**
STEP11	interface *port_list* **Example:** FOS-3110(config)# interface 3 FOS-3110 (config-if-3)#	**Specify Port 3 that you would like to configure it as Dot1q-Tunnel port.**
STEP12	vlan dot1q–vlan access–vlan *vlan_id* **Example:** FOS-3110(config-if-3)# vlan dot1q-vlan access-vlan 20 OK !	**In this example, it configures Access-VLAN ID "20" to Port 3.**
STEP13	vlan dot1q–vlan mode *dot1q–tunnel* **Example:** **FOS-3110** (config-if-3)# vlan dot1q-vlan mode dot1q-tunnel OK !	**Configure Port 3's VLAN mode as "dot1q-tunnel" mode.**
STEP14	exit **Example:** FOS-3110 (config-if-3)# exit FOS-3110 (config)#	**Return to the global configuration mode.**
STEP15	interface *port_list* **Example:** FOS-3110(config)# interface 4 FOS-3110(config-if-4)#	**Specify Port 4 that you would like to configure it as dot1q-tunnel port.**
STEP16	vlan dot1q–vlan access–vlan *vlan_id* **Example:** FOS-3110(config-if-4)# vlan dot1q-vlan access-vlan 20 OK !	**In this example, it configures Access-VLAN ID "20" to Port 4.**

STEP17	vlan dot1q-vlan mode *dot1q-tunnel* **Example:** **FOS-3110** (config-if-4)# vlan dot1q-vlan mode dot1q-tunnel OK !	**Configure Port 4's VLAN mode as "dot1q-tunnel" mode.**
STEP18	exit **Example:** FOS-3110 (config-if-4)# exit FOS-3110 (config)#	**Return to the global configuration mode.**
STEP19	exit **Example:** FOS-3110(config)# exit FOS-3110#	**Return to the Privileged mode.**
STEP20	write **Example:** FOS-3110# write Save Config Succeeded!	**Save the running configuration into the startup configuration.**

After completing the VLAN settings for your FOS-3110 switches, you can issue the commands listed below for checking your configuration

Example 1,

FOS-3110(config)# show vlan interface

```
================================================================================
IEEE 802.1q Tag VLAN Interface :
================================================================================
Dot1q-Tunnel EtherType : : 0x9100
Port  Access-vlan  User Priority  Port VLAN Mode  Trunk-vlan
----  -----------  -------------  --------------  ----------
  1            10              0  dot1q tunnel    1
  2             1              0  trunk           10
  3            20              0  dot1q tunnel    1
  4            20              0  dot1q tunnel    1
  5             1              0  access          1
  6             1              0  access          1
  7             1              0  access          1
  8             1              0  access          1
  9             1              0  access          1
 10             1              0  access          1

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

FOS-3110(config)#
```

Example 2,

FOS-3110(config)# show vlan dot1q-vlan tag-vlan

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

U: untagged port, T: tagged port, D: dot1q-tunnel port, V: member port
--------------------------------------------------------------------------------
VLAN Name       VLAN   1           8  10  CPU
--------------------  - - - -   - - - - - - - -  - -  - - -
Default_VLAN           1  - - - -UUUU UU    V
                      10  DT - - - - - -  - -    -
Access-0020           20  - - DD - - - -  - -    -

FOS-3110(config)#
```

2.6.27 Interface Command

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

1. Entering interface numbers.

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

Note : You need to enter interface numbers first before issuing below 2-18 commands.

2. Enable port auto-negotiation.

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

3. Set up link aggregation or port-trunking.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# channel-group lacp		Set the selected interfaces’ to be aggregated via LACP. **Note : At lease 2 ports but not more than 8 ports can be aggregated.**
Switch(config-if-PORT-PORT)# channel-group lacp key [0-255]	[0-255]	Specify a key to the selected interfaces.
Switch(config-if-PORT-PORT)# no channel-group lacp role		Specify the selected interfaces to passive LACP role.
Switch(config-if-PORT-PORT)# channel-group lacp role active	[active]	Specify the selected interfaces to active LACP role.
Switch(config-if-PORT-PORT)# channel-group trunking [group_name]	[group_name]	Specify the selected interfaces to the trunking group. **Note1 : At lease 2 ports but not more than 8 ports can be aggregated.** **Note2 : Ports can not be in LACP and port-trunking mode at the same time.** **Note3 : A port-trunking group need to created before assigning ports to it. (See Section 2.6.6 “channel-group”)**

No command		
Switch(config-if-PORT-PORT)# no channel-group lacp		Disable LACP on the selected interfaces.
Switch(config-if-PORT-PORT)# no channel-group trunking		Remove the selected ports from a link aggregation group.

4. Set up port description.

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

5. Set up port duplex mode.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# duplex [full]	[full]	Configure port duplex as **full.**
No command		
Switch(config-if-PORT-PORT)# no duplex		Configure port duplex as **half.** **Note1 : Only 9-10 copper ports can be configured as half duplex.** **Note2 : Auto-negotiation needs to be disabled before configuring duplex mode.**

6. Enable flow control operation.

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

7. Setup DHCP snooping/relay sub-commands

Command	Parameter	Description
Switch(config-if-PORT-PORT)# ip dhcp snooping option		Enable the selected interfaces' DHCP Option 82 / DHCPv6 Option 37 relay agent.
Switch(config-if-PORT-PORT)# ip dhcp snooping circuit		Enable the selected interfaces' DHCP Option 82 / DHCPv6 Option 37 Manual Circuit Id.
Switch(config-if-PORT-PORT)# ip dhcp snooping circuit formatted		Enable Formatted 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. 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 trust		Enable the selected interfaces as DHCP Option 82 / DHCPv6 Option 37 trust ports.
Switch(config-if-PORT-PORT)# ip dhcp snooping server-trust		Enable the selected interfaces as DHCP/DHCPv6 server trust ports. **Note : A port / ports can not be configured as option 82 trust and server trust at the same time.**
No command		
Switch(config-if-PORT-PORT)# no ip dhcp snooping option		Disable the selected interfaces' DHCP Option 82 / DHCPv6 Option 37 relay agent.
Switch(config-if-PORT-PORT)# no ip dhcp snooping trust		Reset the selected interfaces back to non-DHCP 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-DHCP/DHCPv6 server trust ports.
Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit		Disable the selected interfaces' DHCP Option 82 / DHCPv6 Option 37 Manual Circuit Id.
Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit id		Clear DHCP Option 82 / DHCPv6 Option 37 Circuit Id.
Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit formatted		Disable Formatted Option 82 / DHCPv6 Option 37 Circuit Id for the selected interfaces.

8. Setup IGMP snooping/MLD sub-commands

Command	Parameter	Description
Switch(config-if-PORT-PORT)# ip igmp filter		Enable IGMP filter for the selected ports.
Switch(config-if-PORT-PORT)# ip igmp filter profile [profile_name]	[profile_name]	Assign the selected ports to an IGMP filter profile. **Note : Need to create an IGMP filter profile first under the igmp global configuration mode before assigning it.**
Switch(config-if-PORT-PORT)# ip igmp max-groups [1-512]	[1-512]	Specify the maximum groups number of multicast streams to the selected ports.
Switch(config-if-PORT-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.
	[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-PORT)# no ip igmp static-multicast-ip [E.F.G.H | E:F:G:H:I:J:K:L] vlan [1-4094]	[A.B.C.D | A:B:C:D:E:F:G:H]	Remove the specified IP/IPv6 address .
	[1-4094]	Remove the specified VLAN ID.

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-PORT)# ip sourceguard static-ip [A.B.C.D | A:B:C:D:E:F:G:H] vlan [1-4094]	[A.B.C.D | A:B:C:D:E:F:G:H]	Add a static IP/IPv6 address to static IP address table.
	[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 setting back to the default (unlimited). **unlimited:** Non-Limited (Allows both static IP and DHCP-assigned IP). This is the default setting.

10. Enable loop-detection per port.

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

11. Configure MAC table learning and static MAC table.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# mac address-table static-mac [xx:xx:xx:xx:xx:xx] vlan [1-4094]	[xx:xx:xx:xx:xx:xx]	Specify a MAC address to VLAN entry.
	[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 learning function.
No command		
Switch(config-if-PORT-PORT)# no mac address-table static-mac [xx:xx:xx:xx:xx:xx] vlan [1-4094]	[xx:xx:xx:xx:xx:xx]	Remove the specified MAC address from the MAC address table.
	[1-4094]	Remove the VLAN to which the specified MAC belongs.
Switch(config-if-PORT-PORT)# no mac learning		Disable MAC learning function of the specified ports.

12. Configure media type.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# media-type [sfp]	[sfp]	Configure the media type of the selected port(s) as SFP.
No command		
Switch(config-if-PORT-PORT)# no media-type		Configure the media type of the selected port(s) as copper. **Note : Only port 9-10 can be configured as copper.**

13. Configure QoS rate limit.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# qos rate-limit ingress [500-1000000]	[0,500-1000000]	Configure the **ingress** rate limit, from 500Kbps to 1000Mbps. 0:Disable
Switch(config-if-PORT-PORT)# qos rate-limit egress [500-1000000]	[0,500-1000000]	Configure the **egress** rate limit, from 500Kbps to 1000Mbps. 0:Disable
No command		
Switch(config-if-PORT-PORT)# no qos rate-limit ingress		Disable QoS ingress rate limit setting.
Switch(config-if-PORT-PORT)# no qos rate-limit egress		Disable QoS egress rate limit setting.

14. 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.

15. Configure RSTP parameters per port.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# spanning-tree		Enable spanning-tree protocol on the selected interfaces.
Switch(config-if-PORT-PORT)# spanning-tree cost [0-200000000]	[0-200000000]	Specify the path cost value on the selected interfaces.
Switch(config-if-PORT-PORT)# spanning-tree priority [0-15]	[0-15]	Specify priority value on the selected interfaces. **0=0, 1=16, 2=32, 3=48, 4=64, 5=80, 6=96, 7=112, 8=128, 9=144, 10=160, 11=176,12=192, 13=208, 14=224, 15=240**
Switch(config-if-PORT-PORT)# spanning-tree edge		Set the selected interfaces to edge ports.
Switch(config-if-PORT-PORT)# spanning-tree p2p [forced_true|forced_false|auto]	[forced_true|forced_false|auto]	Set the selected interfaces to non-point to point ports (forced_false) or allow the Managed Switch to detect point to point status automatically (auto). By default, physical ports are set to point to point ports (forced_true).
No command		
Switch(config-if-PORT-PORT)# no spanning-tree		Disable spanning-tree protocol on the selected interfaces.
Switch(config-if-PORT-PORT)# no spanning-tree cost		Reset the cost value back to the default.
Switch(config-if-PORT-PORT)# no spanning-tree priority		Reset the priority value back to the default.
Switch(config-if-PORT-PORT)# no spanning-tree edge		Reset the selected interfaces back to non-edge ports.

Switch(config-if-PORT-PORT)# no spanning-tree p2p		Reset the selected interfaces back to point to point ports (forced_ true).

16. Set up port speed.

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

17. Set up VLAN parameters per port.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# vlan dot1q-vlan access-vlan [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' Access-VLAN ID (PVID).
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 port. (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 access-vlan		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 back to the default setting (Access Mode).
Switch(config-if-PORT-PORT)# no vlan port-based [name]	[name]	Remove the selected ports from the specified port-based VLAN.

18. Set up MAC Limit.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# security mac-limit		Enable MAC Limit function of the selected port(s).
Switch(config-if-PORT-PORT)# security mac-limit maximum [0-1024]	[0-1024]	Specify the number of MAC address that can be learned. "0" indicates there is no limit on specified ports. The valid range of number that can be configured is 0~1024.
No Command		
Switch(config-if-PORT-PORT)# no security mac-limit		Disable MAC Limit function of the selected port(s).
Switch(config-if-PORT-PORT)# no security mac-limit maximum		Reset the MAC Limit back to the default "0". "0" indicates there is no limit on specified ports.

2.6.28 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.

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

2.6.29 Show sfp Command

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

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

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

Command	Description
Switch(config)# show running-config	Show configurations currently used in the Manged Switch. Please note that you must save running configurations into your switch flash before rebooting or restarting the device.
Switch(config)# show start-up-config	Display system configurations that are stored in flash.
Switch(config)# show default-config	Display the system factory default configuration.

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 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.

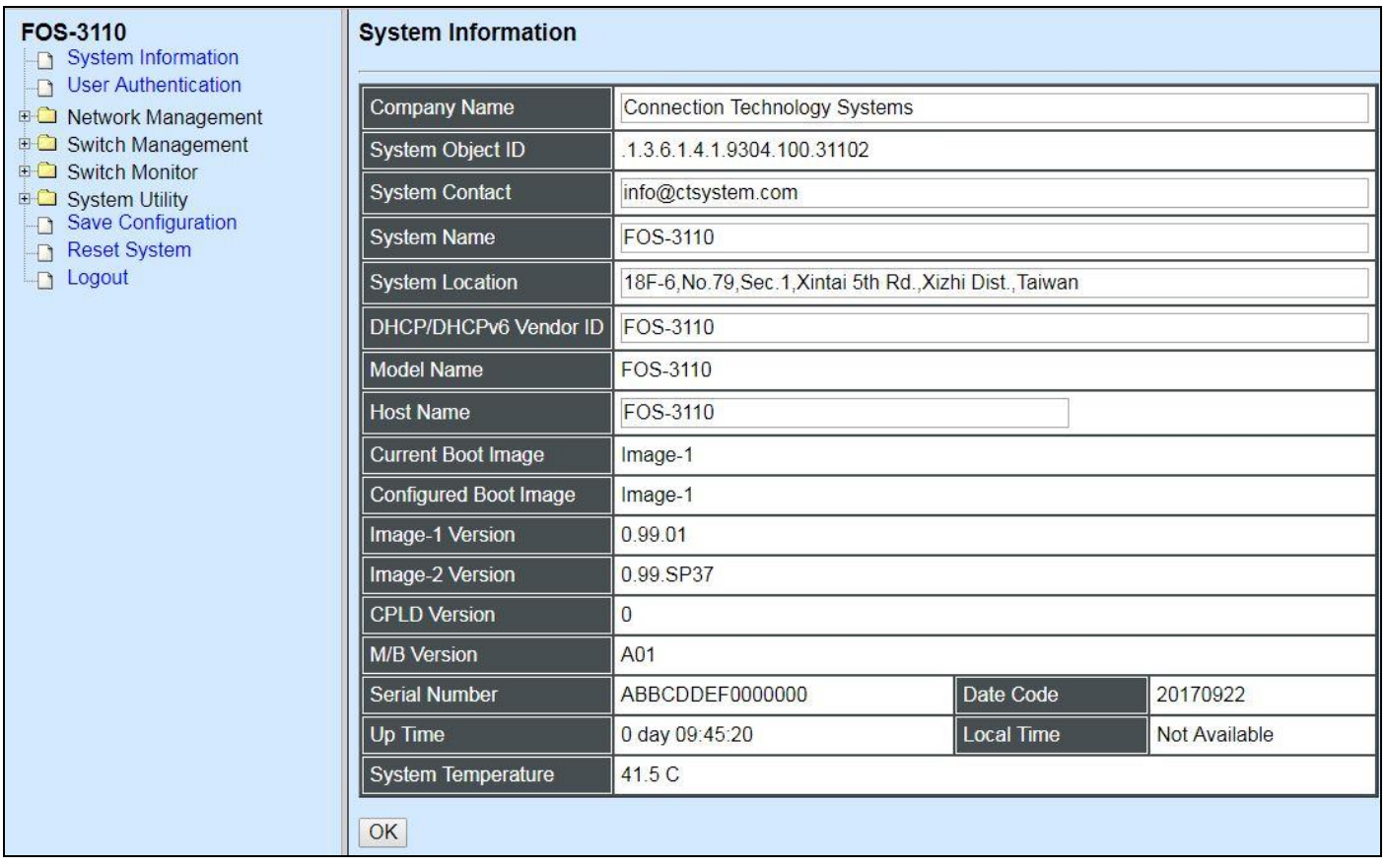
Please refer to the appropriate documentation for the instructions of installing the system private MIB.

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.

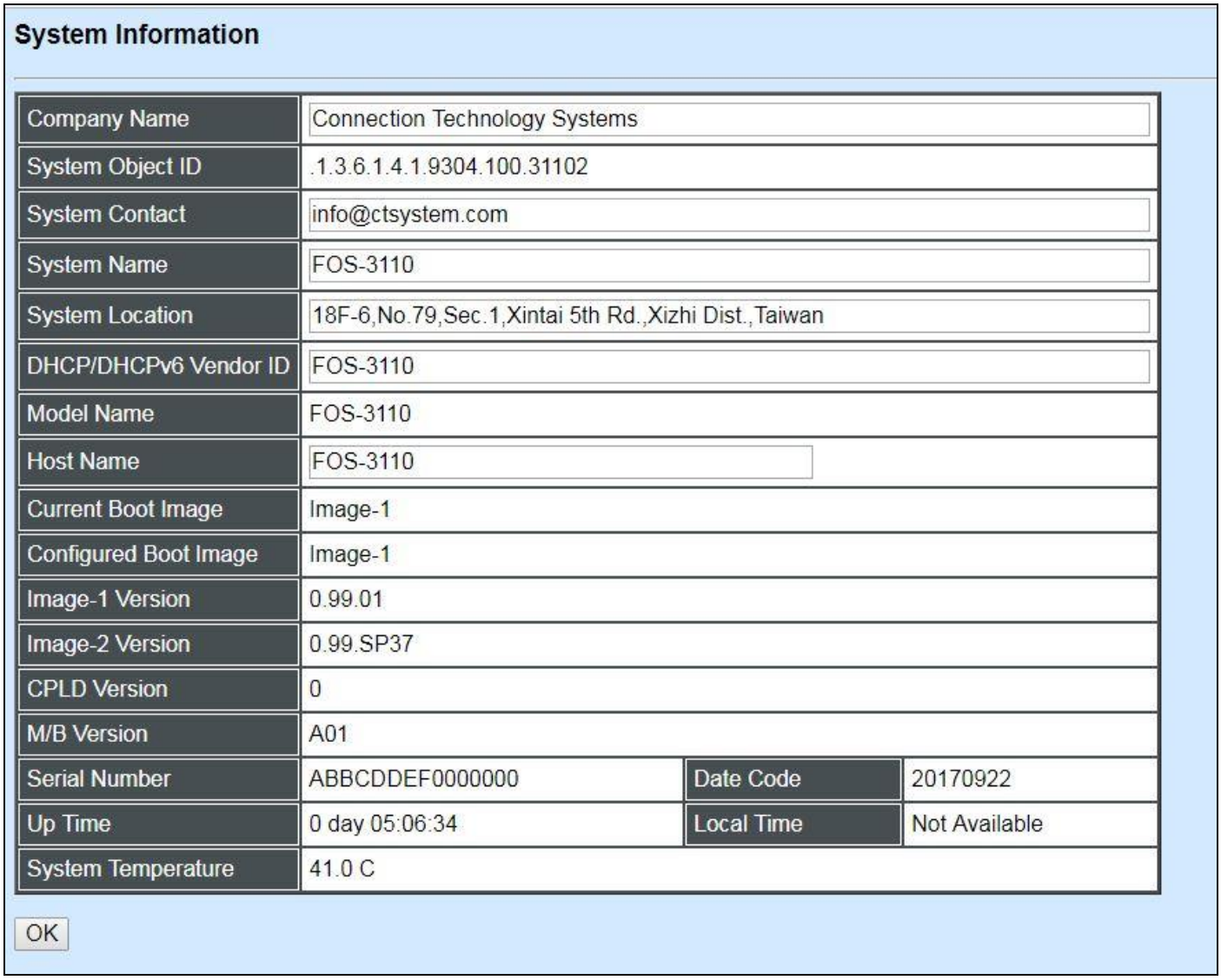


In the Main Menu, there are nine main functions, including System Information, User Authentication, Network Management, Switch Management, Switch Monitor, System Utility, Save Configuration, Reset System and Logout contained. We will respectively describe their sub-functions in the following sections of this chapter.

- **System Information:** Name the Managed Switch, specify the location and check the current version of information.
- **User Authentication:** View the registered user list. Add a new user or remove an existing user.
- **Network Management:** Set up or view the Managed Switch's IP address and related information required for network management applications.
- **Switch Management:** Set up the switch/port configuration, VLAN configuration and other functions.
- **Switch Monitor:** View the operation status and traffic statistics of the ports.
- **System Utility:** Ping, do the firmware upgrade, load the factory default settings, etc..
- **Save Configuration:** Save all changes to the system.
- **Reset System:** Reset the Managed Switch.
- **Logout:** Log out the management interface.

4.1 System Information

Select **System Information** from the **Main 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.

DHCP/DHCPv6 Vendor ID: Enter the Vendor Class Identifier used for DHCP/DHCPv6 relay agent function.

Model Name: Display the product's model name.

Host Name: Enter the product's host name.

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.

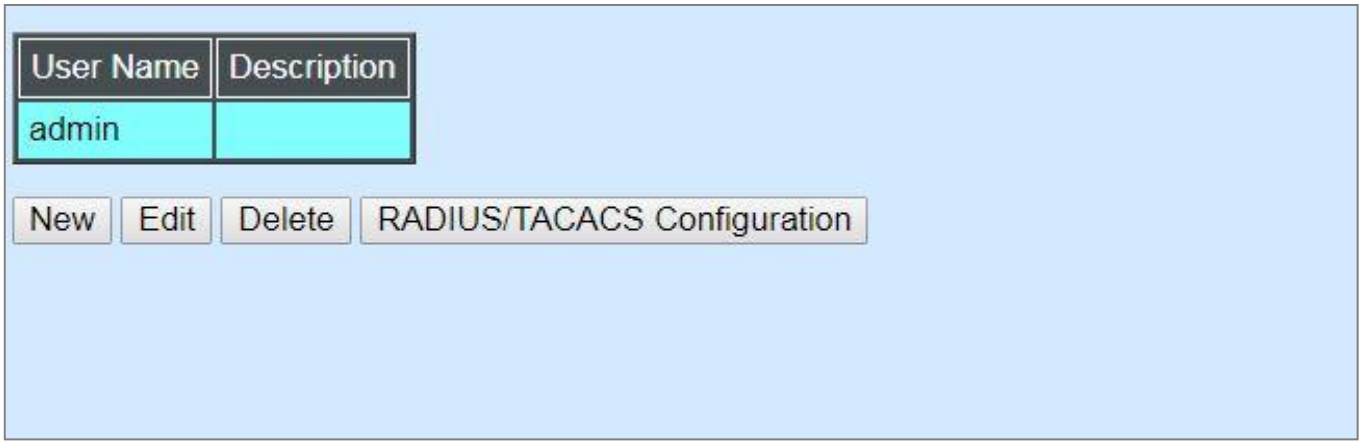
System Temperature: Display the temperature of the device.

4.2 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 **User Authentication** from the **Main 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. The default setting is disabled.

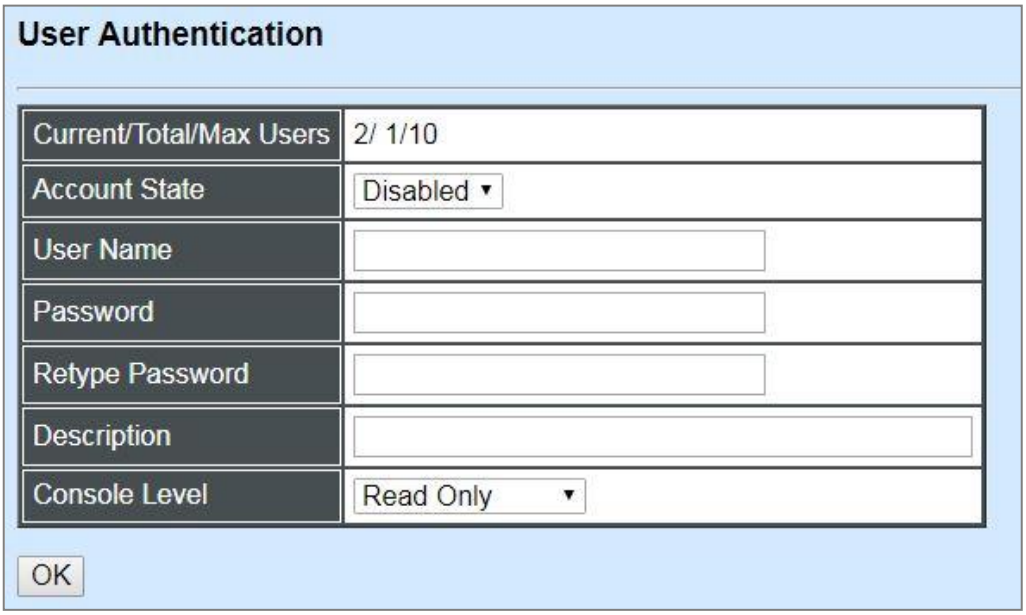


Click **New** to add a new user and then the following screen page appears. Up to 10 users can be registered.

Click **Edit** to modify a registered user's settings.

Click **Delete** to remove the selected registered user from the user list.

Click **RADIUS/TACACS Configuration** for authentication setting via RADIUS/TACACS. For more details on these settings, please refer to Section 4.2.1.



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

Current: This shows the number of current registered user.

Total: This shows the amount of total users who have already registered.

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

Account State: Enable or disable this user account.

User Name: Specify the authorized user login name. Up to 20 alphanumeric characters can be accepted. Only 5 login accounts can be registered in this device at the same time.

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 the 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, system information and items under System Utility menu.

Read Only: Allow to view only.

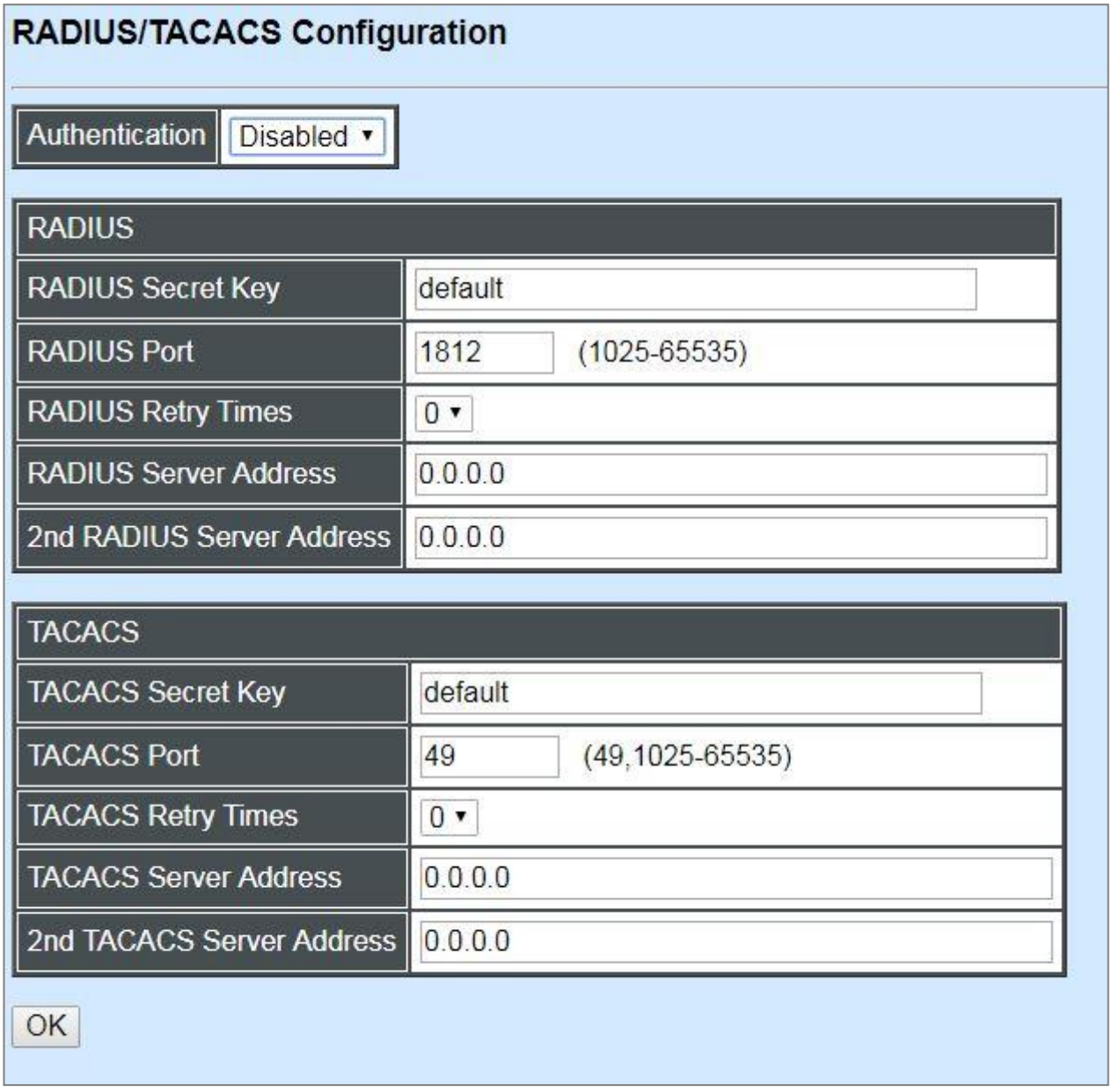
NOTE:

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.

4.2.1 RADIUS/TACACS Configuration

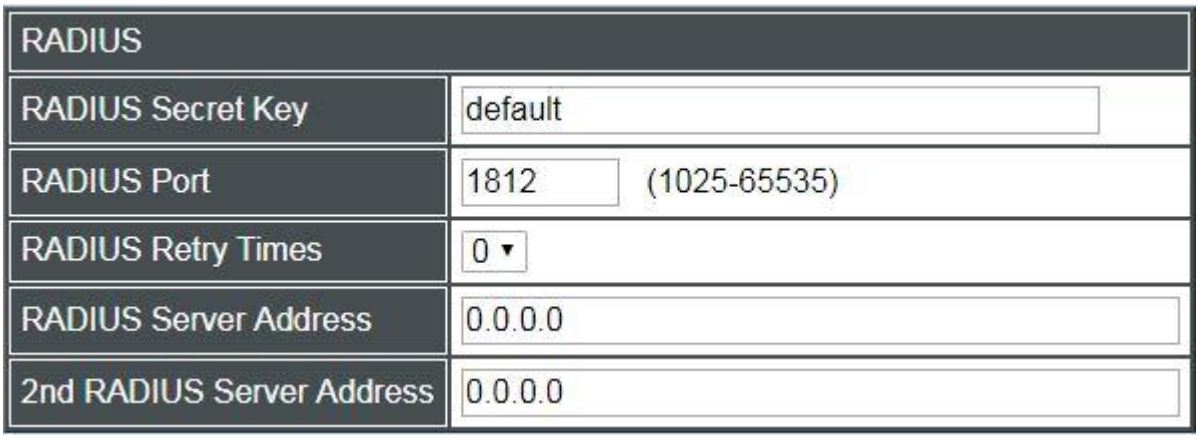
Click **RADIUS/TACACS Configuration** in the User Authentication webpage and then the following screen page appears.



Authentication: From the **Authentication** pull-down menu, you can choose **RADIUS** or **TACACS** option to respectively enable authentication via RADIUS or TACACS. 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.

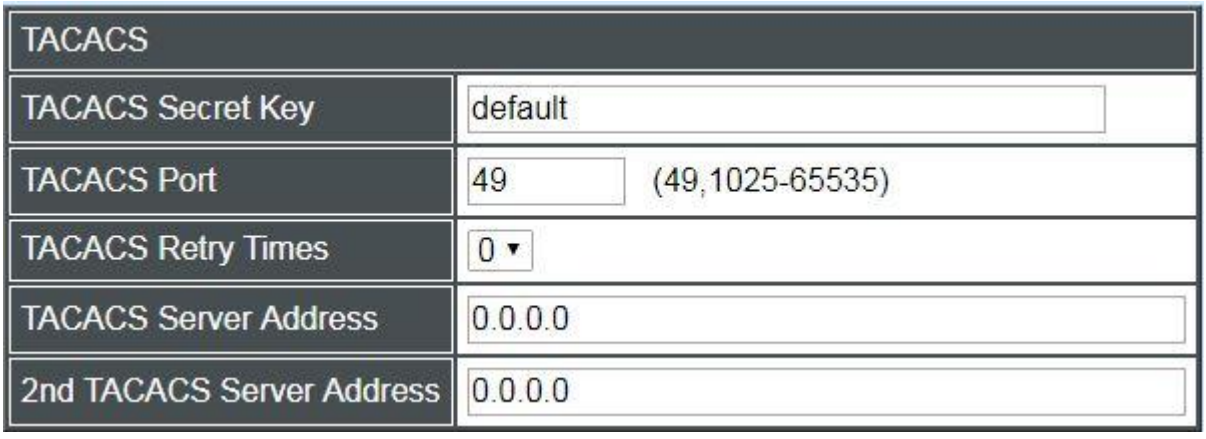
RADIUS Port: The RADIUS service port on RADIUS server.

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

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

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

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



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

TACACS Port: The TACACS service port on TACACS server.

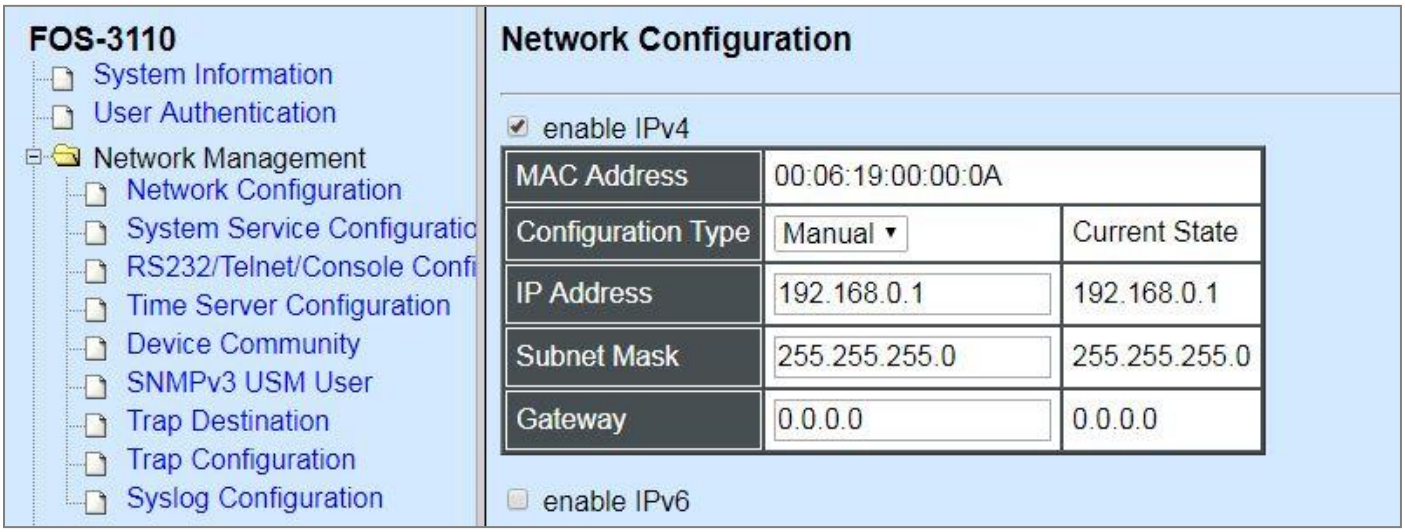
TACACS Retry Time: Times of trying to reconnect if the TACACS server is not reachable.

TACACS Server Address: IP address of the first TACACS server.

2nd TACACS Server Address: IP address of the secondary TACACS server.

4.3 Network Management

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



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

2. **System Service Configuration:** Enable or disable the specified network services.

3. **RS232/Telnet/Console Configuration:** View the RS-232 serial port setting, specific Telnet and Console services.

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

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

6. **SNMPv3 USM User:** Allow administrator to configure password and encryption method of user accounts generated in User Authentication for SNMPv3.

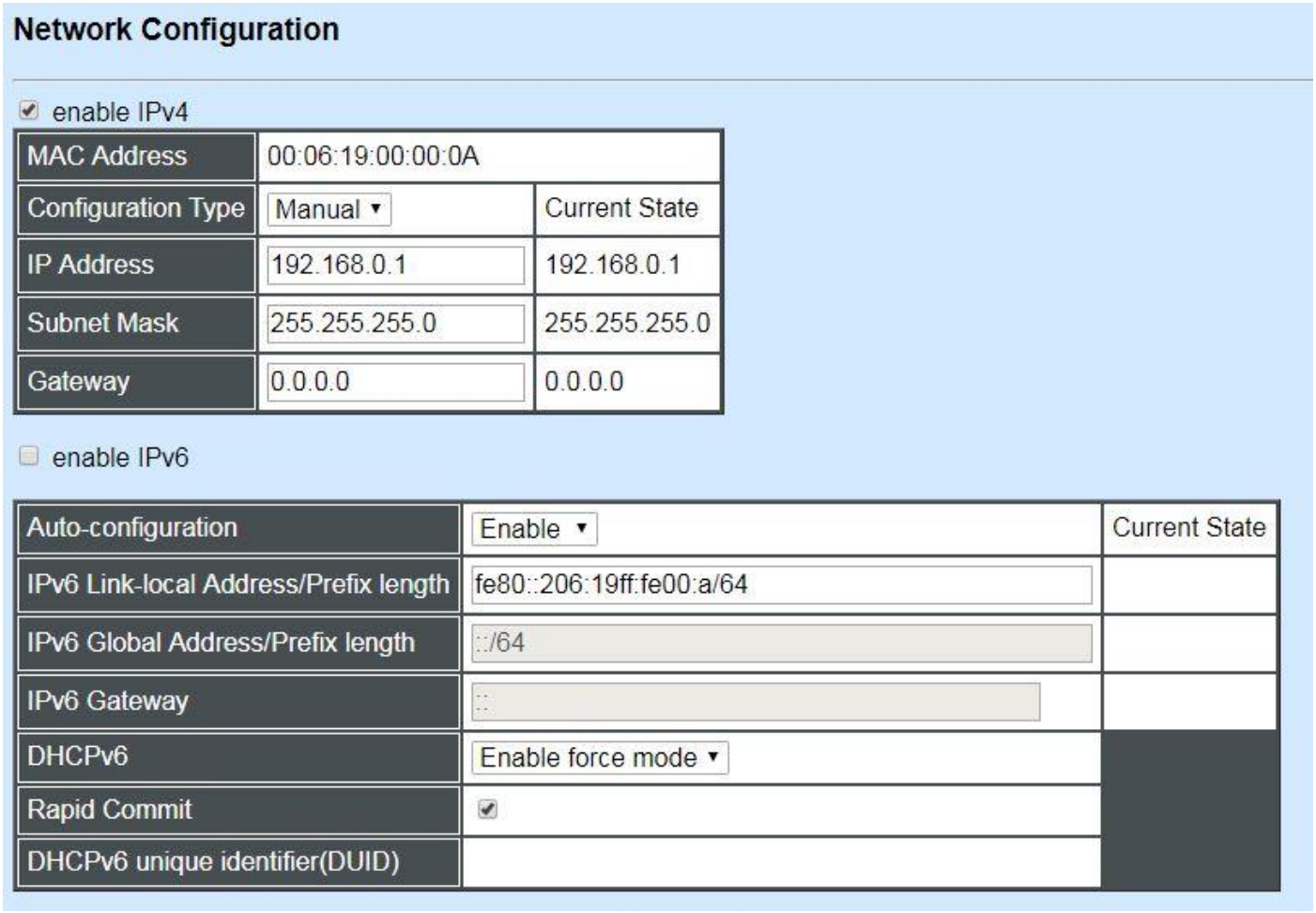
7. **Trap Destination:** View the registered SNMP trap destination list. Add a new trap destination or remove an existing trap destination.

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

9. **Syslog Configuration:** Set up the Mal-attempt Log server's configuration.

4.3.1 Network Configuration

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



Enable IPv4: Click the checkbox in front of **eable 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.

IP 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.

Enable IPv6: Click the checkbox in front of **eable 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

Disable: Disable DHCPv6.

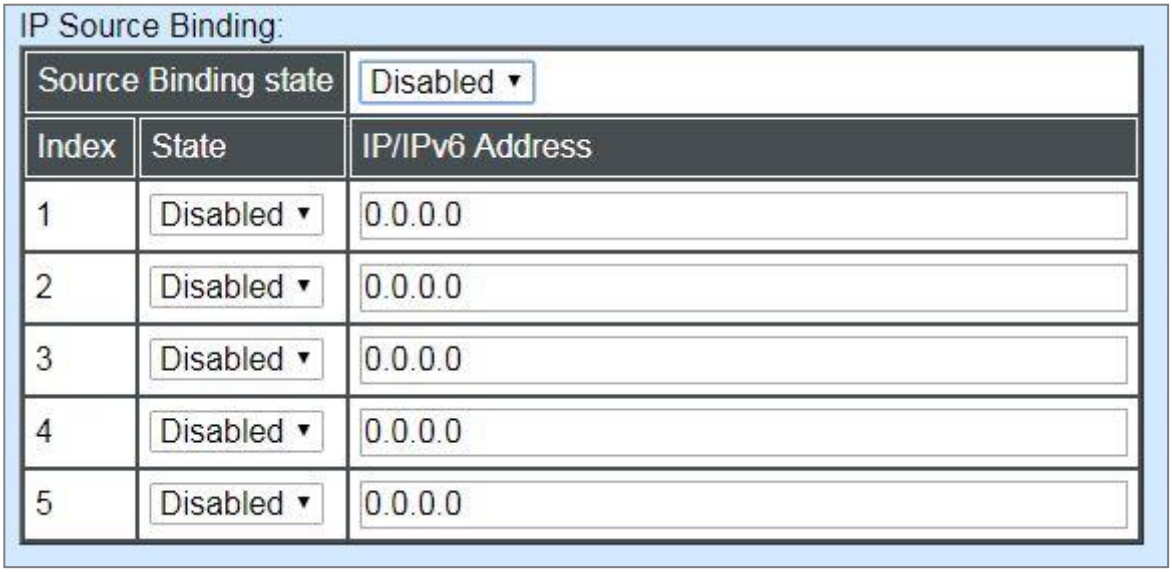
Enable auto mode: Configure DHCPv6 function in auto mode.

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 shows The DHCP Unique Identifier (DUID).

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



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

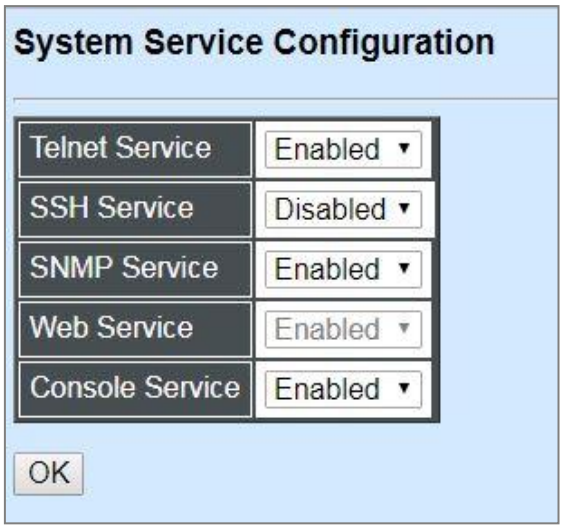
State: Disable or enable the assigned IP address to reach the management.

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

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 information about how to set up a DHCP server, please refer to APPENDIX B.*

4.3.2 System Service Configuration

Click the option **System Service Configuration** from the **Network 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.

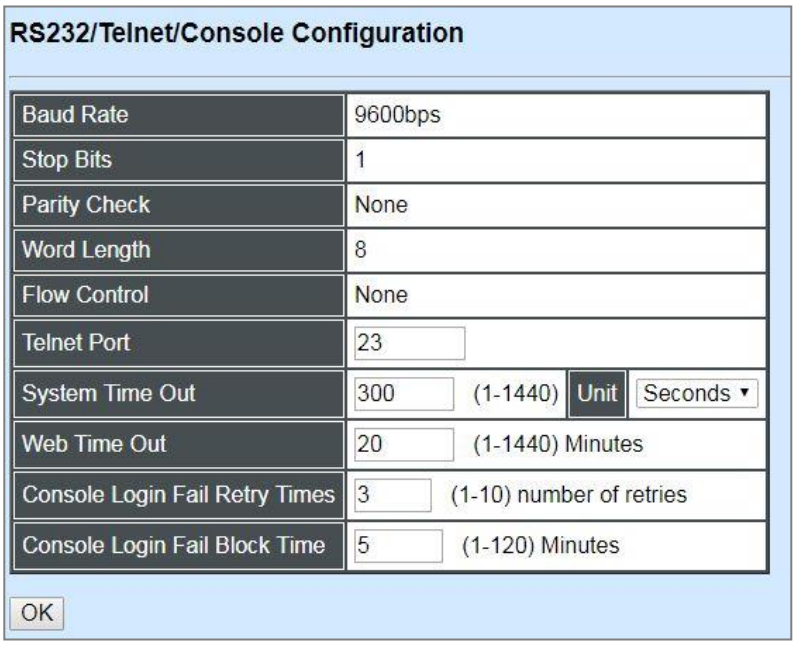
SNMP Service: To enable or disable the SNMP Management service.

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

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

4.3.3 RS232/Telnet/Console Configuration

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



Baud Rate: 9600 bps, RS-232 setting, view-only field.

Stop Bits: 1, RS-232 setting, view-only field.

Parity Check: None, RS-232 setting, view-only field.

Word Length: 8, RS-232 setting, view-only field.

Flow Control: None, RS-232 setting, view-only field.

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

System 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.

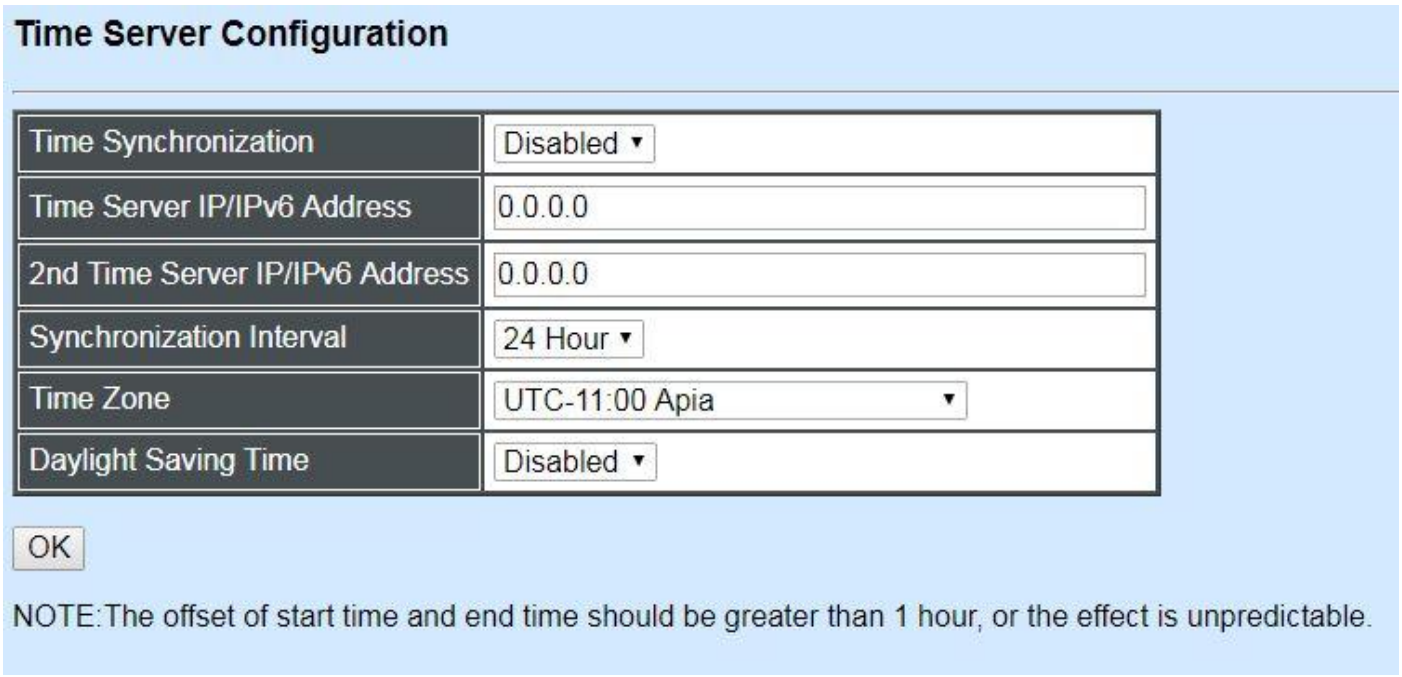
Web Time Out: Specify the desired time that the Managed Switch will wait before disconnecting an inactive web session. Valid range:1-1440 minutes.

Console Login Fail Retry Times: Specify the desired times that the Managed Switch will allow the user to retry to login the system via console if the console login fails. Valid range: 1-10

Console Login Fail Block Time: Specify the desired time that the Managed Switch will unblock the console for user's login if the accumulated retries times exceed the value you set up in **Console Login Fail Retry Times** parameter.

4.3.4 Time Server Configuration

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



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

Time Server IP/IPv6 Address: Set up the IP address of the first NTP time server.

2nd Time Server IP/IPv6 Address: Set up the IP 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"** and **"date"** 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" 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" option is selected in Daylight Saving Time, click the pull-down menu to select the end date of daylight saving time.

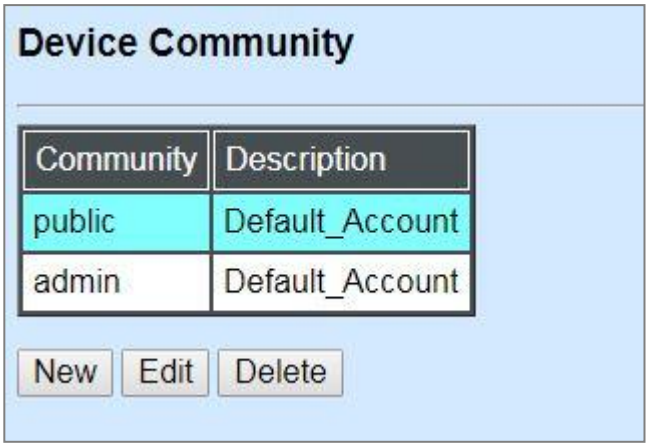
Daylight Saving Time Recurring Star: If the "recurring" option is selected in Daylight Saving Time, click the pull-down menu to select the recurring start date of daylight saving time.

Daylight Saving Time Recurring End If the "recurring" 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.*

4.3.5 Device Community

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



Click **New** to add a new community and then the following screen page appears. Up to 3 Device Communities can be created.

Click **Edit** to modify the current community settings.

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

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

Current: This shows the number of current registered community.

Total: This shows the amount of total registered communities.

Max Agents: This shows the maximum communities are available for registration. The maximum number is 3.

Account State: Enable or disable this Community Account.

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.

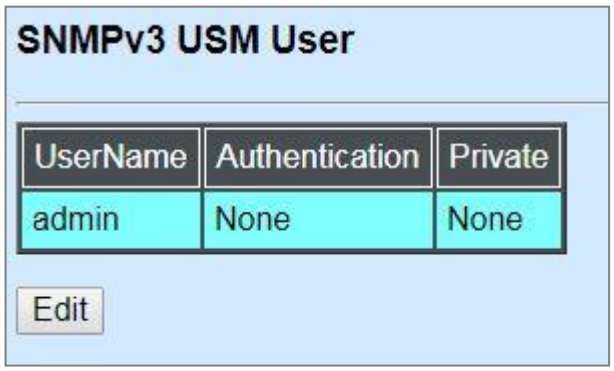
SNMP Level: Click the pull-down menu to select the desired privilege for the SNMP operation.

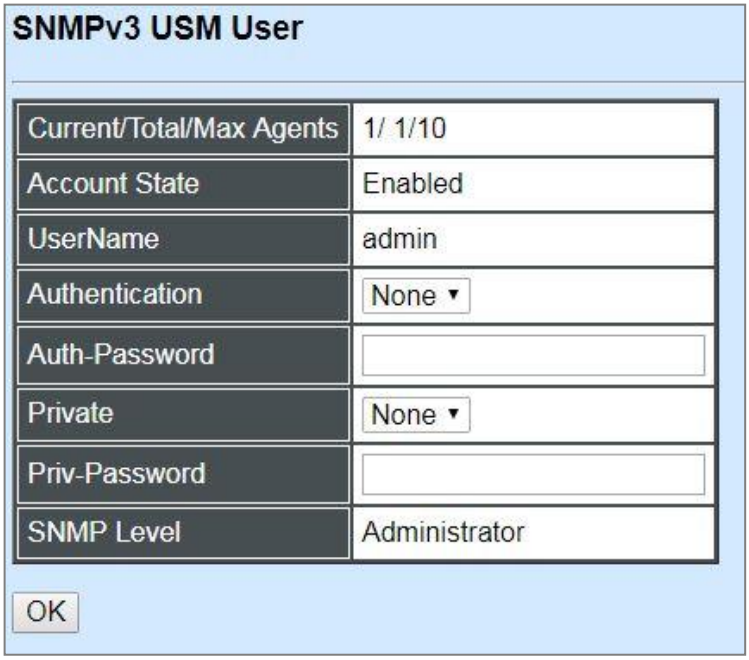
NOTE: *When the community browses the Managed Switch without proper access right, the Managed Switch will not respond. For example, if a community only has Read & Write privilege, then it cannot browse the Managed Switch's user table.*

4.3.6 SNMPv3 USM User

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

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





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

Current: This shows the number of current registered community.

Total: This shows the amount of total registered communities.

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

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

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

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

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

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

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

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

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

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

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

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

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

Administrator: 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.

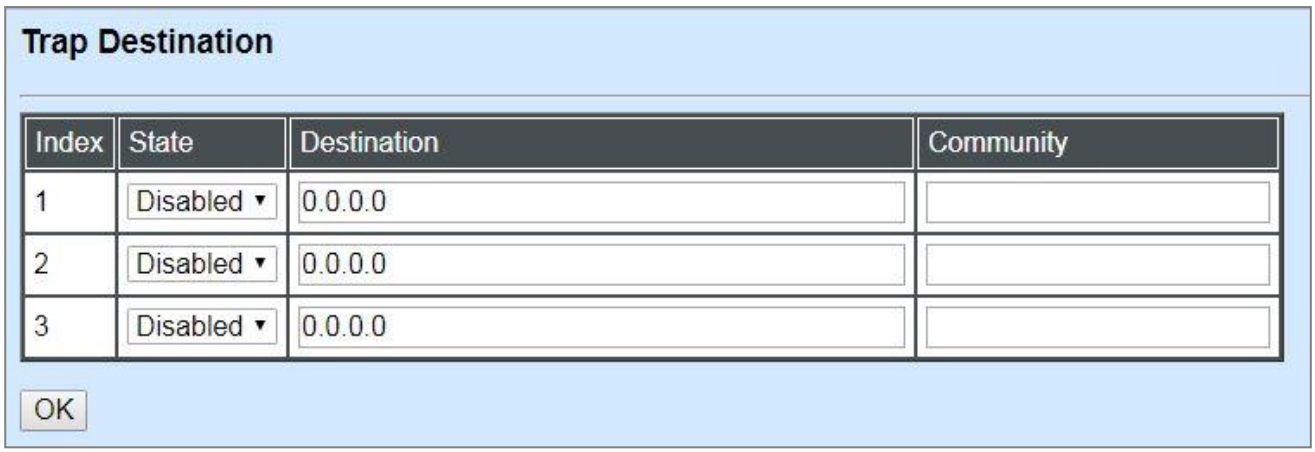
Read Only: Allow to view only.

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

4.3.7 Trap Destination

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



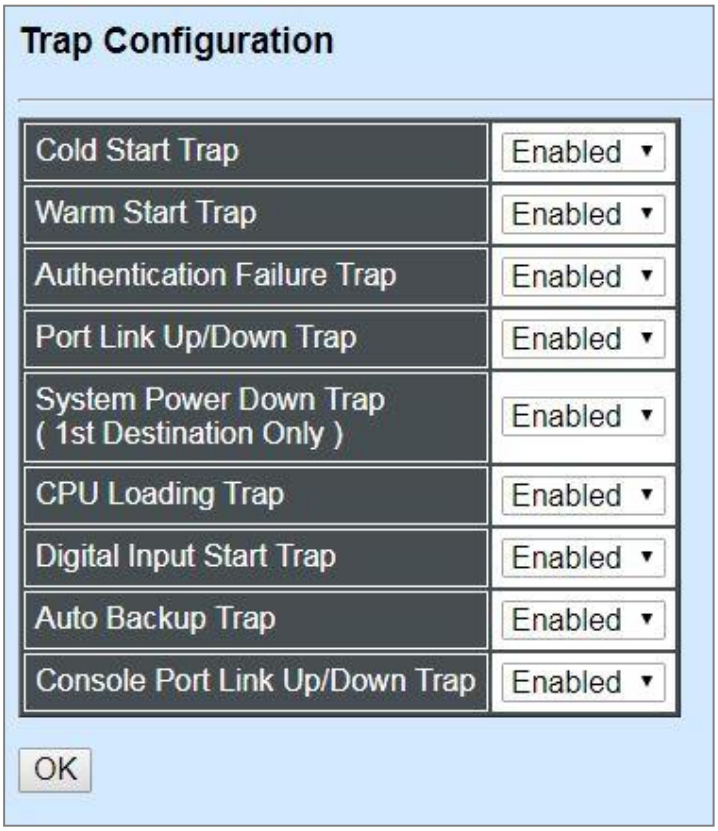
State: Enable or disable the function of sending trap to the specified destination.

Destination: Enter the specific IP address of the network management system that will receive the trap.

Community: Enter the description for the specified trap destination.

4.3.8 Trap Configuration

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



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.

System Power Down Trap(1st Destination Only): Enable or disable the Managed Switch to send a trap when the power failure occurs.

CPU Loading Trap: Enable or disable the Managed Switch to send a trap when the CPU is overloaded.

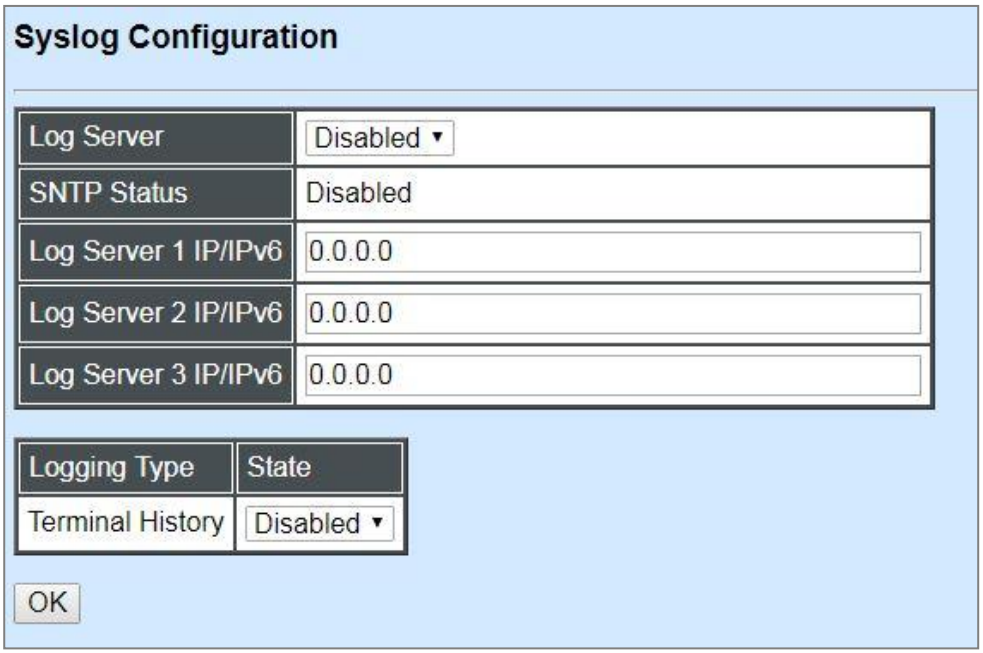
Digital Input Start Trap: Enable or disable the Managed Switch to send a trap when the alarm occurs.

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

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

4.3.9 Syslog Configuration

Click the option **Syslog Configuration** from the **Network Management** 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.

Log Server 1 IP/IPv6: Specify the default Log server IP/IPv6 address.

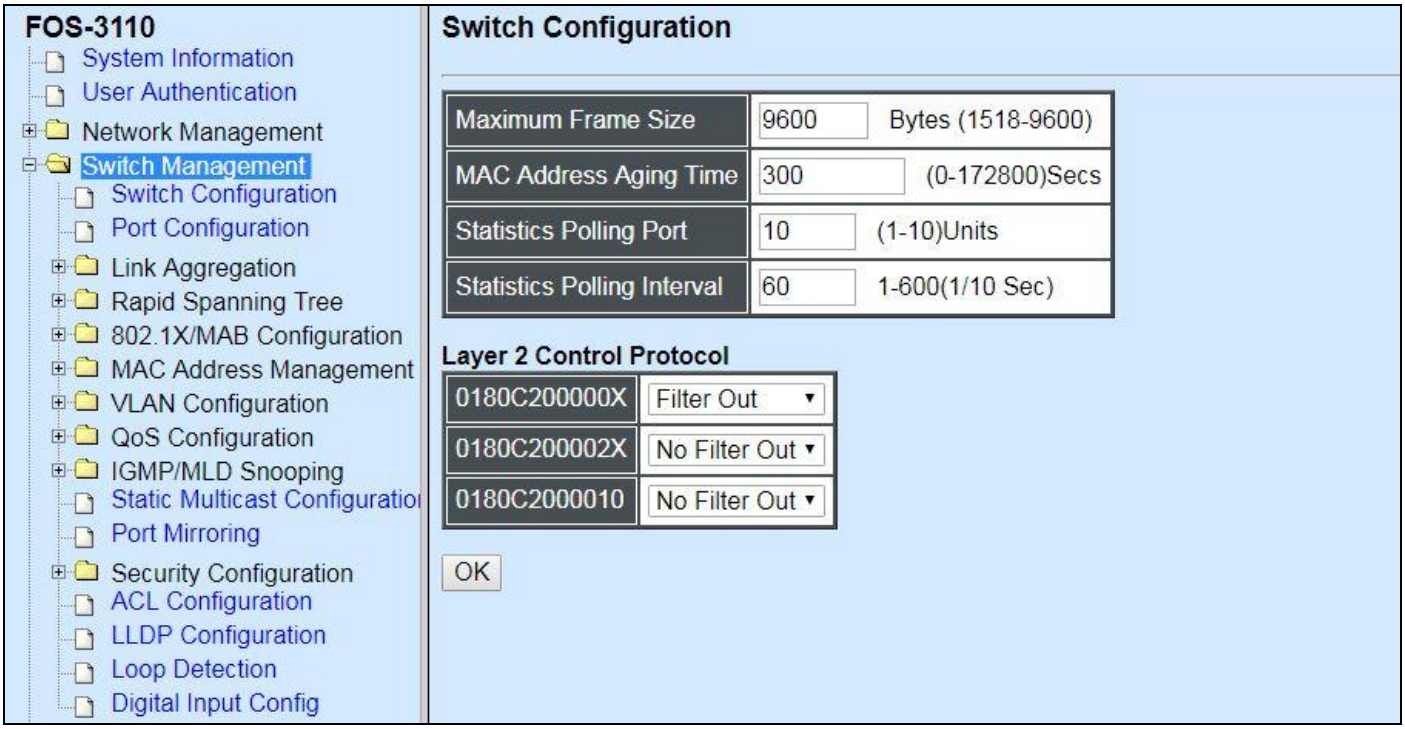
Log Server 2 IP/IPv6: Specify the secondary Log server IP/IPv6 address. When the default Log Server is down, the Managed Switch will automatically contact the second or third Log server.

Log Server 3 IP/IPv6: Specify the third Log server IP/IPv6 address. When the default Log Server is down, the Managed Switch will automatically contact the second or third Log server.

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

4.4 Switch Management

In order to manage the Managed switch and set up required switching functions, click the folder **Switch Management** from the **Main Menu** and then several options and folders will be displayed for your selection.



1. **Switch Configuration:** Set up frame size, address learning, etc.

2. **Port Configuration:** Enable or disable port speed, flow control, etc.

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

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

5. **802.1X/MAB Configuration:** Set up the 802.1X/MAB system, port Admin state, port reauthenticate.

6. **MAC Address Management:** Set up MAC address, enable or disable MAC security, etc.

7. **VLAN Configuration:** Set up VLAN mode and VLAN configuration.

8. **QoS Configuration:** Set up the priority queuing, rate limit and storm control.

9. **IGMP/MLD Snooping:** Configuring IGMP/MLD Snooping parameters.

10. **Static Multicast Configuration:** To create, edit or delete Static Multicast table.

11. **Port Mirroring:** Set up target port mirrors source port to enable traffic monitoring.

12. **Security Configuration:** Set up DHCP option 82 agent relay, port setting, filtering and static IP table configuration.

13. **Access Control List (ACL) Configuration:** Set up access control entries and lists.

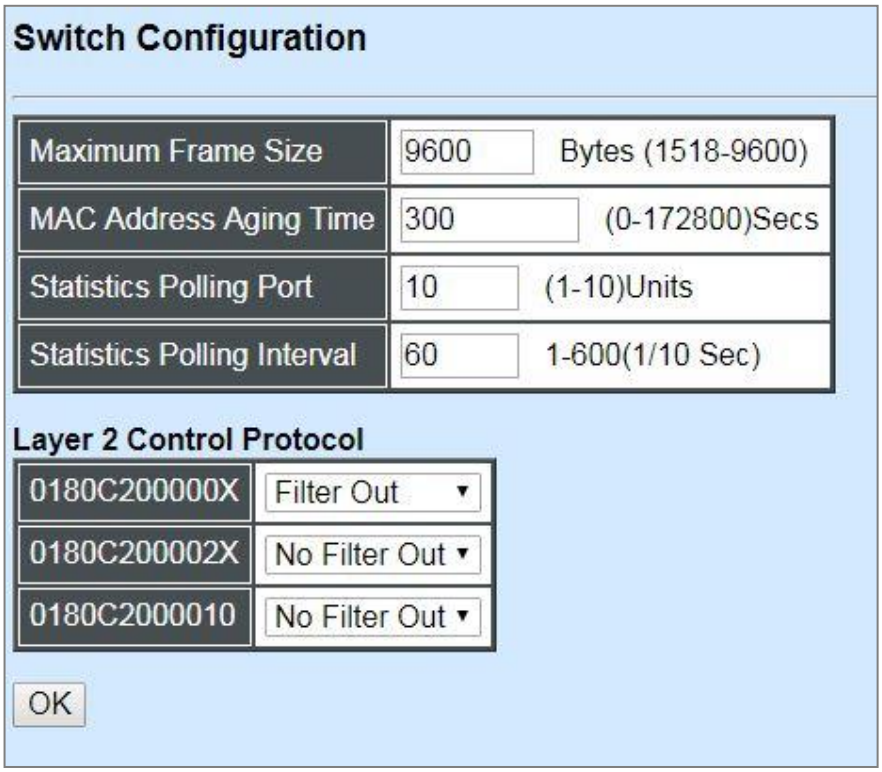
14. **LLDP Configuration:** Enable or disable LLDP on ports and set up LLDP-related attributes.

15. **Loop Detection Configuration:** Enable or disable Loop Detection function and set up Loop Detection configuration.

16. **Digital Input Configuration:** Set up the normal status of the digital input.

4.4.1 Switch Configuration

Click the option **Switch Configuration** from the **Switch 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 9600bytes.

MAC Address Aging Time: Specify MAC Address aging time between 0 and 172800 seconds. “0” means that MAC addresses will never age out.

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

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

For more details on the data statistics, you may refer to Section 4.5.3, 4.5.4 and 4.5.5 in this manual.

Layer 2 Control Protocol

0180C200000X: Select either “No Filter Out” or “Filter Out”. When “Filter Out” is selected, packets from the address ranging from 0180C2000000 to 0180C200000F will be dropped.

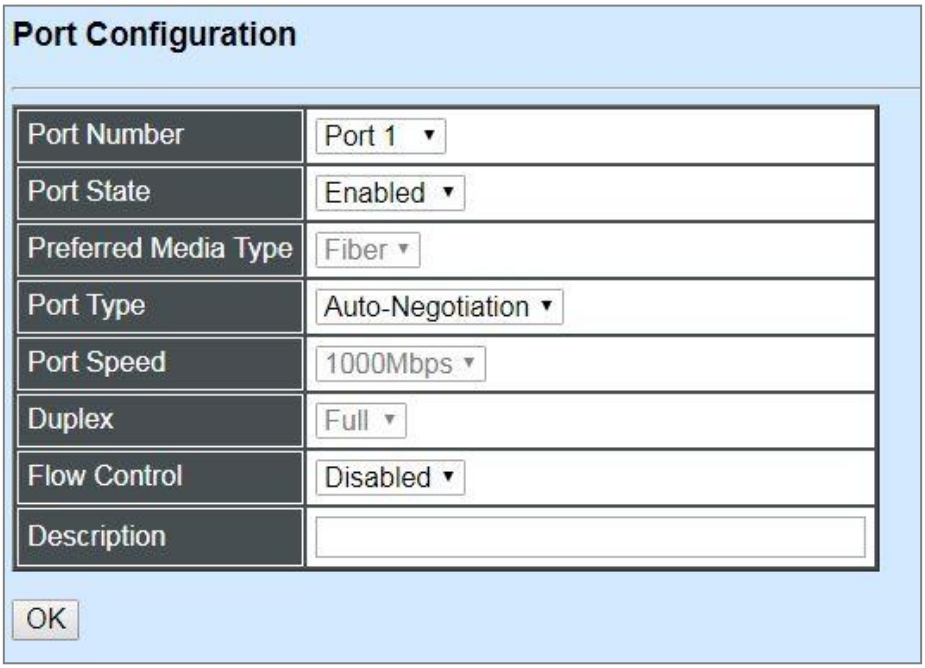
Multicast MAC addresses from 0180C2000000 to 0180C200000F are reserved for use by 802.1/802.3 protocols. The purpose for each multicast address is described briefly below:

0180C200002X: Select either “No Filter Out” or “Filter Out”. When “Filter Out” is selected, packets from the address ranging from 0180C2000020 to 0180C200002F will be dropped. Multicast addresses from 0180C2000020 to 0180C2000022 are for GMRP, GVRP, and GARP respectively.

0180C2000010: Select either “No Filter Out” or “Filter Out”. When “Filter” is selected, packets from the address 0180C2000010 will be dropped.

4.4.2 Port Configuration

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



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

Port State: Enable or disable the current port state.

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

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

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

Duplex: In TP ports with 10Mbps/100Mbps port speed and select “Manual” as port type, you can further specify the current operation Duplex mode (full or half duplex) of the port(s).

Flow Control: Enable or disable the flow control.

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

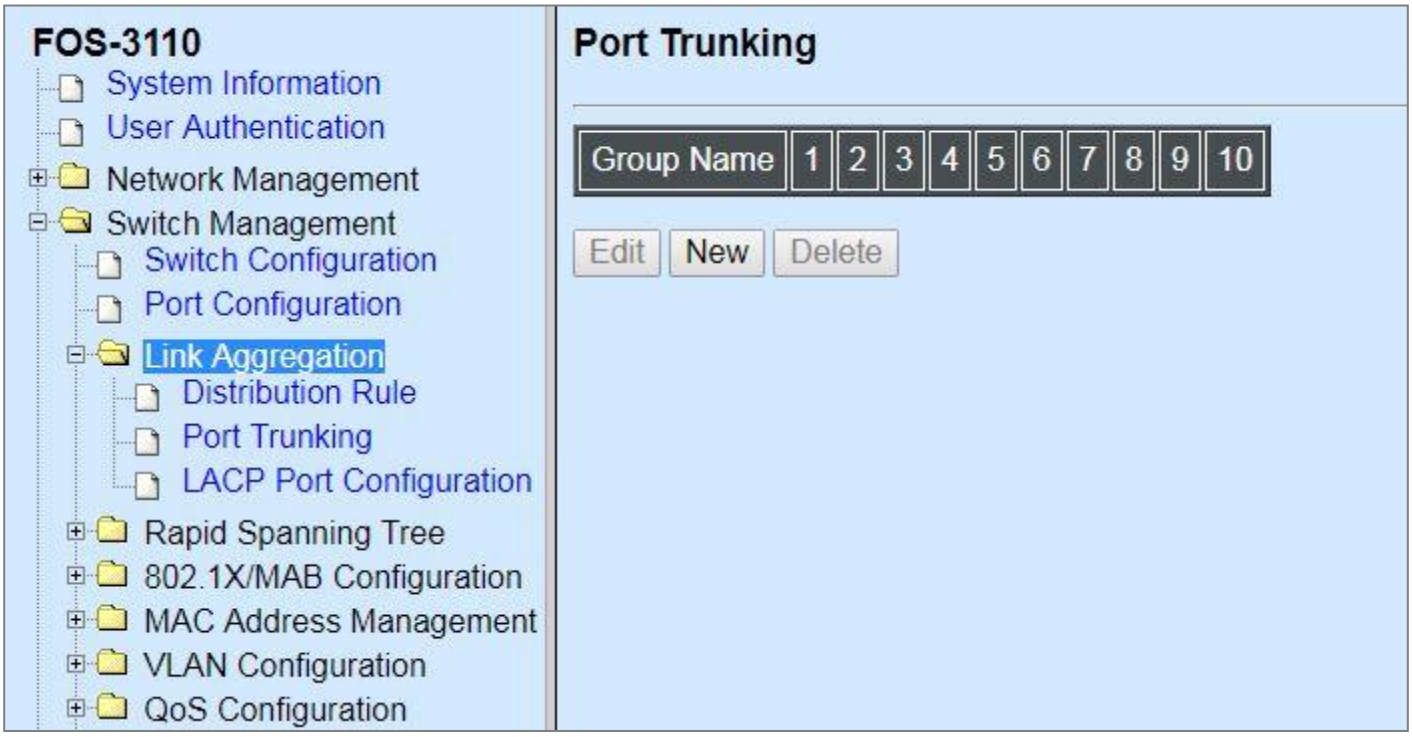
4.4.3 Link Aggregation

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

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

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

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



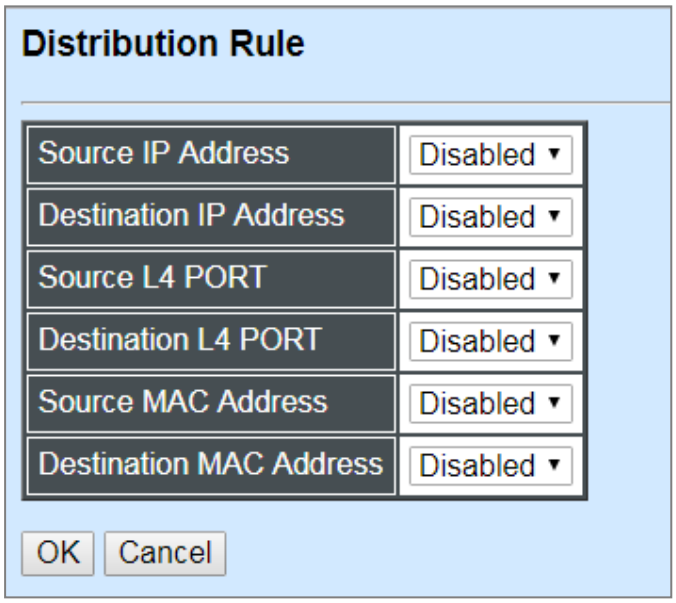
1. **Distribution Rule:** Configure the distribution rule of Port Trunking group(s).

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

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

4.4.3.1 Distribution Rule

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



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

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

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

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

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

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

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

4.4.3.2 Port Trunking

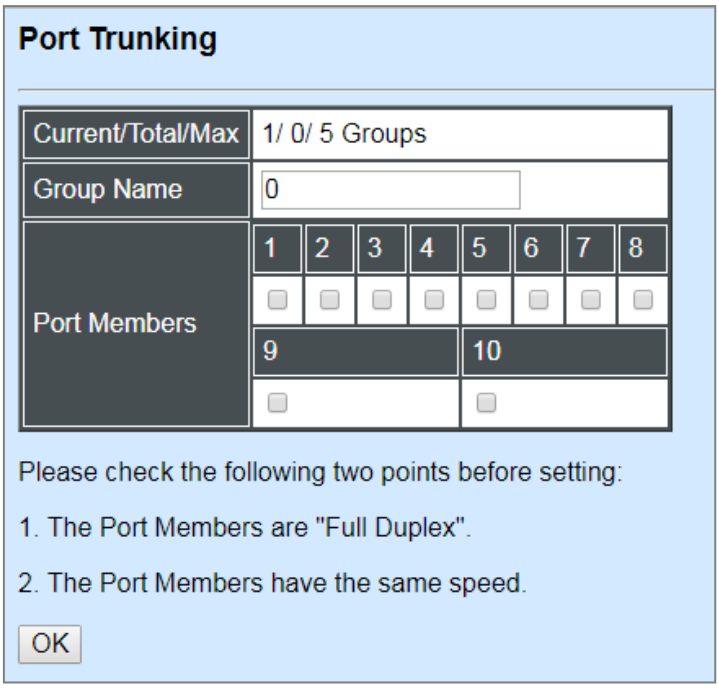
Click the option **Port Trunking** from the **Link Aggregation** menu and then the following screen page appears.

The Managed Switch allows users to create 5 trunking groups. Each group consists of 2 to 8 links (ports).

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

Click **Edit** to modify a registered trunking group's settings.

Click **Delete** to remove a specified registered trunking group and its settings.



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

Current: This shows the number of current registered group.

Total: This shows the amount of total registered groups.

Max: This shows the maximum number available for registration. The maximum number is 5.

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

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

- Must have 2 to 8 ports in each trunking group.

- Each port can only be grouped in one group.

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

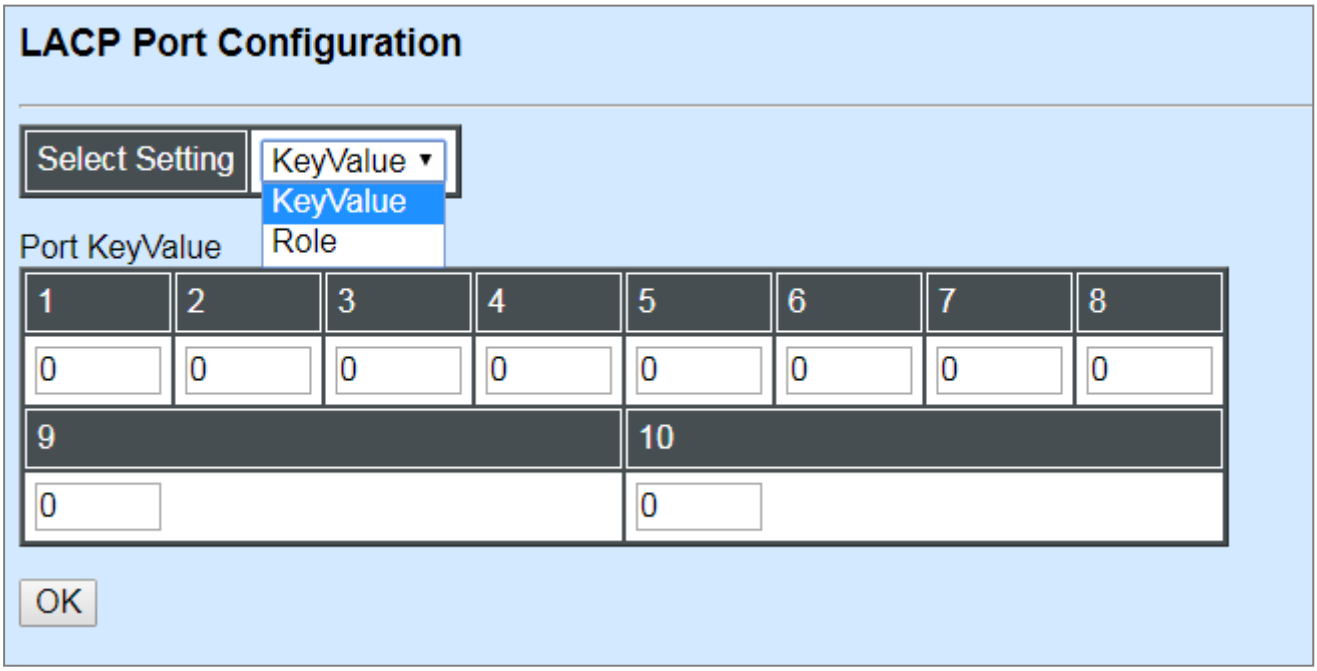
Click **OK** and return to **Link Aggregation** menu.

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

4.4.3.3 LACP Port Configuration

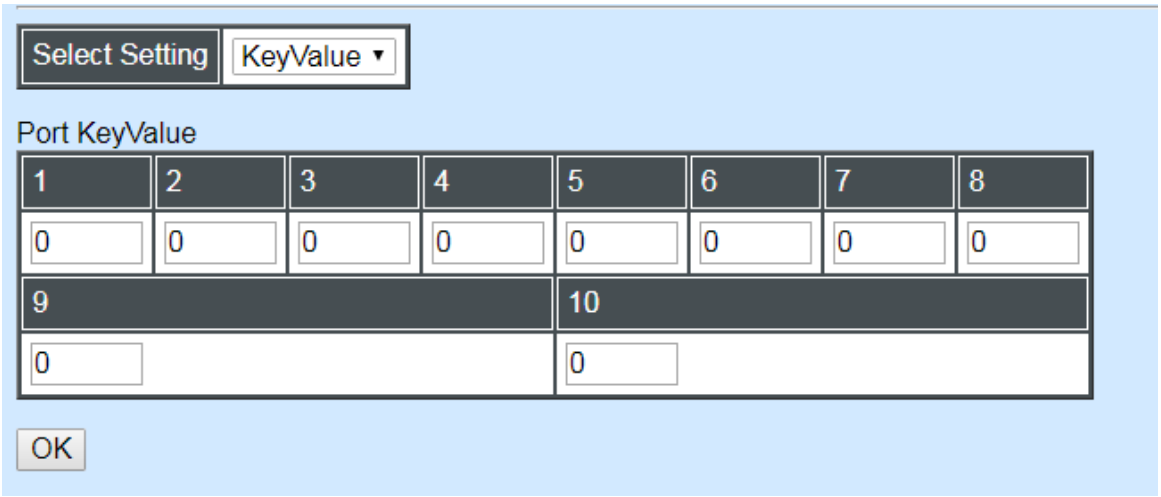
The Managed Switch supports dynamic Link Aggregation Control Protocol (LACP) which is specified in IEEE 802.3ad. Static trunks have to be manually configured at both ends of the link. In other words, LACP configured ports can automatically negotiate a trunked link with LACP configured ports on other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

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



Configure Key Value:

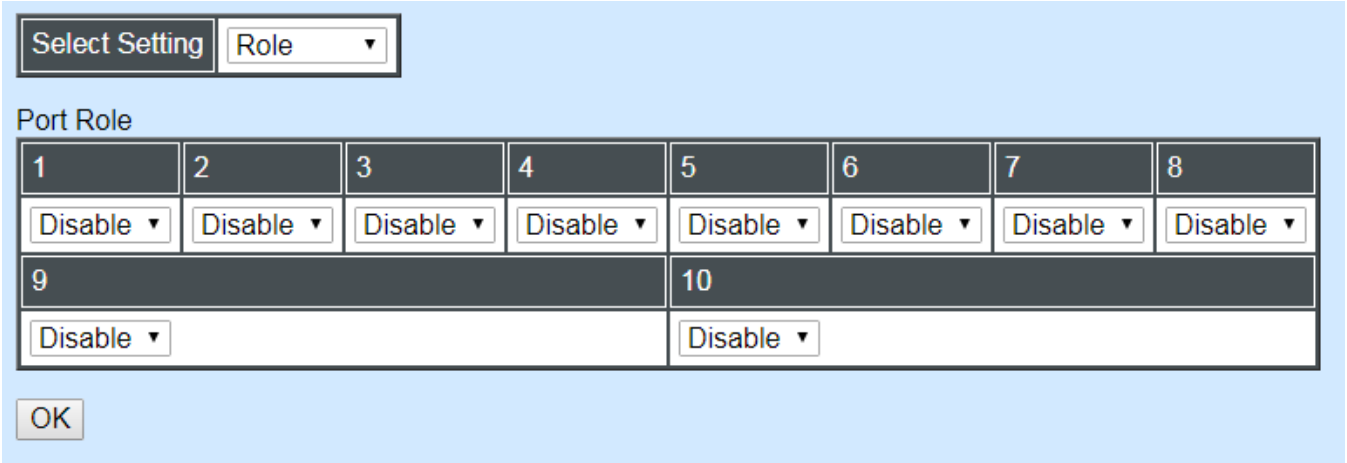
Select “Key Value” from the pull-down menu of Select Setting.



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

Configure Port Role:

Select “Role” from the pull-down menu of Select Setting. This allows LACP to be enabled (active or passive) or disabled on each port.



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

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

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

4.4.4 Rapid Spanning Tree

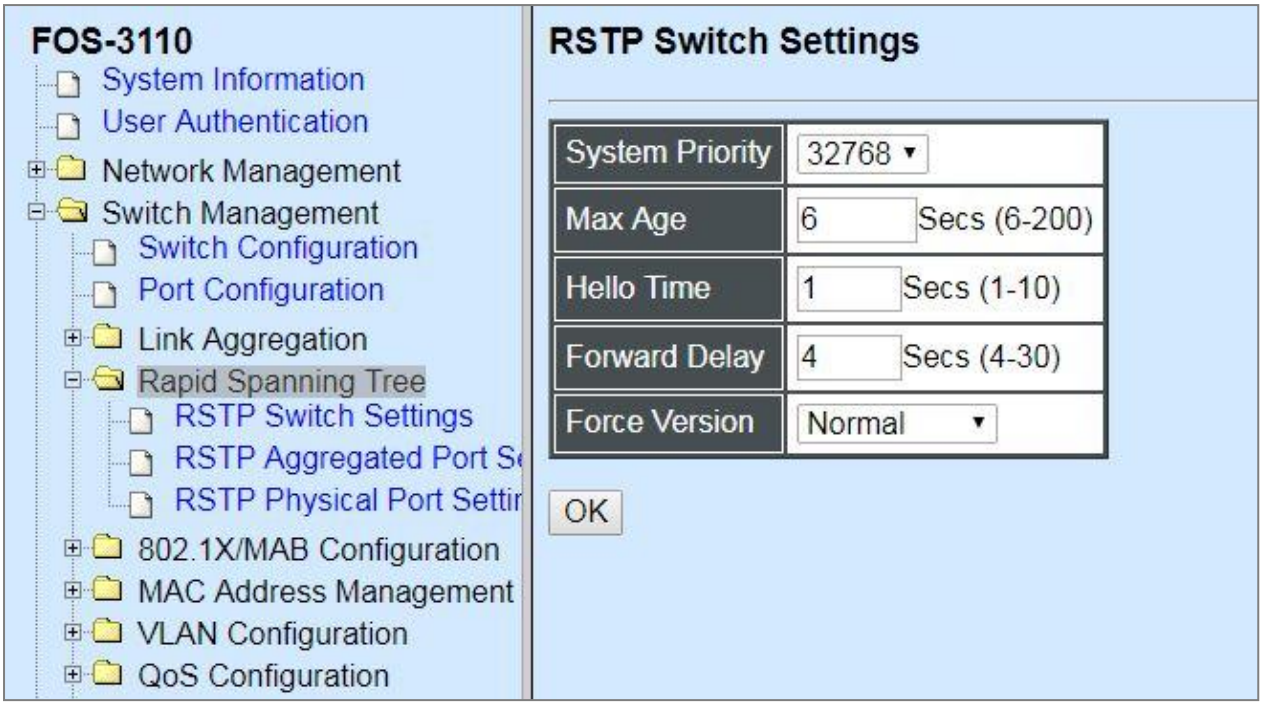
The Spanning Tree Protocol (STP), defined in the IEEE Standard 802.1D, creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches) and disables the links which are not part of that tree, leaving a single active path between any two network nodes.

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

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

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

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



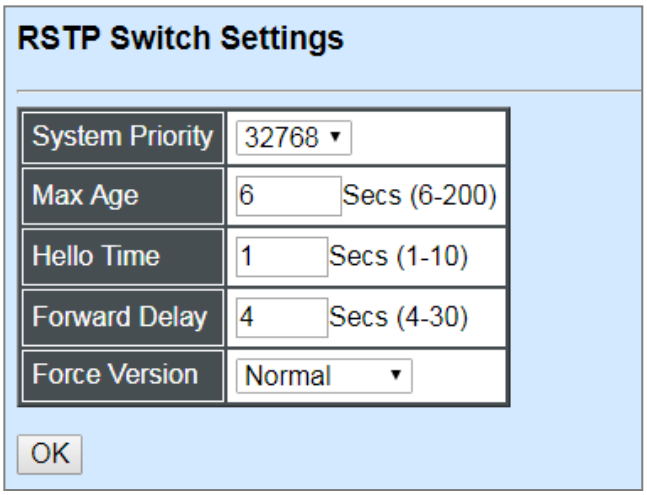
1. **RSTP Switch Settings:** Set up the system priority, max Age, hello time, forward delay time and force version.

2. **RSTP Aggregated Port Settings:** Set up the RSTP state, path cost, priority, edge status, and point to point setting of aggregated groups.

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

4.4.4.1 RSTP Switch Settings

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



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

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

Max Age: If another switch in the spanning tree does not send out a hello packet for a long period of time, it is assumed to be disconnected. The default Max. Age is 6 seconds.

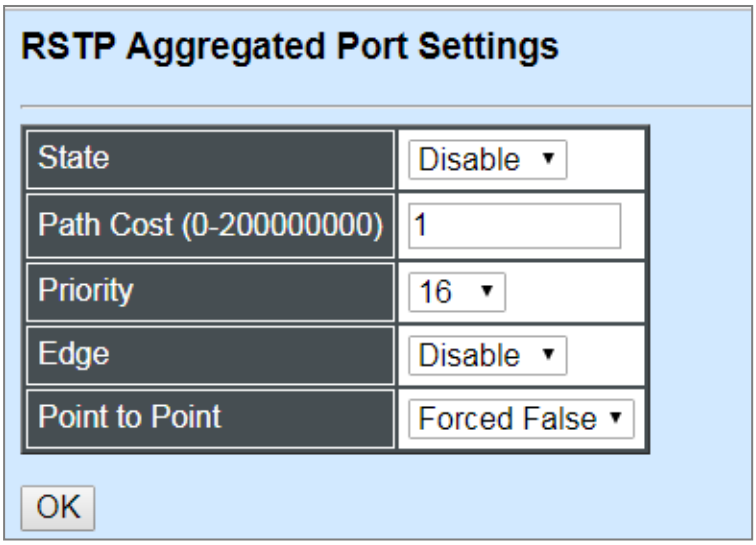
Hello Time: Periodically, a hello packet is sent out by the Root Bridge and the Designated Bridges that are used to communicate information about the topology throughout the entire Bridged Local Area Network.

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

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

4.4.4.2 RSTP Aggregated Port Settings

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



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

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

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

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

Point to Point:

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

Forced False: the port cannot have P2P status.

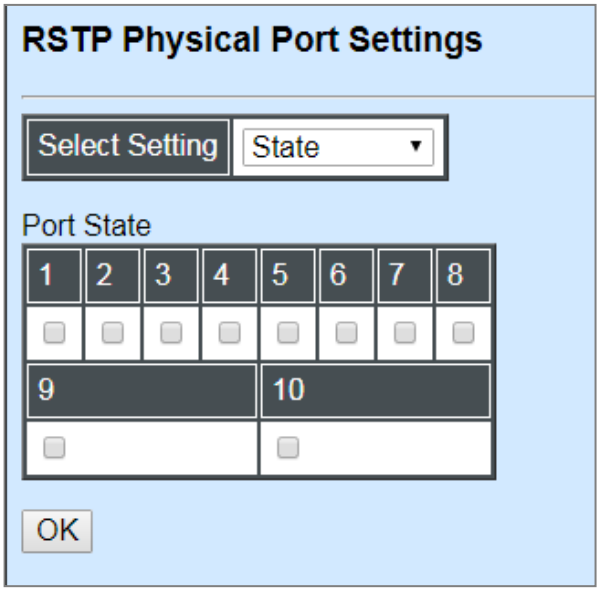
Auto: allows the port to have P2P status whenever possible and operates as if the P2P status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the P2P status changes to operate as if the P2P value were false. The default setting for this parameter is true.

4.4.4.3 RSTP Physical Port Settings

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

Configure Port State:

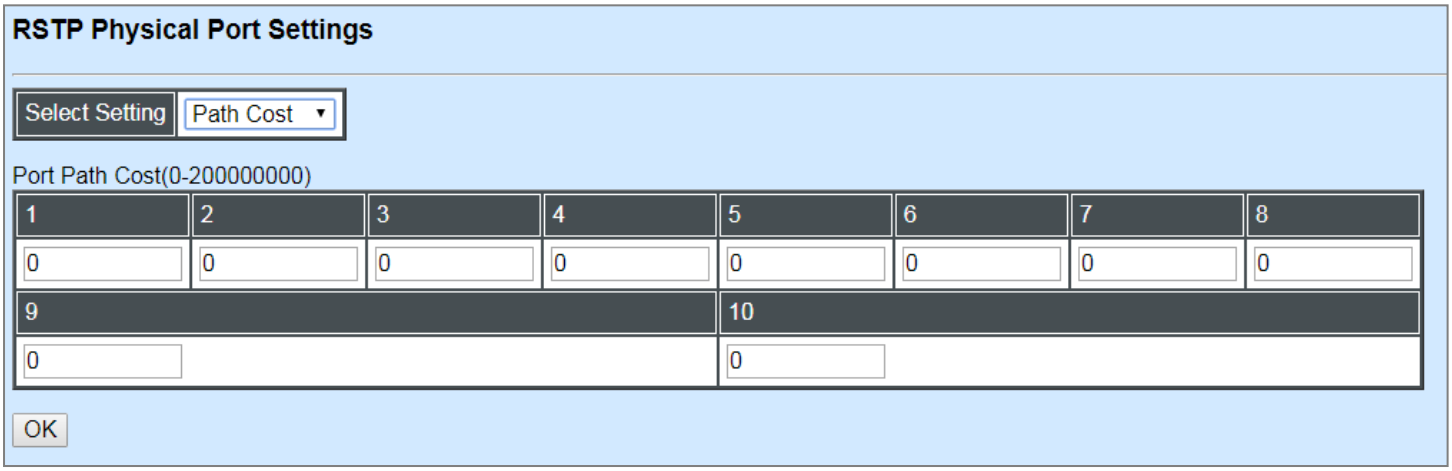
Select “State” from the pull-down menu of Select Setting.



This allows ports to be enabled or disabled. When clicking on the checkbox of the corresponding port number, RSTP will be enabled.

Configure Port Path Cost:

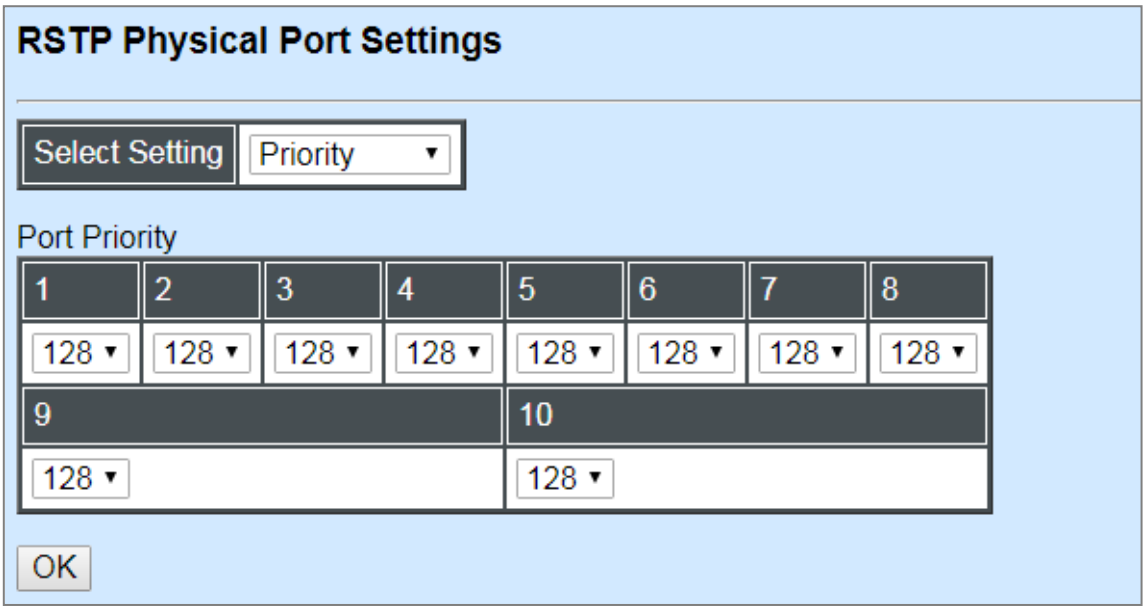
Select “Path Cost” from the pull-down menu of Select Setting.



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

Configure Port Priority:

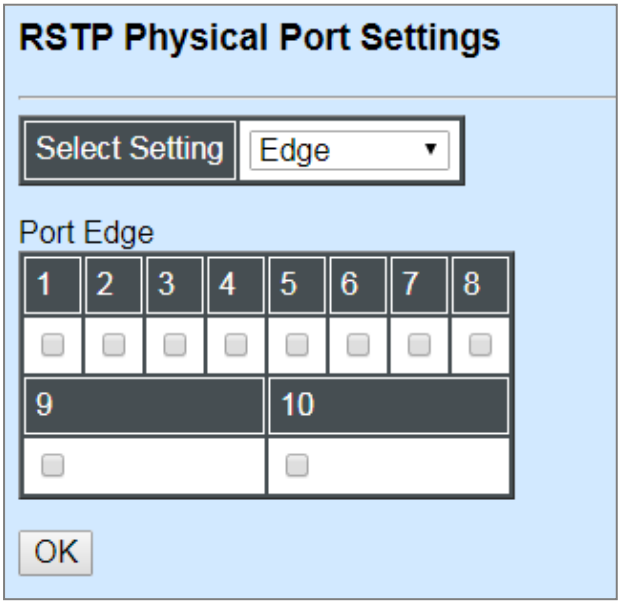
Select “Priority” from the pull-down menu of Select Setting.



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

Configure Port Edge:

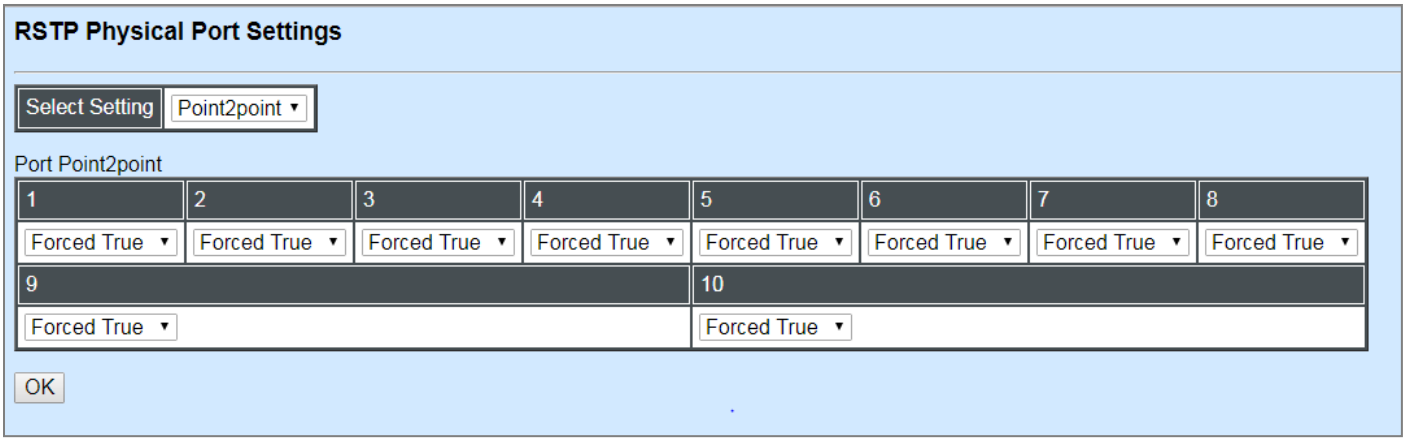
Select “Edge” from the pull-down menu of Select Setting.



Set the port to “enabled” or “disabled”. When clicking on the checkbox of the corresponding port number, Port Edge will be enabled.

Configure Port Point2point:

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



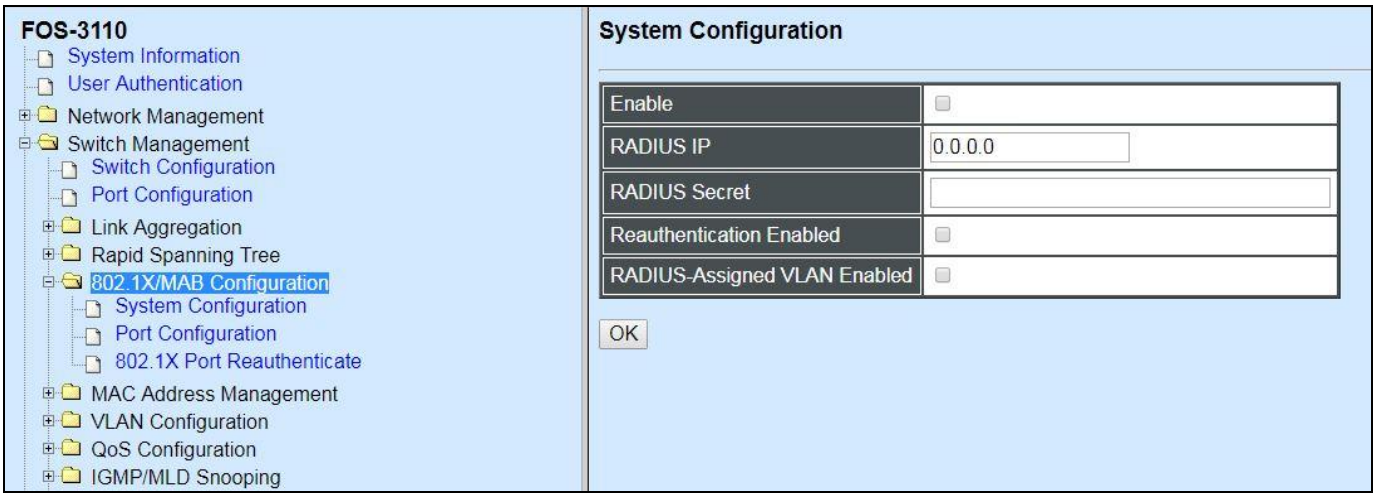
Set up the Point to Point setting of each port. The default setting is “Forced True”.

4.4.5 802.1X/MAB Configuration

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

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

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



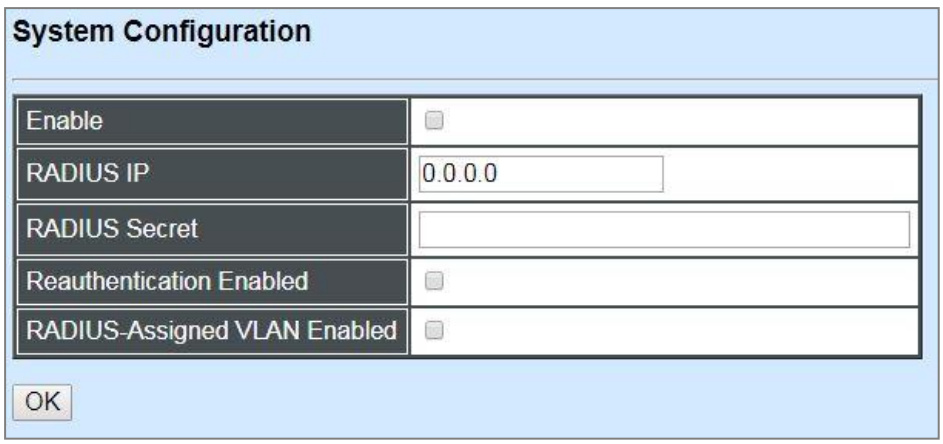
1. **System Configuration:** Set up system 802.1X/MAB RADIUS IP, RADIUS Secret, Reauthentication, RADIUS-Assigned VLAN.

2. **Port Configuration:** Set up port 802.1X/MAB configuration. (Includes MAB, reAuth, reAuthPeriod, EAP Timeout, etc.)

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

4.4.5.1 System Configuration

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



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

RADIUS IP: Specify RADIUS Authentication server address.

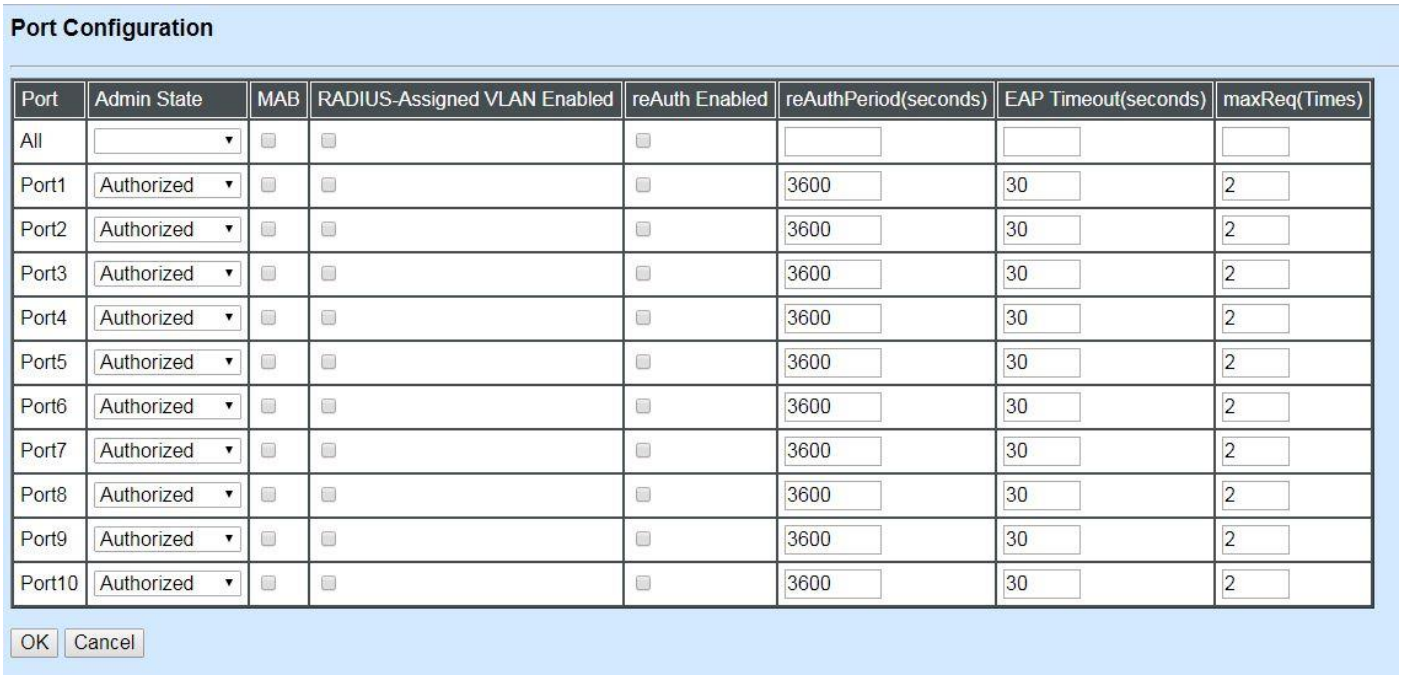
RADIUS Secret: The identification number assigned to each RADIUS authentication server with which the client shares a secret.

Reauthentication Enabled: Enable or disable Reauthentication.

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

4.4.5.2 802.1X/MAB Port Configuration

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



Admin state: Include Authorized, Unauthorized and Auto 3 options for the user to set up the port authorization state for each port. Each state is described as below.

> **Authorized:** This forces the Managed Switch to grant access to all clients, either 802.1X-aware or 802.1x-unaware. No authentication exchange is required. By default, all ports are set to “Authorized”.
>
> **Unauthorized:** This forces the Managed Switch to deny access to all clients, either 802.1X-aware or 802.1X-unaware.
>
> **Auto:** This requires 802.1X-aware clients to be authorized by the authentication server. Accesses from clients that are not 802.1X-aware will be denied.

MAB: MAC Authentication Bypass (MAB), which uses the connecting device's MAC address to grant or deny network access.

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

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

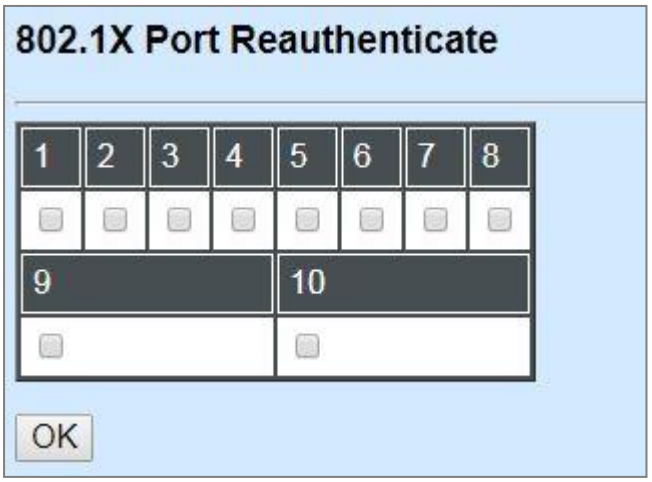
Reauthentication Period/reAuthPeriod(seconds): Specify a period of authentication time that a client authenticates with the authentication server.

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

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

4.4.5.3 802.1X Port Reauthenticate

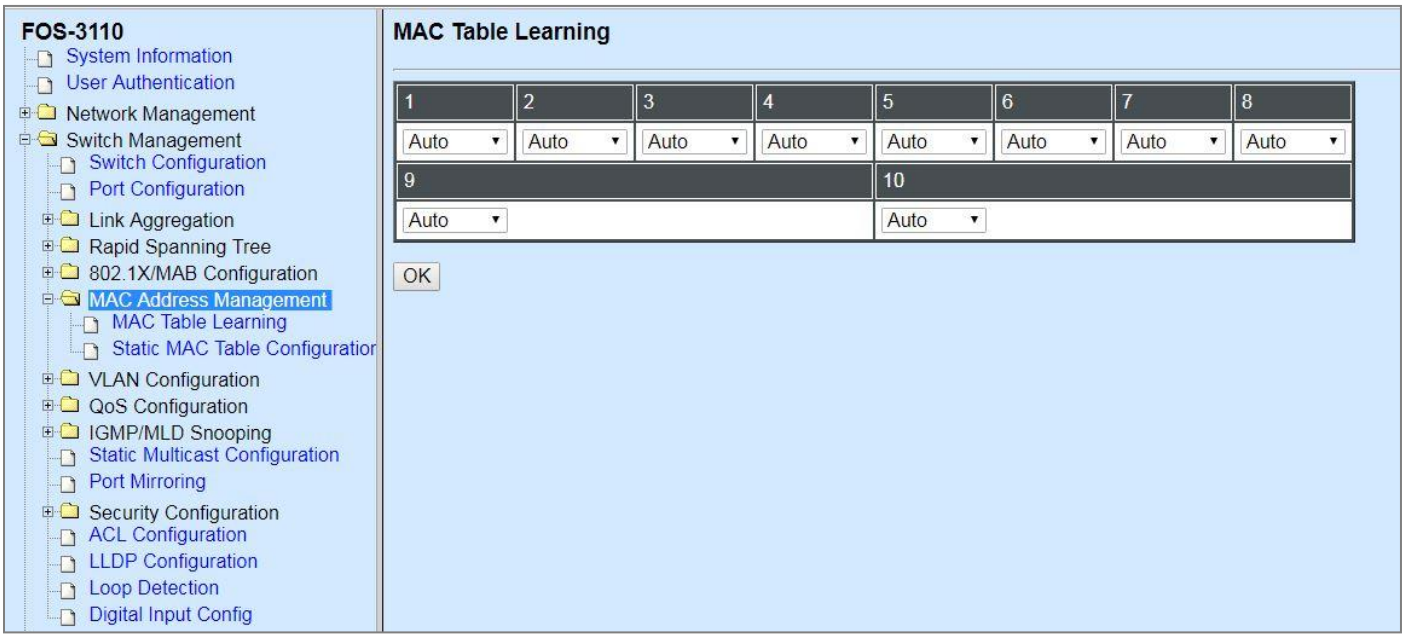
Click the option **802.1X Port Reauthenticate** from the **802.1X/MAB Configuration** menu and then the following screen page appears.



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

4.4.6 MAC Address Management

Click the folder **MAC Address Management** from the **Switch Management** menu and then the following screen page appears.

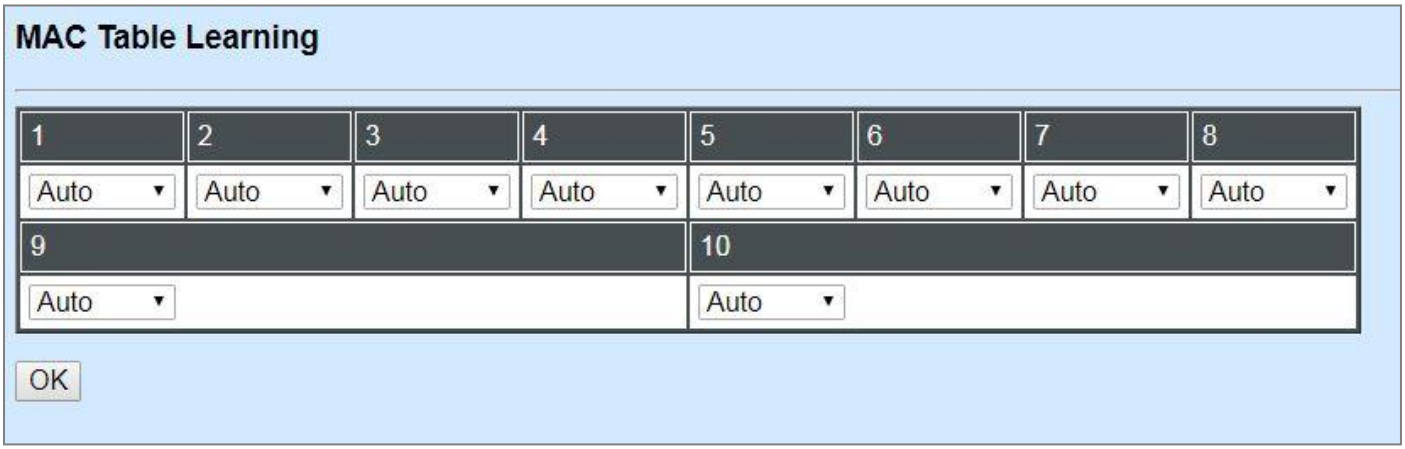


1. **MAC Table Learning:** To enable or disable learning MAC address function.

2. **Static MAC Table Configuration:** To create, edit or delete Static MAC Table setting.

4.4.6.1 MAC Table Learning

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

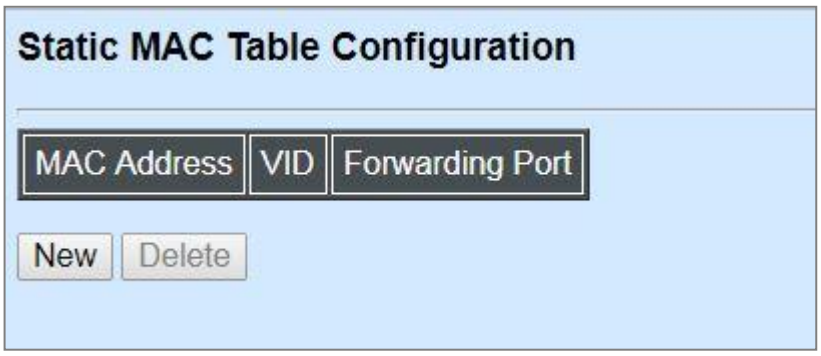


Auto: Enable port MAC address learning.

Disabled: Disable port MAC address learning.

4.4.6.2 Static MAC Table Configuration

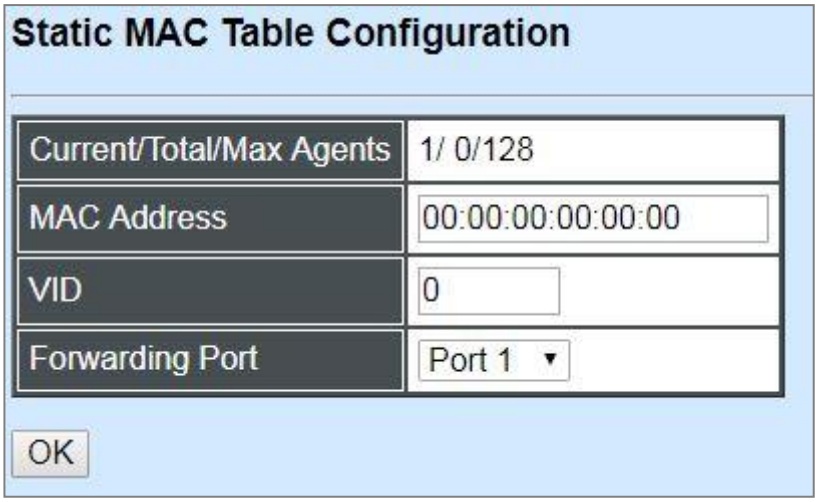
Click the option **Static MAC Table Configuration** from the **MAC Address Management** menu and then the following screen page appears.



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.*

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

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



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

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

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

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

4.4.7 VLAN Configuration

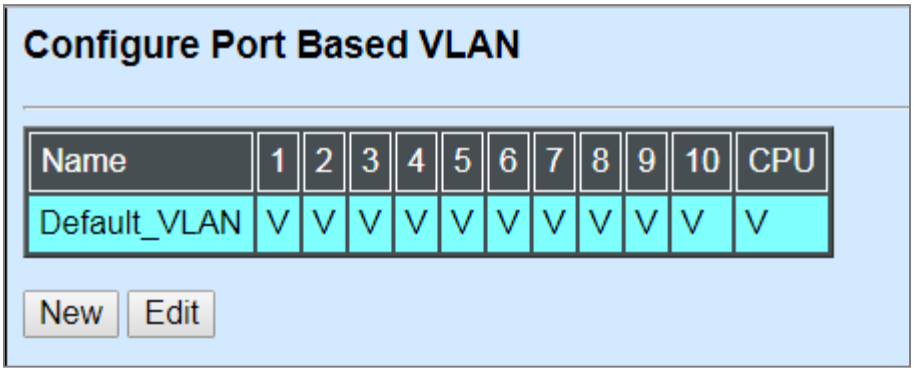
A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast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

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

4.4.7.1 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.

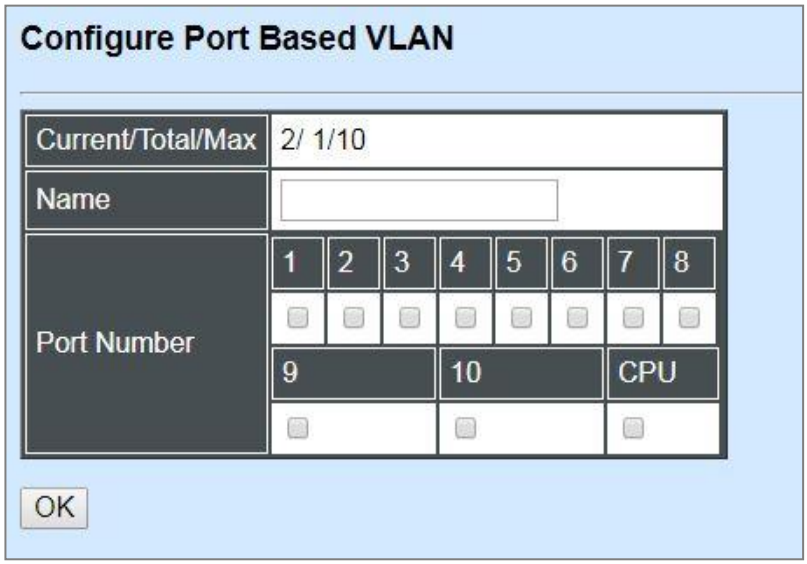
The following screen page appears when you choose **Port Based VLAN** mode from the **VLAN Configuration** menu and then select **Configure VLAN** function.



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

Use **Edit** to modify the current VLAN setting.



Current/Total/Max: The number of current, total and maximum Port-Based VLAN entry or entries.

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

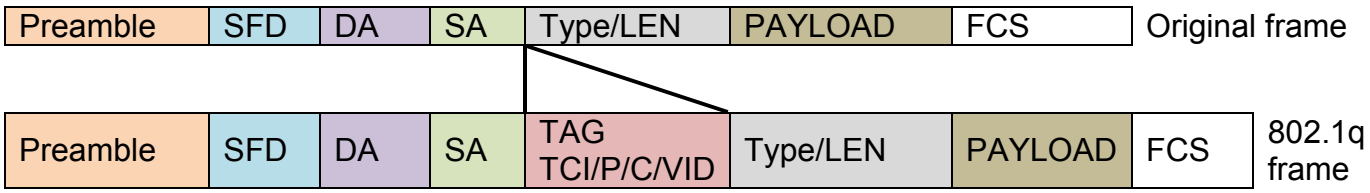
Port Number: By clicking on the checkbox of the corresponding ports, it denotes that the selected ports belong to the specified Port-Based VLAN.

4.4.7.2 802.1Q 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.

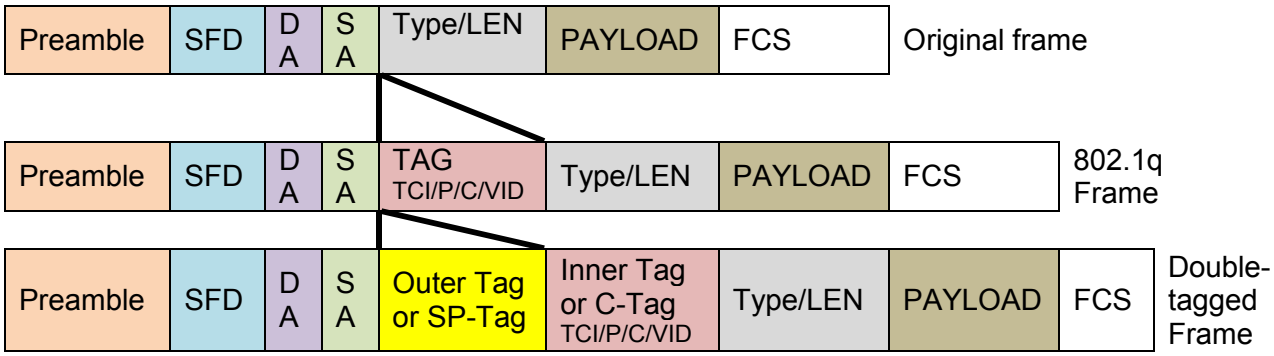
Customer traffic tagged in the normal way with appropriate VLAN IDs comes from an IEEE 802.1Q trunk port on the customer device and into a tunnel port on the service-provider edge switch. The link between the customer device and the edge switch is asymmetric because one end is configured as an IEEE 802.1Q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

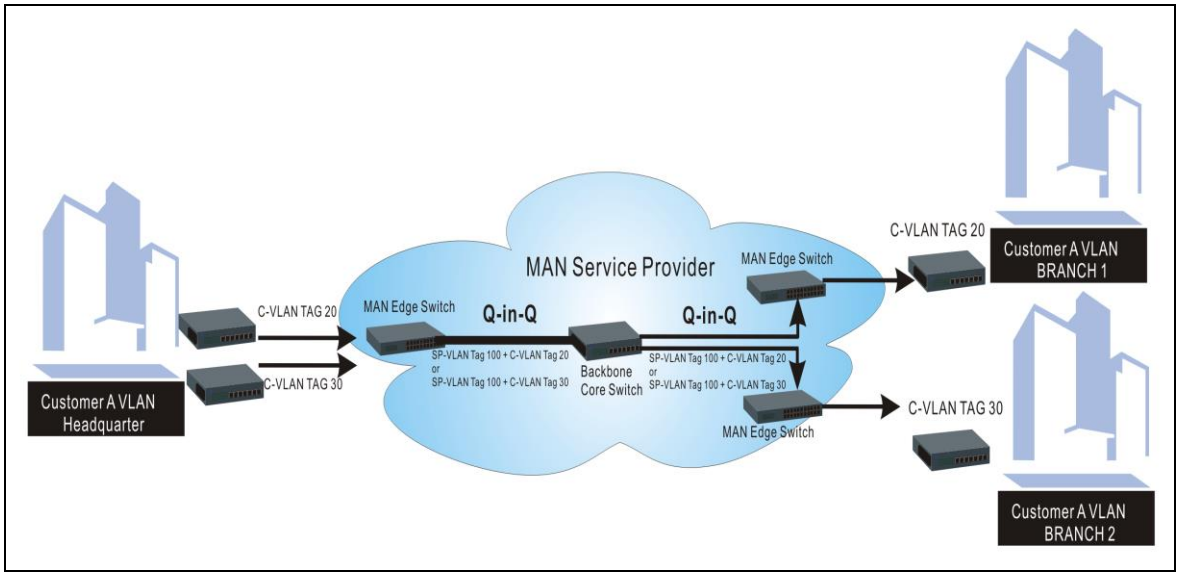
4.4.7.3 Introduction to Q-in-Q (DOT1Q-Tunnel)

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



Double-Tagged Frame Format

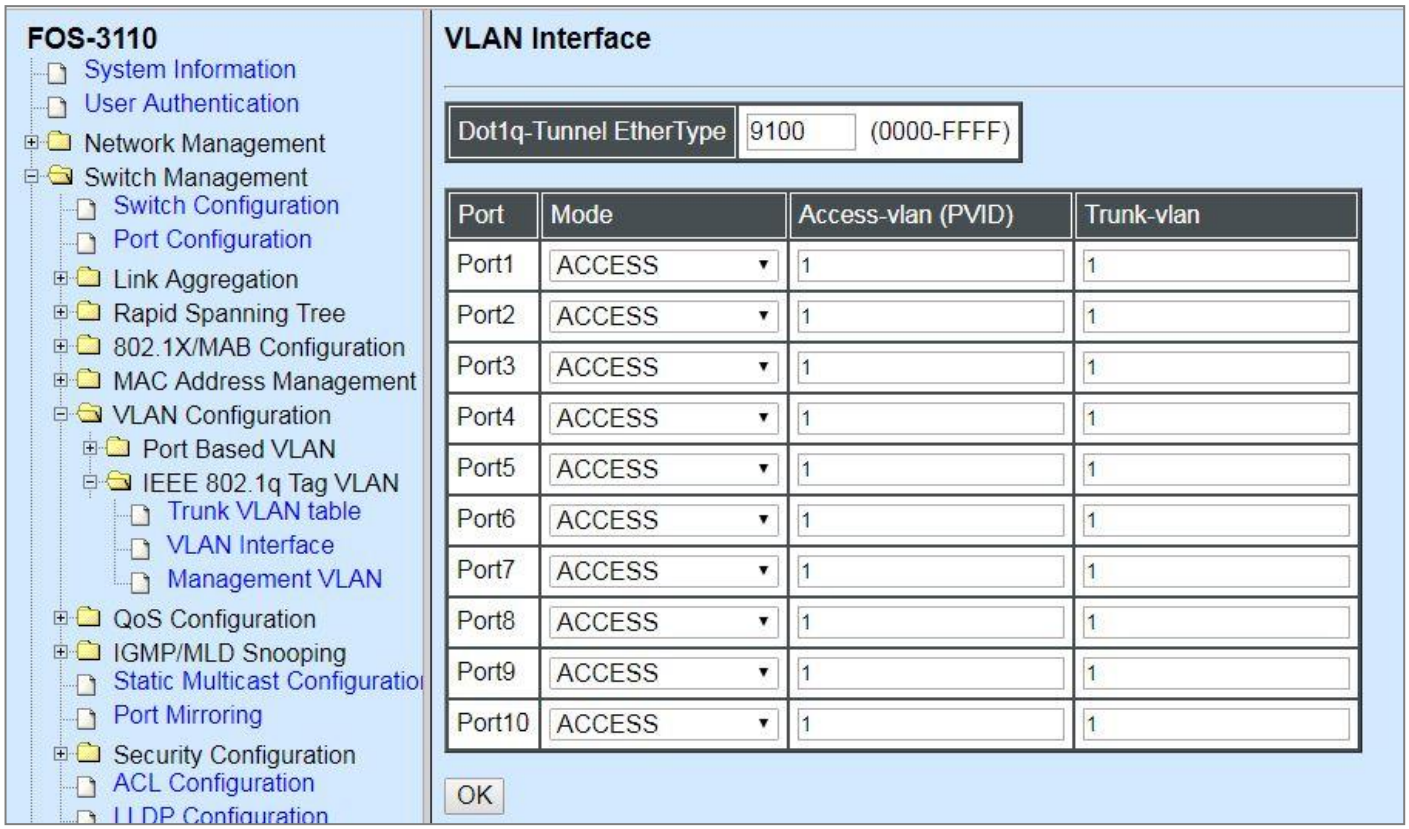
As shown below in “Q-in-Q Example” illustration, Headquarter A wants to communicate with Branch 1 that is 1000 miles away. One common thing about these two locations is that they have the same VLAN ID of 20, called C-VLAN (Customer VLAN). Since customer traffic will be routed to service provider’s backbone,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



Q-in-Q Example

4.4.7.4 802.1Q VLAN

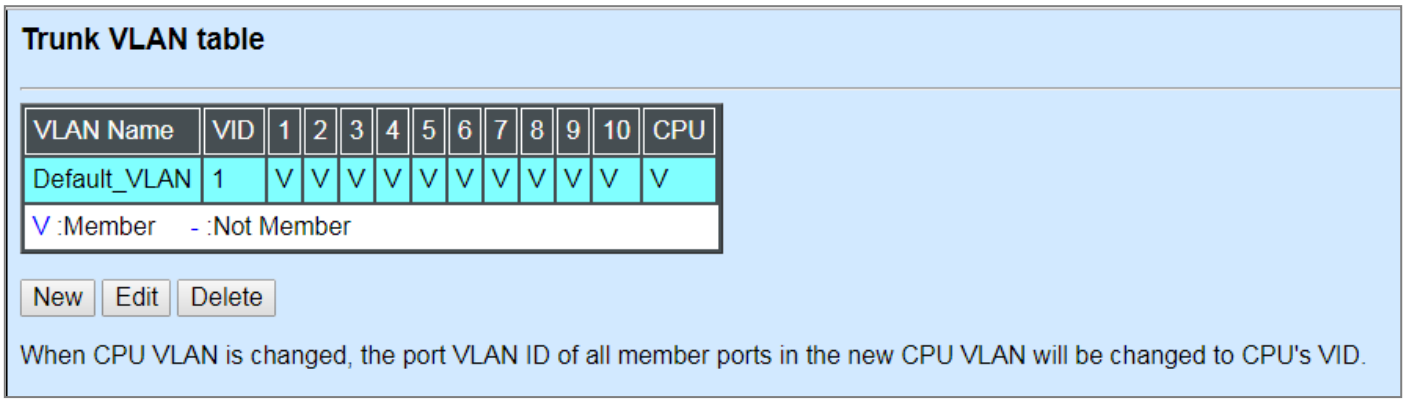
The following screen page appears when you choose **IEEE 802.1q Tag VLAN** mode from the **VLAN Configuration** menu and then select **VLAN interface** function.



1. **Trunk VLAN table:** To create, modify or remove 802.1Q Tag VLAN settings.
2. **VLAN Interface:** To set up VLAN mode and create 802.1Q VLAN on the selected port(s).
3. **Management VLAN:** To set up management VLAN and management ports.

4.4.7.4.1 Trunk VLAN Table

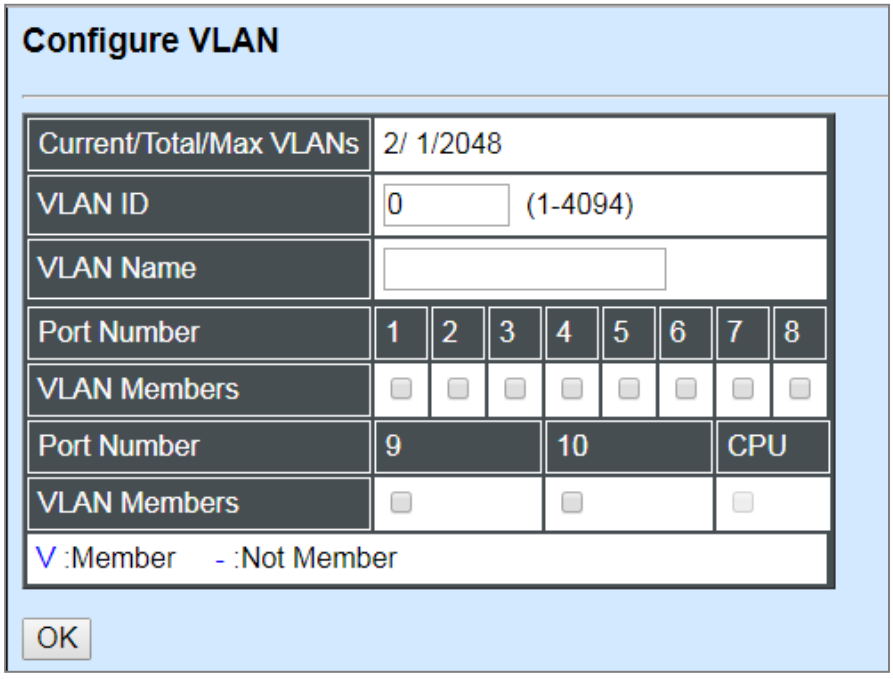
The following screen page appears if you choose **Trunk VLAN table**.



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

Click **Edit** to modify the selected IEEE 802.1Q Tag VLAN setting.

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



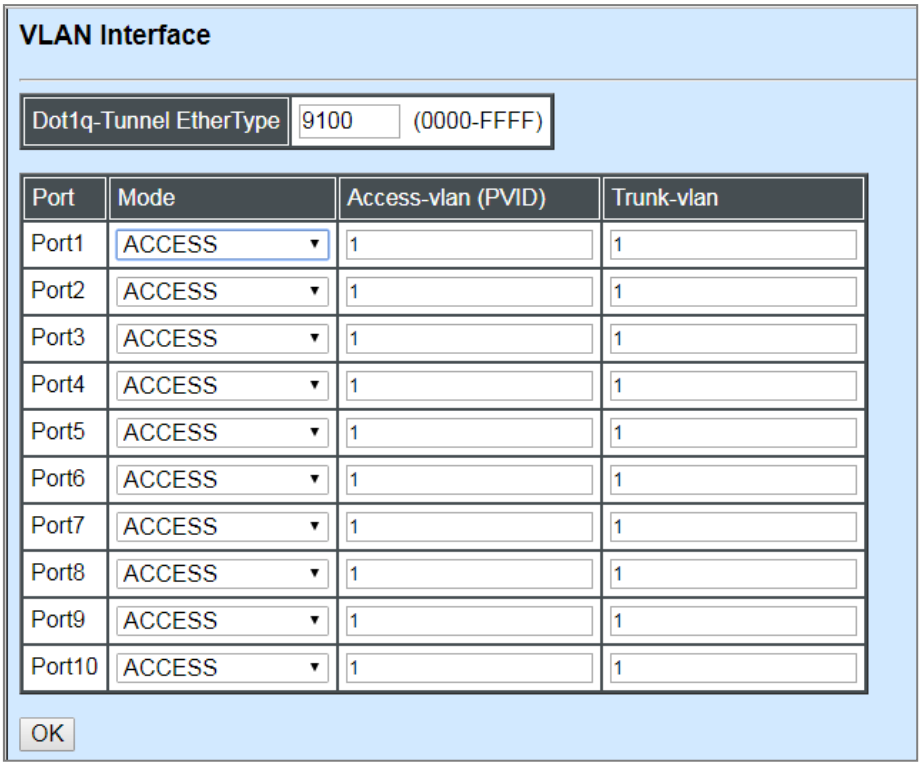
VLAN ID: View only field shows the VLAN ID of this VLAN group.

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

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

4.4.7.4.2 VLAN Interface

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



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

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).

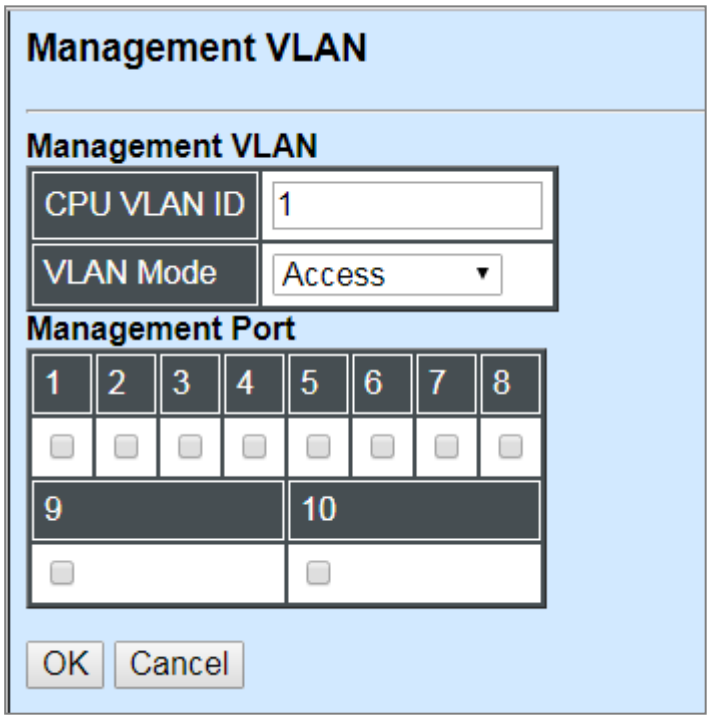
Mode	Port Behavior	
Access	Receive untagged packets only. Drop tagged packets.	
	Send untagged packets only.	
Trunk	Receive tagged packets only. Drop untagged packets.	
	Send tagged packets only.	
Trunk Native	Receive both untagged and tagged packets	Untagged packets: PVID is added
		Tagged packets: Stay intact
	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.	
DOT1Q-Tunnel	Receive all tag and untag packets. Send the packets with the outer tag marked as PVID.	

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

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

4.4.7.4.3 Management VLAN

The following screen page appears if you choose **Management VLAN**.



CPU VLAN ID: Specify an existing VLAN ID.

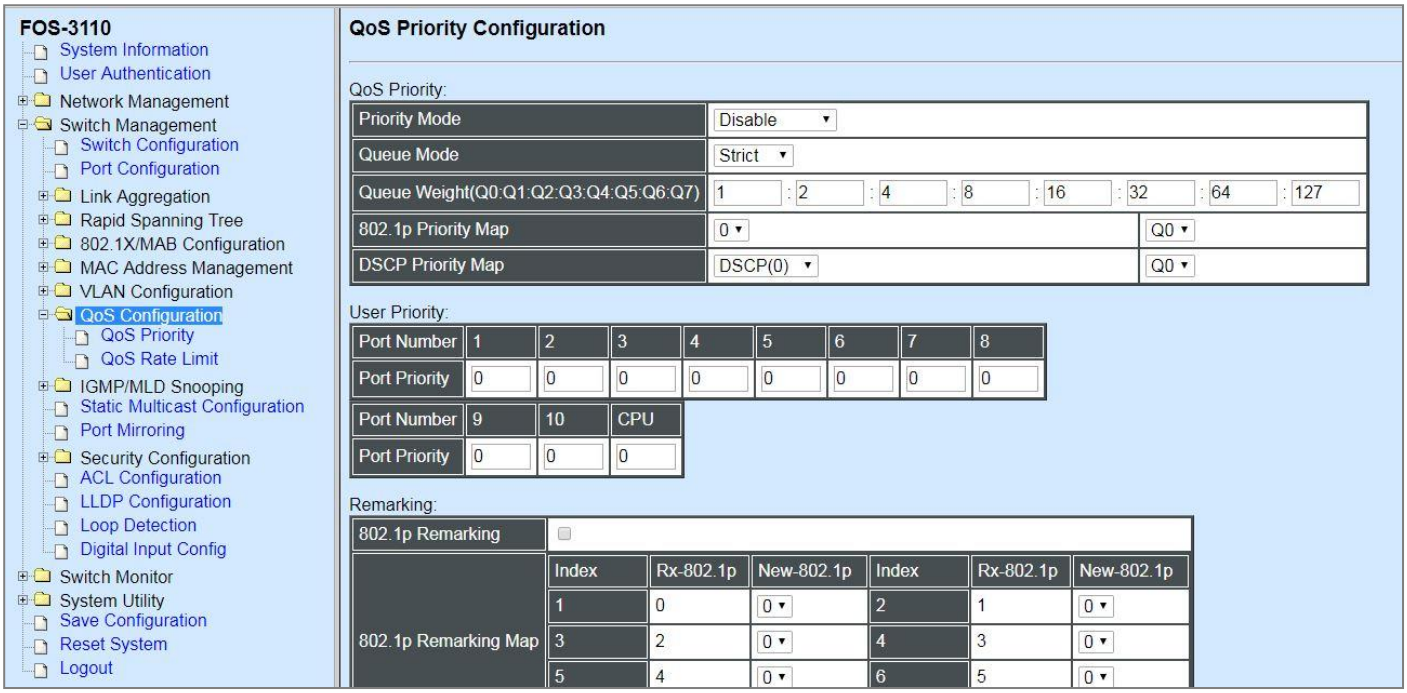
Mode: Select the VLAN mode for this Management VLAN.

Management Port: Click on the checkbox of the corresponding ports that you would like them to become Management ports.

4.4.8 QoS Configuration

Network traffic is always unpredictable and the only basic assurance that can be offered is the best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. 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 Configuration** from the **Switch Management** menu and then two options within this folder will be displayed.

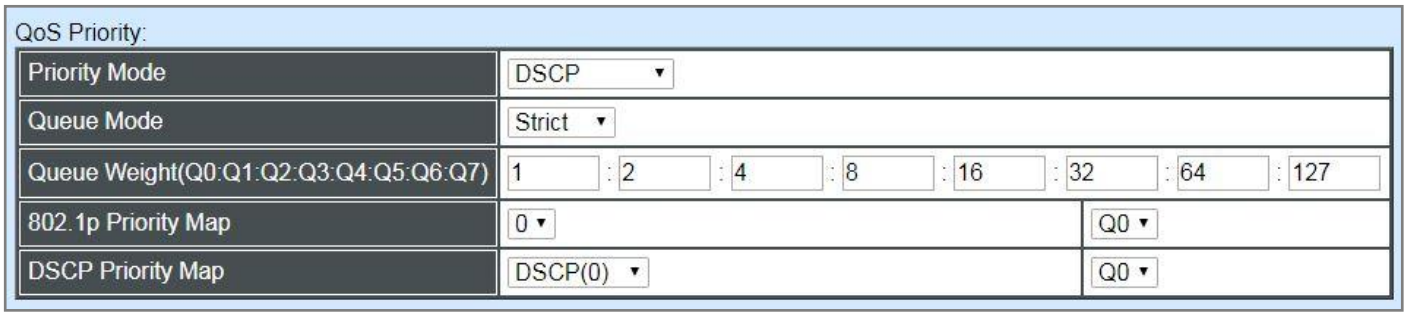


1. **QoS Priority:** To set up each port's QoS default class, Priority, Queuing Mode, Queue Weighted and Remarking.

2. **QoS Rate Limit:** To configure each port's Policer and Shaper Rate.

4.4.8.1 QoS Priority

Select the option **QoS Priority** from the **QoS Configuration** 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.

Disable: 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.

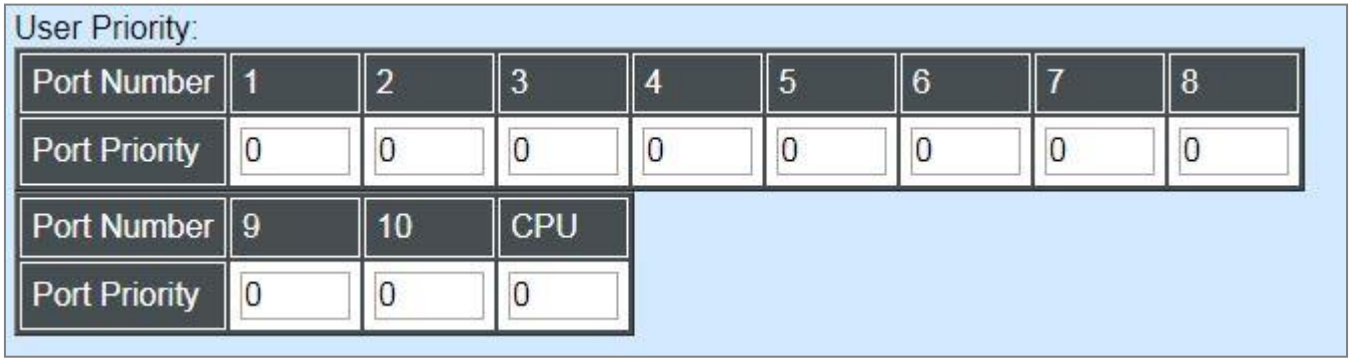
Weight: Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 8 for queues 1 through 4 respectively.

Queue Weight: Specify the Queue weight for each Queue.

802.1p Priority Map: Assign a value (0~7) to 8 different levels.

DSCP Priority Map: Assign a value (0~63) to 64 different levels.

User Priority:

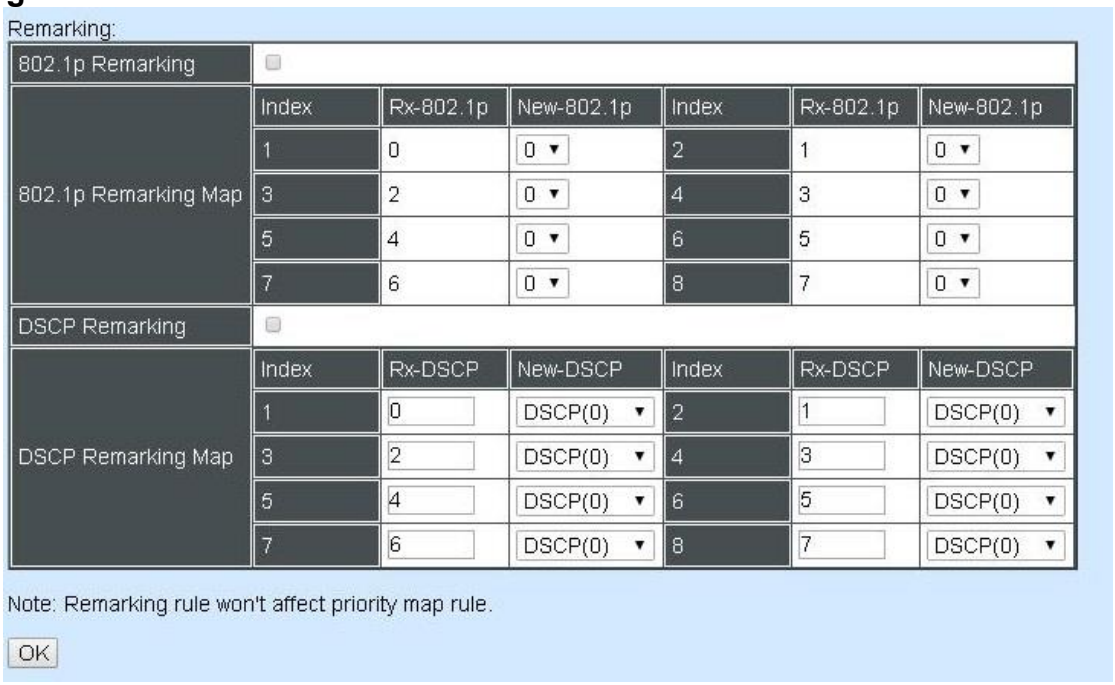


There are eight priority levels that you can choose to classify data packets. Specify one of the listed options for CoS (Class of Service) priority tag values. The default value is “0”.

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

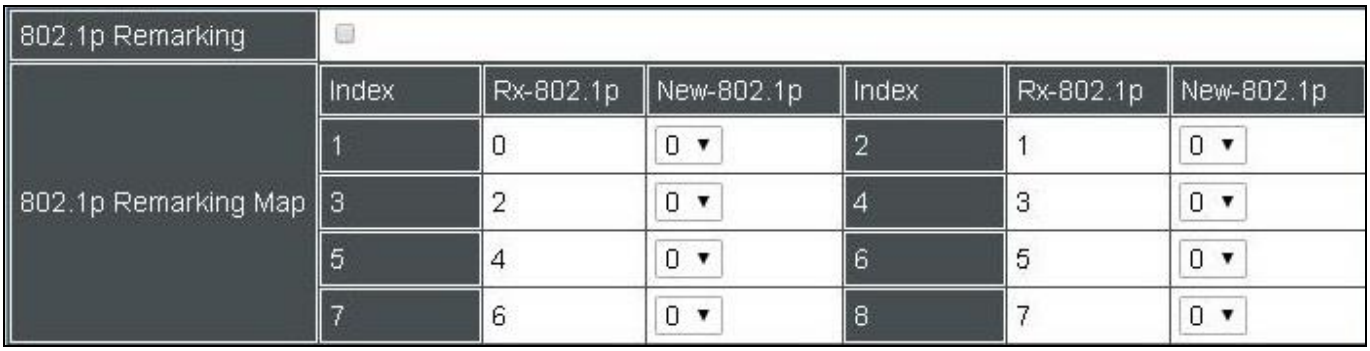
Priority Level	normal	low	low	normal	medium	Medium	High	high
802.1p Value	0	1	2	3	4	5	6	7

Remarking:



Configure 802.1p Remarking:

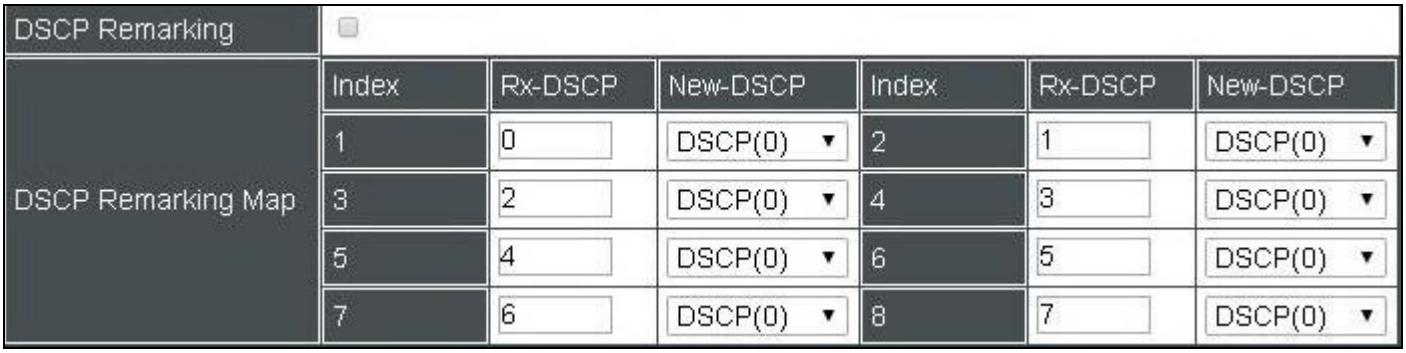
Check **802.1p Remarking** to enable.



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

Configure DSCP Remarking:

Check **DSCP Remarking** to enable.

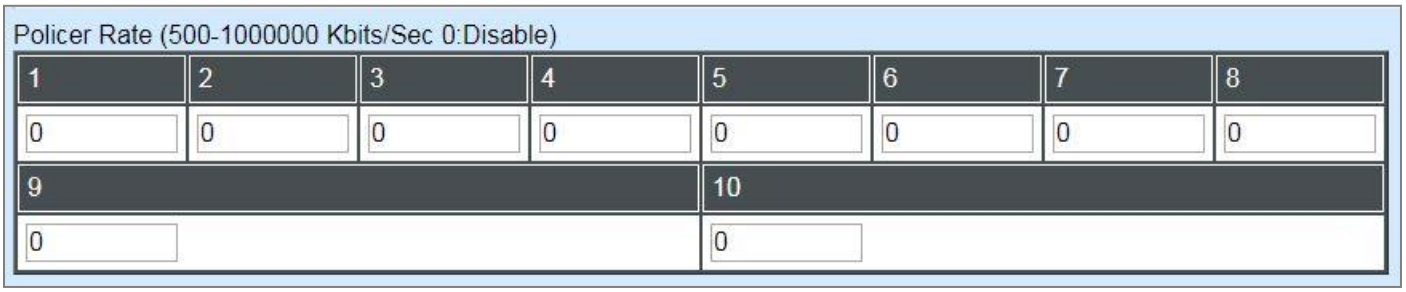


This allows you to enable or disable DSCP remarking for each port. The default setting is disabled.

4.4.8.2 QoS Rate Limit

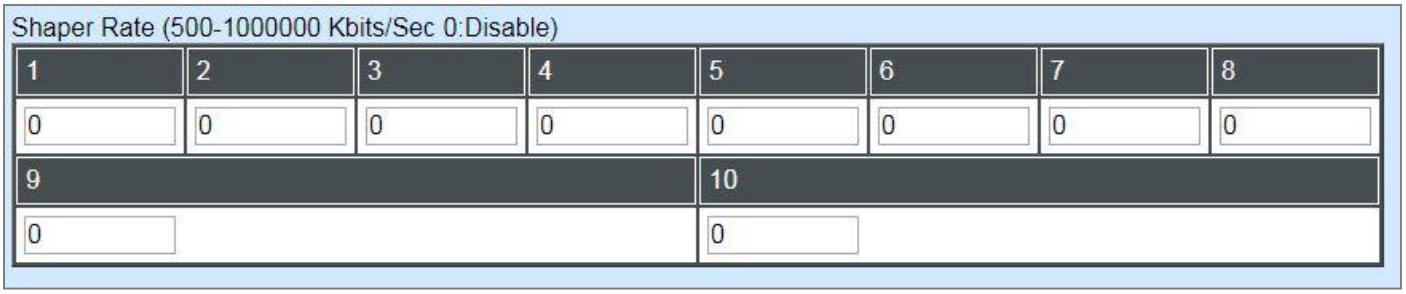
Select the option **QoS Rate Limit** from the **QoS Configuration** menu and then the following screen page appears.

Configure Policer Rate:



This allows users to specify each port's inbound bandwidth. The excess traffic will be dropped. Specifying "0" is to disable this function.

Configure Shaper Rate:



This allows users to specify each port's outbound bandwidth. The excess traffic will be dropped. Specifying "0" is to disable this function.

4.4.9 IGMP/MLD Snooping

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

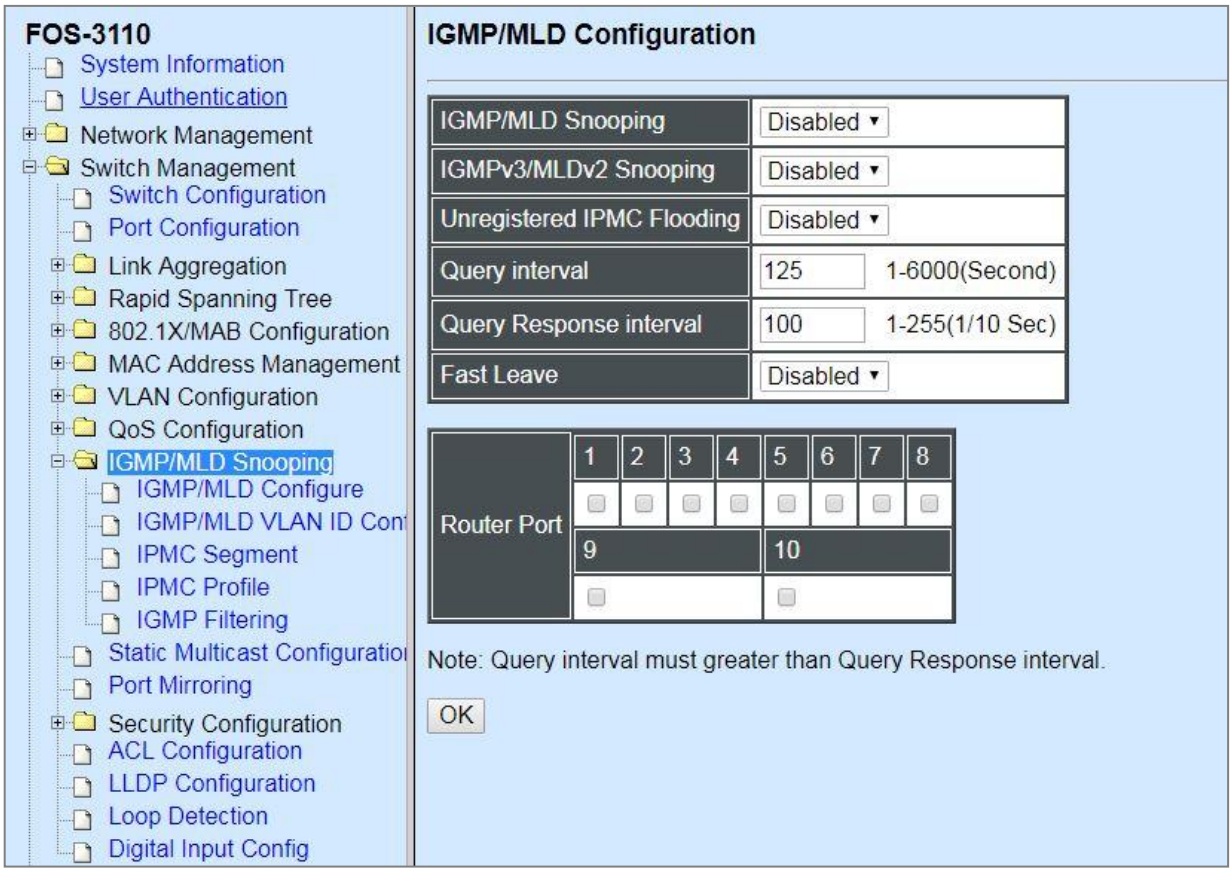
IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers by processing the layer 3 packets that IGMP packets sent in a multicast network.

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

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

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

Select the folder **IGMP/MLD Snooping** from the **Switch Management** menu and then five options within this folder will be displayed.



1. **IGMP/MLD Configure:** To enable or disable IGMP/MLD Snooping, IGMPv3/MLDv2 Snooping, Unregistered IPMC Flooding and set up router ports.

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

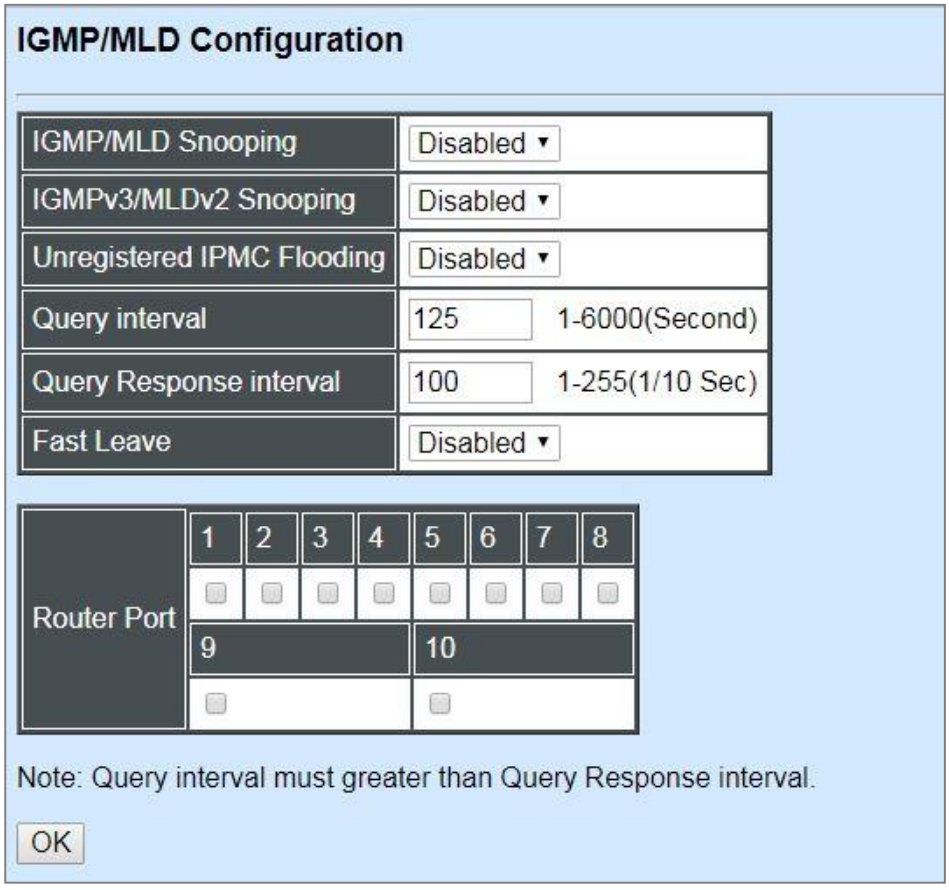
3. **IPMC Segment:** To create, edit or delete IPMC segment.

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

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

4.4.9.1 IGMP/MLD Configure

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



IGMP/MLD 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 125, One Unit =1 second)

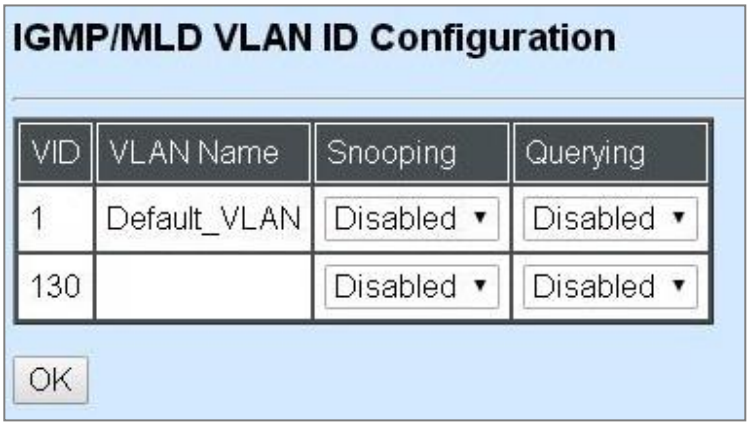
Query Response Interval: This determines the maximum amount of time allowed before sending an IGMP response report. (Default value 100, One Unit=0.1 second)

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

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

4.4.9.2 IGMP/MLD VLAN ID Configuration

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



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.

4.4.9.3 IPMC Segment

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

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

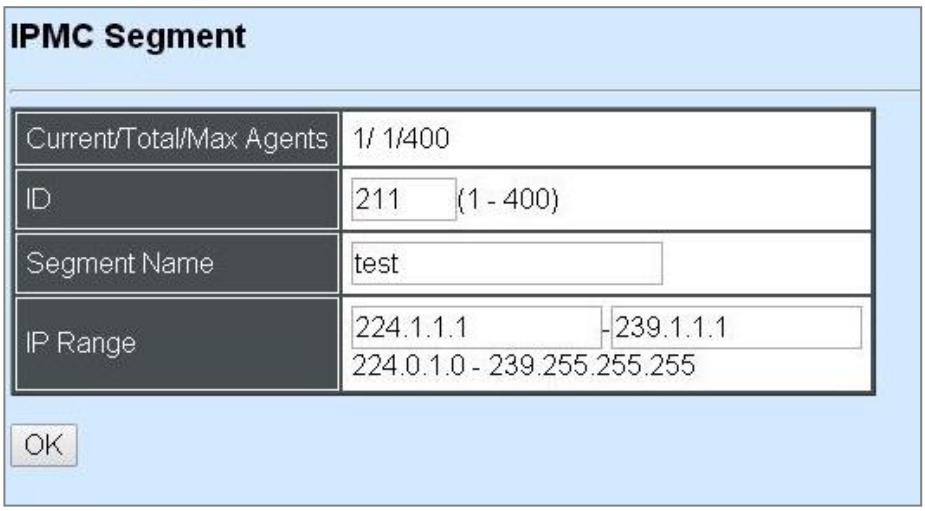
Segment Name: View-only field that shows the current registered Name.

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

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

Click **Edit** to modify the selected IPMC Segment settings.

Click **Delete** to remove an existing IPMC Segment registration.



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

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

Total: This shows the amount of total registered IPMC Segments.

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

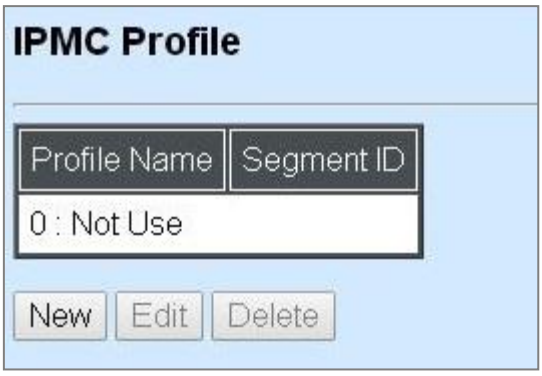
ID: Specify a number from 1~400 for a new ID.

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.)

4.4.9.4 IPMC Profile

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



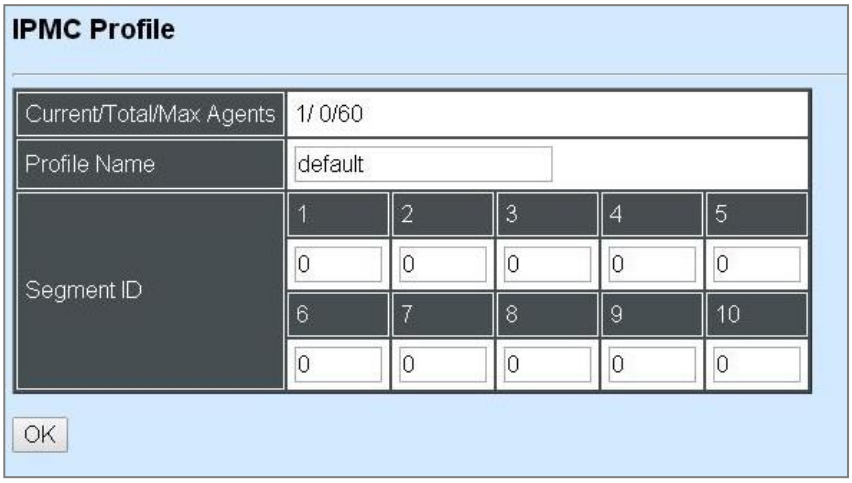
Profile Name: View-only field that shows the current registered profile name(s).

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

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

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

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



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

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

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

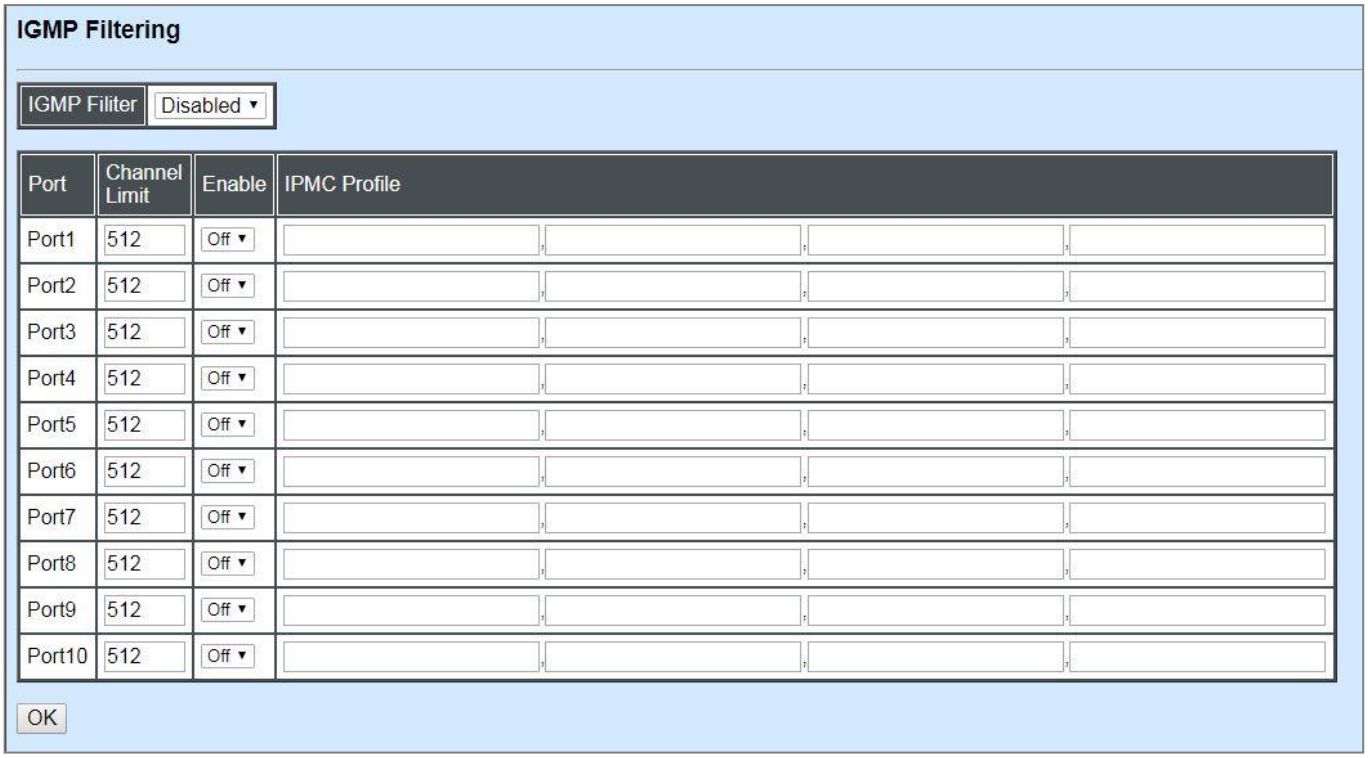
Max: This shows the maximum number available for IPMC Profile. The maximum number is 60.

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

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

4.4.9.5 IGMP Filtering

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



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

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

Channel Limit: Specify the maximum transport multicast stream.

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

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

4.4.10 Static Multicast Configuration

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

IP/IPv6 Address: View-only field that shows the current source IP address of multicast stream.

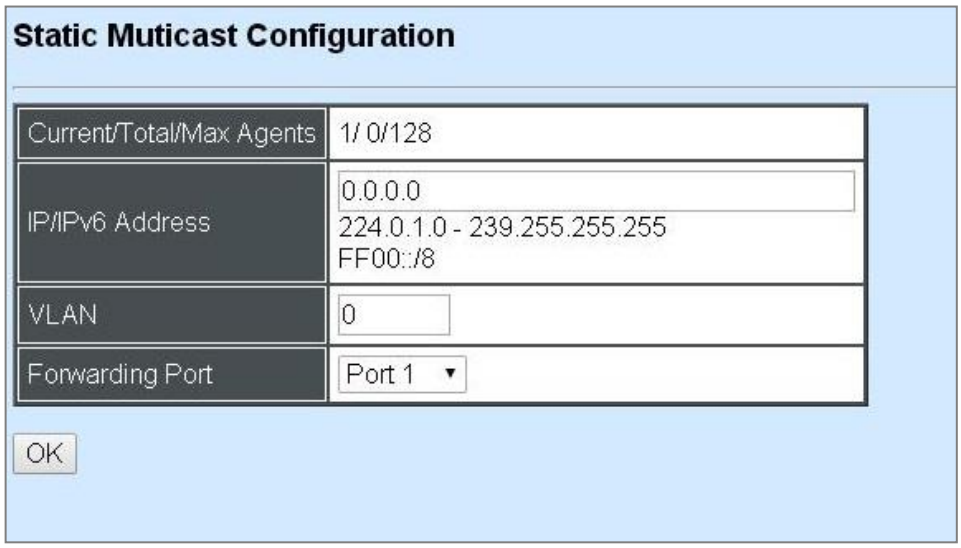
VID: View-only field that shows the specified VLAN ID for current multicast stream.

Forwarding port: View-only field that shows the forwarding port for current multicast stream.

Click **New** to register a new Static Multicast configuration and then the following screen page appears.

Click **Edit** to modify static multicast configuration settings.

Use **Delete** to remove a current Static Multicast configuration.



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

Current: This shows the number of current registered static multicast configuration.

Total: This shows the amount of total registered static multicast configuration.

Max: This shows the maximum number available for static multicast configuration. The default maximum number is 128.

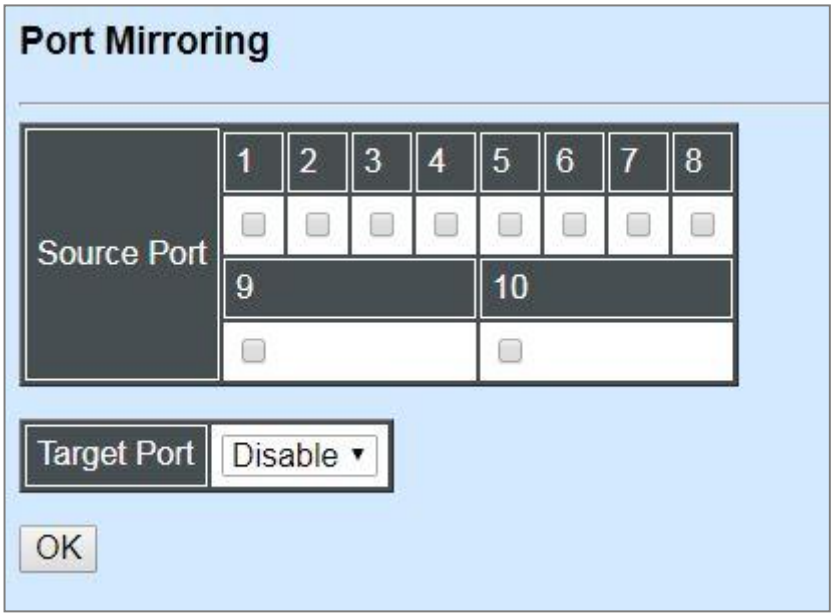
IP/IPv6 Address: Specify the multicast stream source IP/IPv6 address.

VLAN: Specify a VLAN ID for multicast stream.

Forwarding port: Select a port number for multicast stream forwarding.

4.4.11 Port Mirroring

In order to allow the target port to mirror the source Port(s) and enable traffic monitoring, select the option **Port Mirroring** from the **Switch Management** menu and then the following screen page appears.



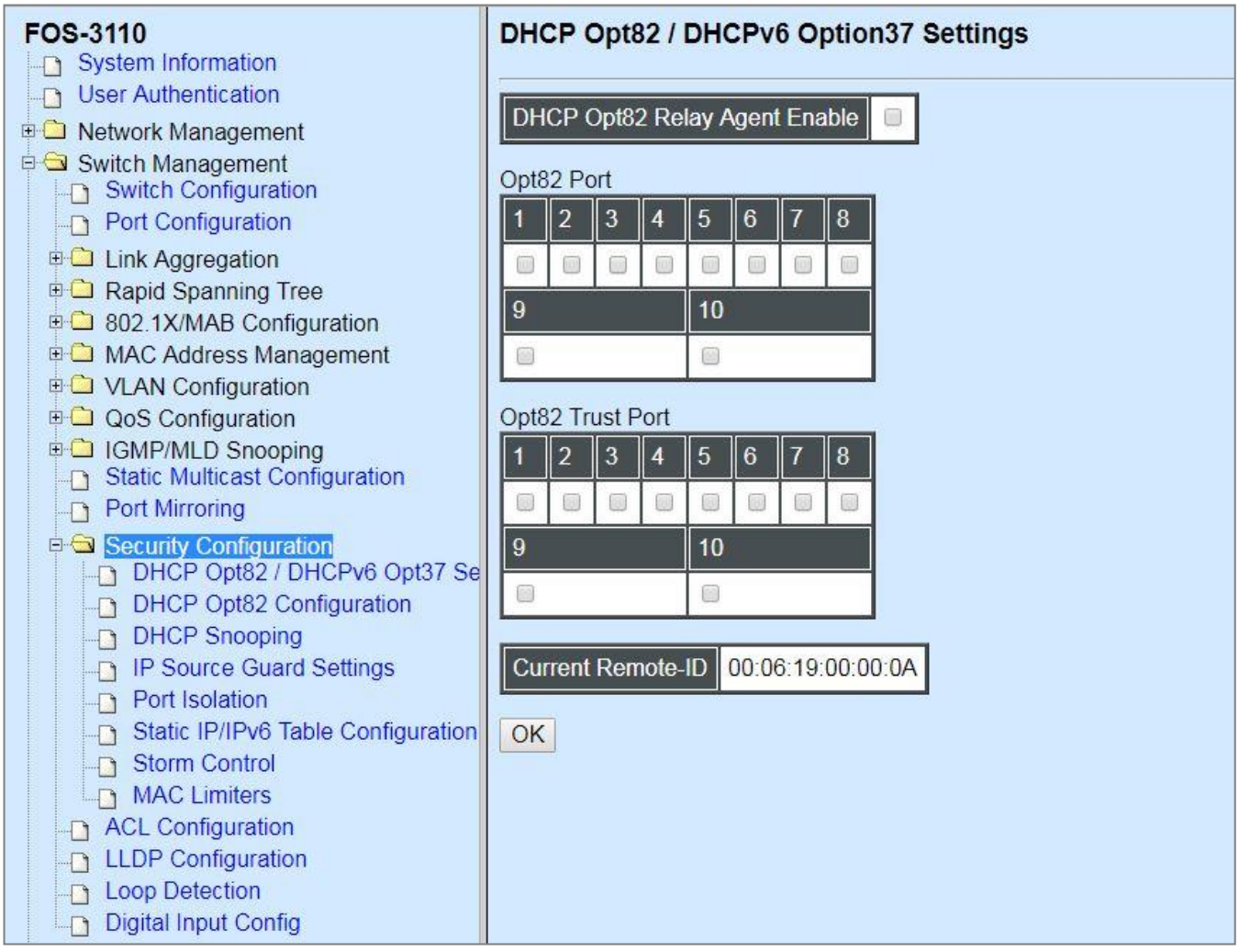
Source Port: Select the preferred source port(s) for mirroring by clicking on the checkbox of the corresponding port number. Please note that the port selected as the target port cannot be the source port.

Target Port: Choose from port 1 to port 10 or “disable” from the pull-down menu to designate the target port or disable the port mirroring function.

4.4.12 Security Configuration

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 Configuration** from the **Switch Management** menu and then eight options within this folder will be displayed



1. **DHCP Opt82/DHCPv6 Opt37 Settings:** To enable or disable DHCP Option 82 (for DHCPv4) and Option 37 (for DHCPv6) relay agent global setting and show each port's configuration.

2. **DHCP Opt82 Configuration:** Set up suboptions such as Circuit-ID and Remote-ID.

3. **DHCP Snooping:** Customer port filtering setting.

4. **IP Source Guard Settings:** Customer port DHCP snooping setting.

5. **Port Isolation:** Set up port’s communication availability that they can only communicate with a given "uplink"

6. **Static IP/IPv6 Table Configuration:** To create static IP/IPv6 table for DHCP snooping setting.

7. **Storm Control:** To prevent the Managed Switch from unicast, broadcast, and multicast storm.

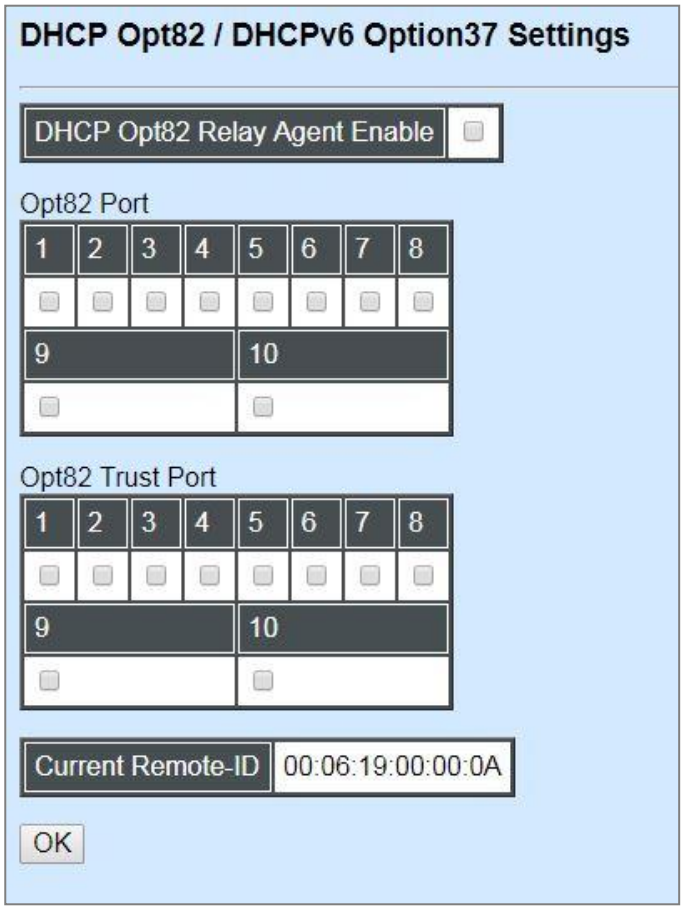
8. **MAC Limiters:** Set up MAC Address limit.

4.4.12.1 DHCP Option 82/DHCPv6 Option 37 Settings

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.

Configure Opt82/Opt37 Port Setting:

Select the option **DHCP Option 82 / DHCPv6 Option 37 Settings** from the **Security Configuration** menu and then the following screen page appears.



Relay Agent: To 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.

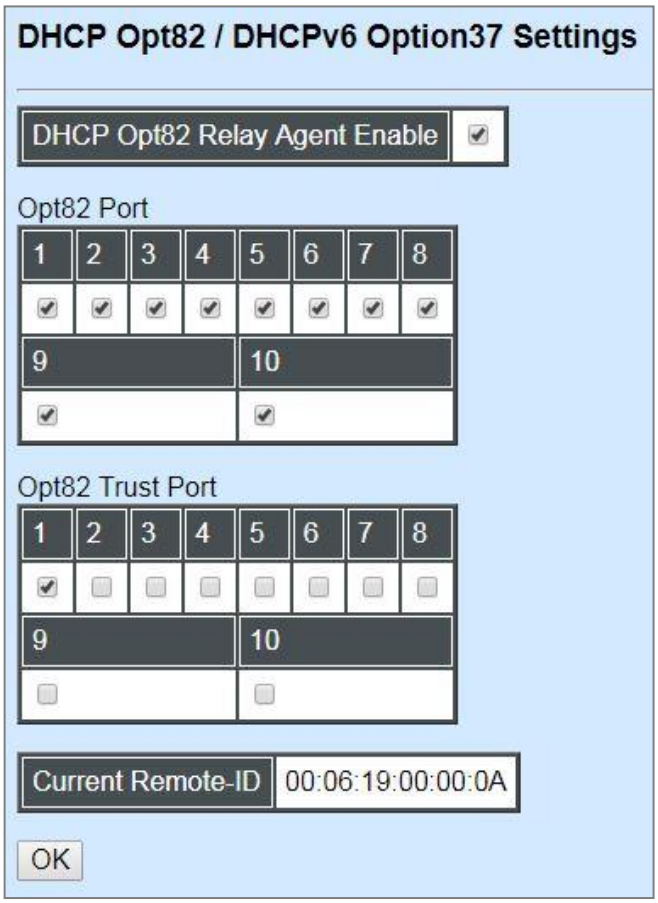
Opt82 Port:

Enable (check): Add Agent information.

Disable (uncheck): Forward.

Opt82 Trust Port: 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.

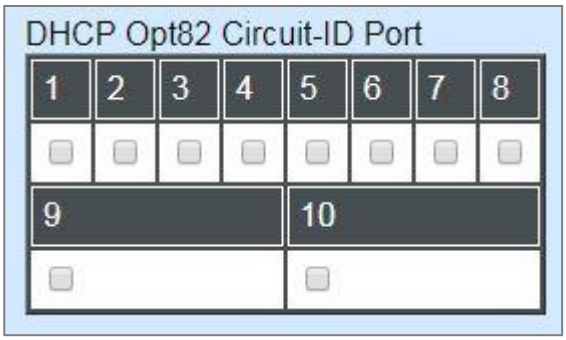
A. If a DHCP request is with Opt82 Agent information and then the Managed Switch will drop it because it is not marked as a trust port.
B. If a DHCP request is without Opt82 Agent information and then the Managed Switch will add Opt82 Agent information and then forward it.

4.4.12.2 DHCP Option 82 Configuration

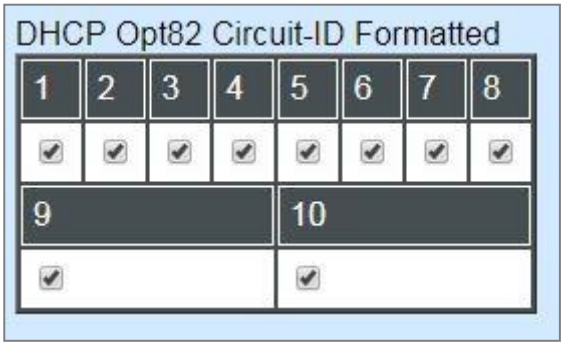
The Managed Switch adds the option 82 information in the packet when it receives the DHCP request. In general, the switch MAC address(the remote-ID suboption) and the port identifier, vlan-mod-port or snmp-ifindex are included in the option 82 information. You can configure the remote ID and circuit ID. Click **DHCP Opt82 Configuration** from the **Security Configuration** and the following screen page appear.

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.

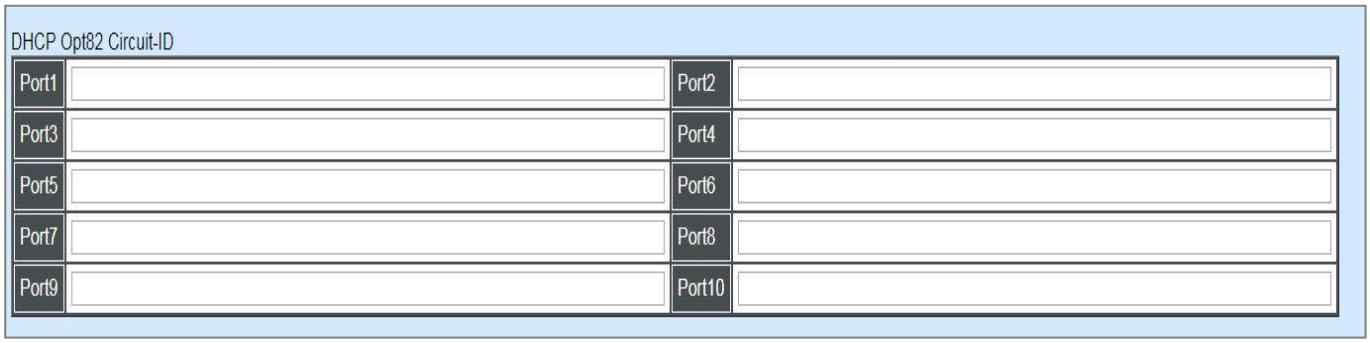
Remote ID Suboption: This suboption may be added by DHCP relay agents that terminate switched or permanent circuits and have machanisms to identify the remote host end of the circuit. DHCP servers may use this option to select parameters specific to particular users, hosts, or subscriber modems. The 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.



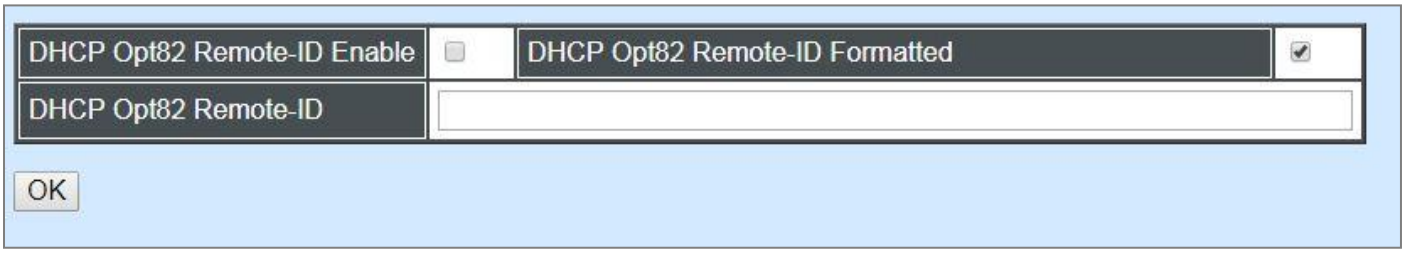
Click on the checkbox of the corresponding port number you would like to configure with circuit ID.



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.



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 64 characters. The default circuit ID is the port identifier, the format of which is **vlan-mod-port**.



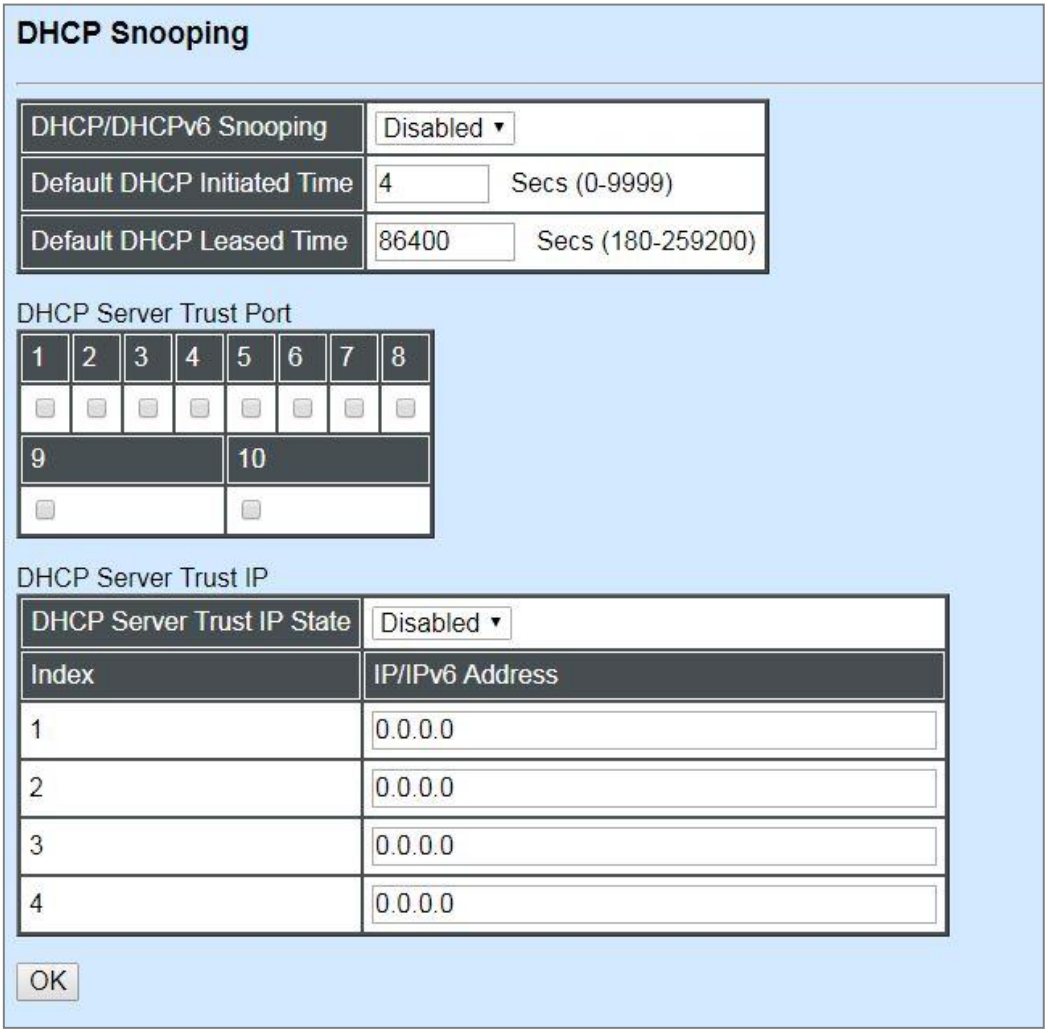
DHCP Opt82 Remote-ID Enable: Click on the checkbox to enable Remote ID suboption or uncheck to disable it.

DHCP Opt82 Remote-ID: You can configure the remote ID to be a string of up to 64 characters. The default remote ID is the switch MAC address.

DHCP Opt82 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.

4.4.12.3 DHCP Snooping

Select the option **DHCP Snooping** from the **Security Configuration** menu and then the following screen page appears.

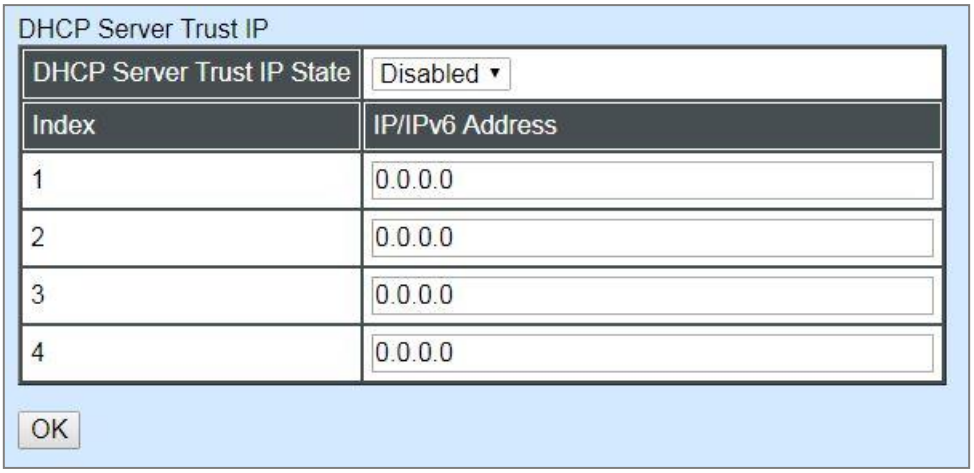


DHCP/DHCPv6 Snooping: Enable or disable DHCP/DHCPv6 Snooping function.

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).

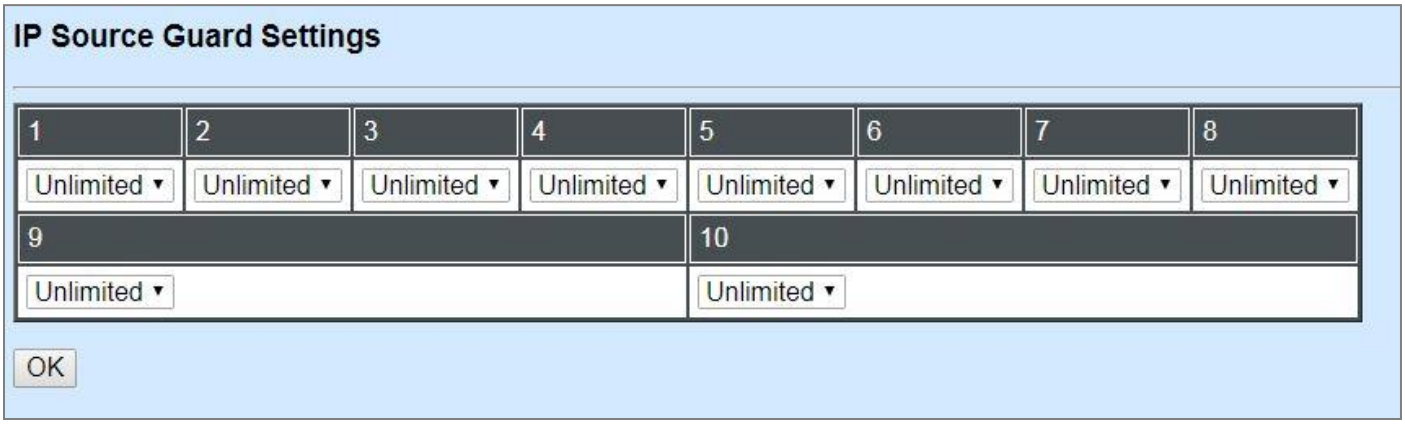
DHCP Server Trust Port: Specify designated port to be Trust Port that can give you "offer" from DHCP server. Check any port box to enable it.



DHCP Server Trust IP: After enabling Trust Port, you may additionally specify Trust IP address for identification of DHCP server. Click drop-down box and select “enable”, then specify Trust IP address.

4.4.12.4 IP Source Guard Settings

Select the option **IP Source Guard Settings** from the **Security Configuration** menu and then the following screen page appears.



Source Guard: To specify the authorized access type for each port. There are three options available.

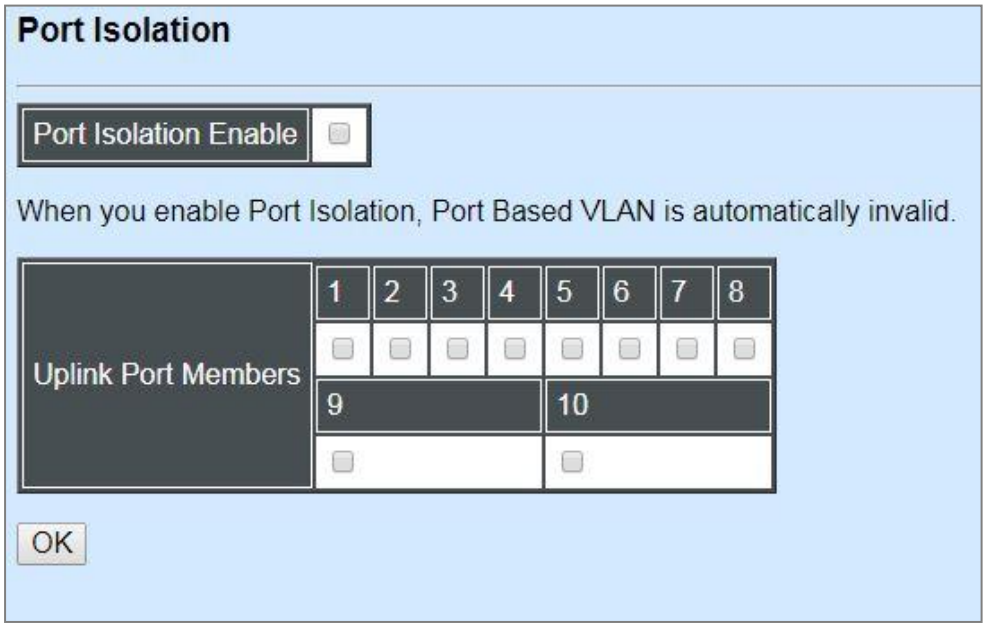
Unlimited: Non-Limited (Allows both static IP and DHCP-assigned IP).

DHCP: DHCP-assigned IP address only.

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

4.4.12.5 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.



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 Members: 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.

4.4.12.6 Static IP/IPv6 Table Configuration

Select the option **Static IP/IPv6 Table Configuration** from the **Security Configuration** menu and then the following screen page appears.

This static IP address and Port mapping table shows the following information.

IP/IPv6 Address: View-only field that shows the current static IP address.

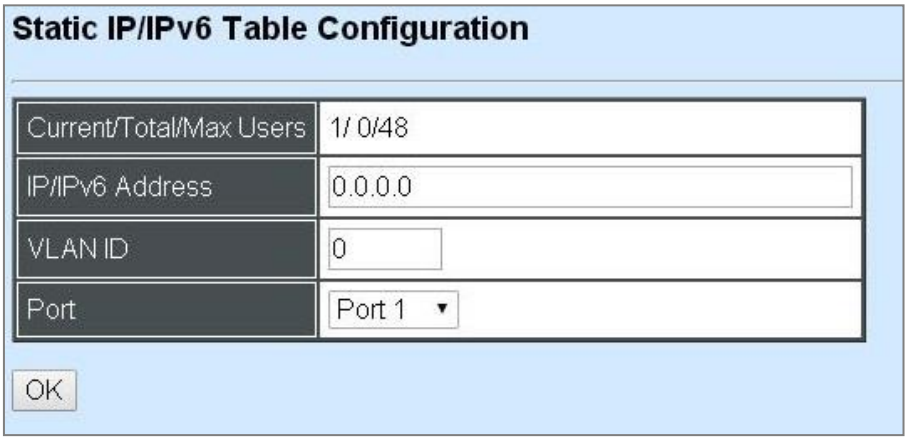
VLAN ID: View-only field that shows the VLAN ID.

Port: View-only field that shows the connection port number.

Click **New** to register a new Static IP address and then the following screen page appears.

Click **Edit** to modifyStatic IP Table settings.

Use **Delete** to remove a current Static IP address.



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

Current: This shows the number of current registered Static IP address.

Total: This shows the amount of total registered Static IP addresses.

Max: This shows the maximum number available for Static ID address registration.

IP/IPv6 address: Specify an IP/IPv6 address that you accept.

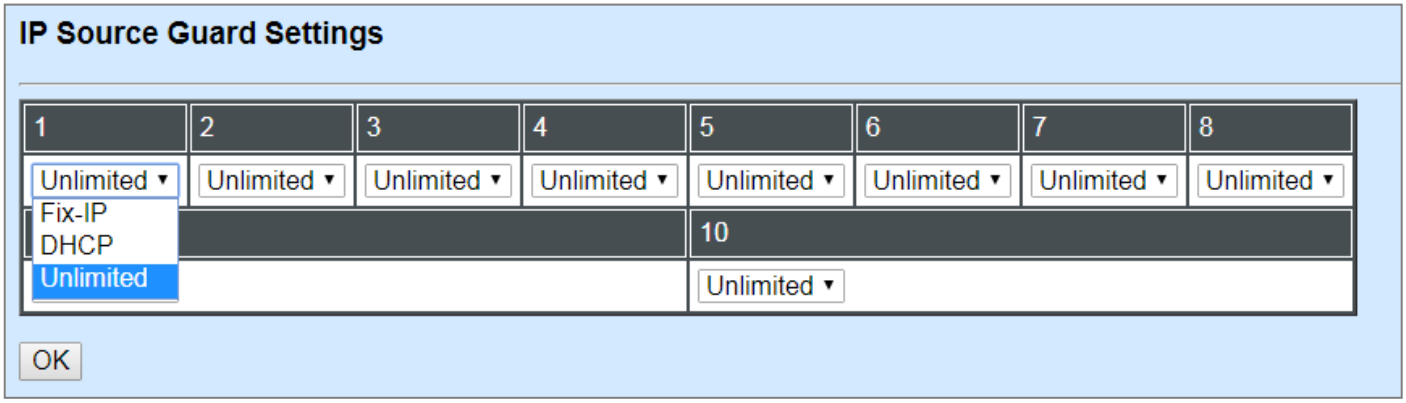
VLAN ID: Specify the VLAN ID. (0 means without VLAN ID)

Port: Specify the communication port number. (Port 1~10)

4.4.12.6.1 Configure DHCP Snooping

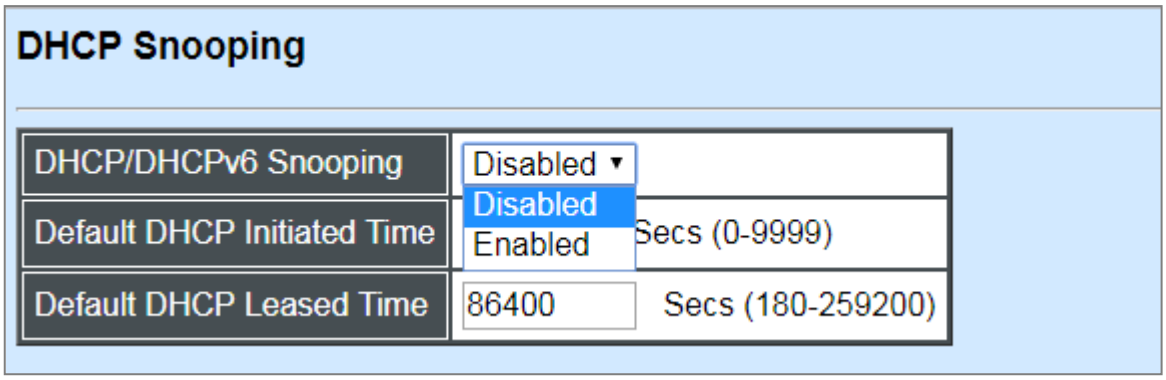
When you would like to use DHCP Snooping function, follow the steps described below to enable a client to receive an IP from DHCP server.

Step 1. Select each port's IP type



Select "Unlimited" or "DHCP"

Step 2. Enable DHCP Snooping



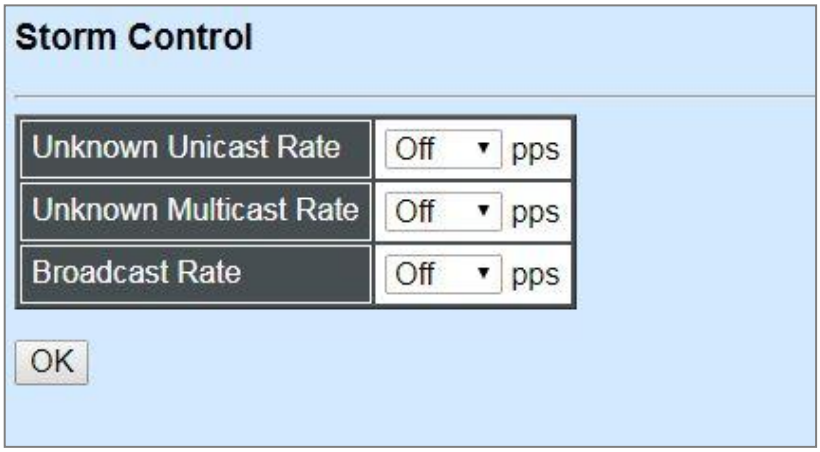
Step 3. Connect your clients to the Managed Switch

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.

4.4.12.7 Storm Control

Select the option **Storm Control** from the **Security Configuration** menu to set up storm control parameters for ports and then the following screen page appears.



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

Three options of frame traffic are provided to allow users to enable or disable the storm control.

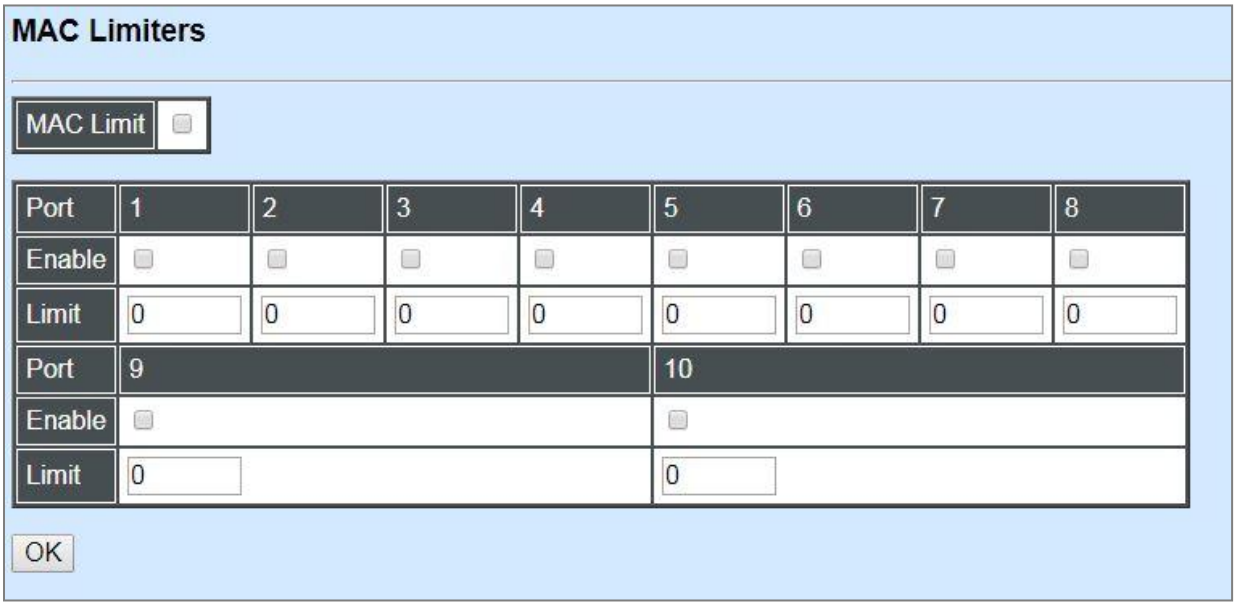
Unknown Unicast Rate: Enable or disable unknown Unicast traffic control and set up unknown Unicast Rate packet per second (pps). 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k can be chosen from this pull-down menu.

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

Broadcast Rate: Enable or disable Broadcast traffic control and set up broadcast Rate packet per second (pps). 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k can be chosen from this pull-down menu..

4.4.12.8 MAC Limiters

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



MAC Limit: Globally enable the MAC Limit function of the switch. After that, proceed to further port settings as shown below.

Port: The number of each port.

Enable: Click on the checkbox of the corresponding port number to enable the MAC Limit function on the specific port(s). Please note that port mac address table will be erased if the Mac Limit function is enabled.

Limit: Specify the maximum number of source MAC that can be learned. “0” indicates there is no limit on specified ports. The range of number that can be configured is 0~1024.

4.4.13 Access Control List (ACL) Configuration

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 rules applied to port numbers to permit or deny actions.

Select the folder **ACL Configuration** from the **Switch Management** menu and then the following screen page appears.

ACL Configuration

Rule ID	Status	Rule ID	Status	Rule ID	Status	Rule ID	Status	Rule ID	Status	Rule ID	Status
1	invalid	2	invalid	3	invalid	4	invalid	5	invalid	6	invalid
7	invalid	8	invalid	9	invalid	10	invalid	11	invalid	12	invalid
13	invalid	14	invalid	15	invalid	16	invalid	17	invalid	18	invalid
19	invalid	20	invalid	21	invalid	22	invalid	23	invalid	24	invalid
25	invalid	26	invalid	27	invalid	28	invalid	29	invalid	30	invalid
31	invalid	32	invalid	33	invalid	34	invalid	35	invalid	36	invalid
37	invalid	38	valid	39	invalid	40	invalid	41	invalid	42	invalid
43	invalid	44	invalid	45	invalid	46	invalid	47	invalid	48	invalid
49	invalid	50	invalid	51	invalid	52	invalid	53	invalid	54	invalid
55	invalid	56	invalid	57	invalid	58	invalid	59	invalid	60	invalid
61	invalid	62	invalid	63	invalid	64	invalid	65	invalid	66	invalid
67	invalid	68	invalid	69	invalid	70	invalid	71	invalid	72	invalid
73	invalid	74	invalid	75	invalid	76	invalid	77	invalid	78	invalid
79	invalid	80	invalid	81	invalid	82	invalid	83	invalid	84	invalid
85	invalid	86	invalid	87	invalid	88	invalid	89	invalid	90	invalid
91	invalid	92	invalid	93	invalid	94	invalid	95	invalid	96	invalid
97	invalid	98	invalid	99	invalid	100	invalid	101	invalid	102	invalid
103	invalid	104	invalid	105	invalid	106	invalid	107	invalid	108	invalid
109	invalid	110	invalid	111	invalid	112	invalid	113	invalid	114	invalid
115	invalid	116	invalid	117	invalid	118	invalid	119	invalid	120	invalid
121	invalid	122	invalid	123	invalid	124	invalid	125	invalid	126	invalid
127	invalid	128	invalid	129	invalid	130	invalid	131	invalid	132	invalid
133	invalid	134	invalid	135	invalid	136	invalid	137	invalid	138	invalid
139	invalid	140	invalid	141	invalid	142	invalid	143	invalid	144	invalid
145	invalid	146	invalid	147	invalid	148	invalid	149	invalid	150	invalid
151	invalid	152	invalid	153	invalid	154	invalid	155	invalid	156	invalid
157	invalid	158	invalid	159	invalid	160	invalid	161	invalid	162	invalid
163	invalid	164	invalid	165	invalid	166	invalid	167	invalid	168	invalid
169	invalid	170	invalid	171	invalid	172	invalid	173	invalid	174	invalid
175	invalid	176	invalid	177	invalid	178	invalid	179	invalid	180	invalid
181	invalid	182	invalid	183	invalid	184	invalid	185	invalid	186	invalid
187	invalid	188	invalid	189	invalid	190	invalid	191	invalid	192	invalid

Edit Delete

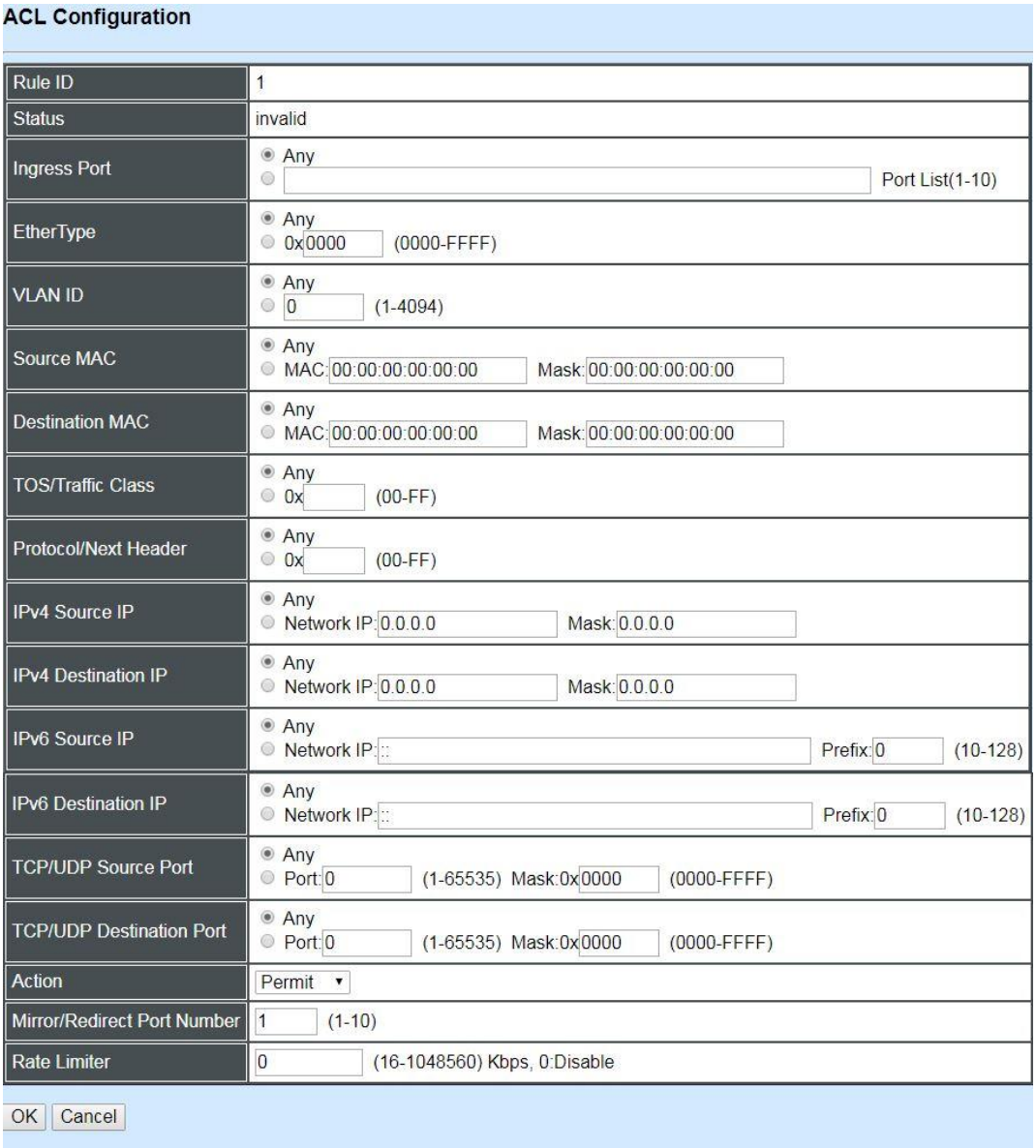
Refresh

This is the overview of ACL status.

Rule ID: The identification number for each rule.

Status: The current status for each rule.

Click **"Edit"** to modify settings of the specified rule and then the following screen page appears. Click **"Delete"** to remove a rule configured. Click **"Refresh"** to update the latest status.



Rule ID: Specify a rule ID. A port can only use one rule ID; however, a rule ID can be applied to many ports.

Status: View only field shows the status of this rule.

Ingress Port: Select "Any" or specify a port number as the ingress port.

EtherType: Select "Any" or specify an Ethernet type value.

VLAN ID: Select “Any” or specify a VLAN ID.

Source MAC: Select “Any” or specify a source MAC address.

Destination MAC: Select “Any” or specify a destination MAC address.

TOS/Traffic Class: Select “Any” or specify a TOS/Traffic class.

Protocol/Next Header: Specify IPv4 protocol and IPv6 next header

IPv4 Source IP: Select “Any” or specify an IPv4 Source IP address.

IPv4 Destination IP: Select “Any” or specify an IPv4 Destination IP address.

IPv6Source IP: Select “Any” or specify an IPv6 Source IP address.

IPv6 Destination IP: Select “Any” or specify an IPv6 Destination IP address.

TCP/UDP Source Port: Select “Any” to filter frames from any source port or specify a source port number.

TCP/UDP Destination Port: Select “Any” to filter frames bound for any destination port or specify a destination port number.

Action: Deny or permit the action.

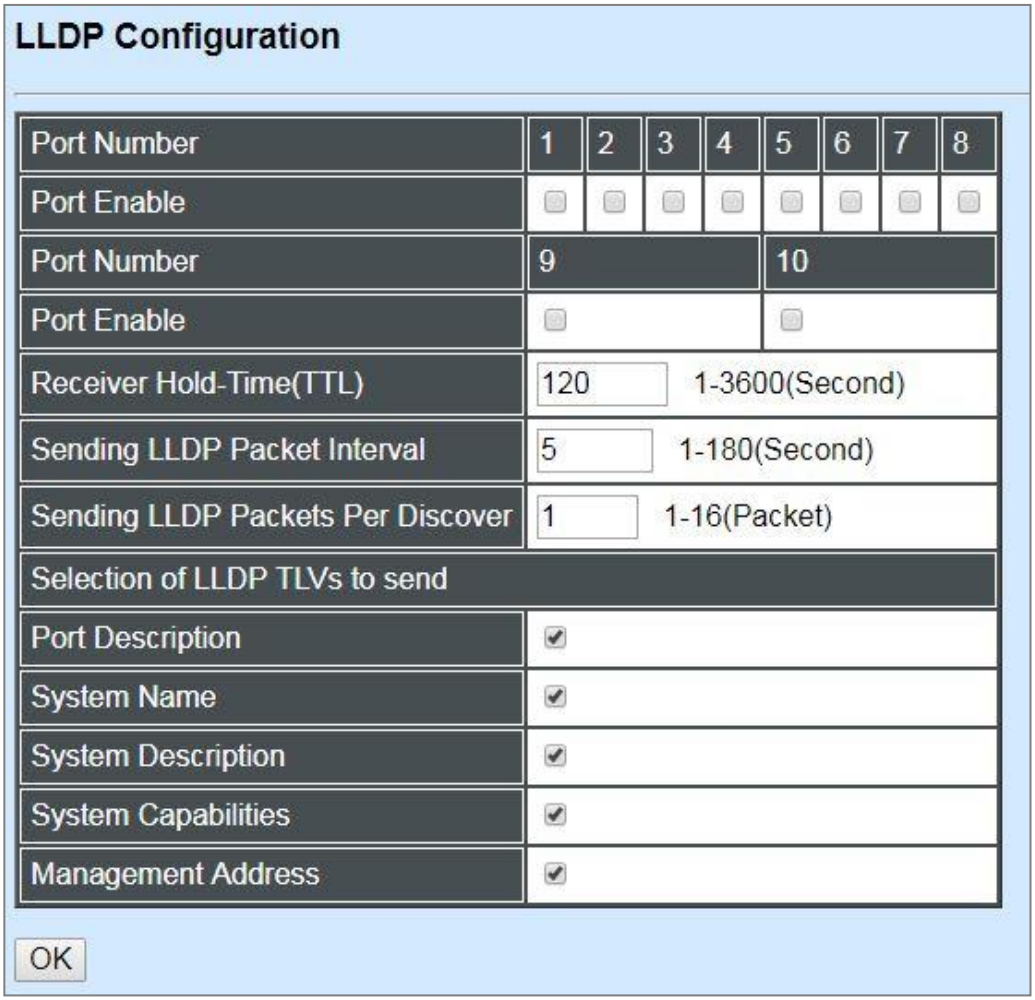
Mirror/Redirect Port Number: Specify a port number that you would like to configure for Mirror/Redirect.

Rate Limiter: Configure the rate limiter. Valid Range: (16-1048560) Kbps, 0:Disable.

4.4.14 LLDP Configuration

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

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



Port Number: Click on the checkbox of corresponding port number to enable LLDP function on the specific port(s).

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

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

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

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

4.4.15 Loop Detection Configuration

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

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

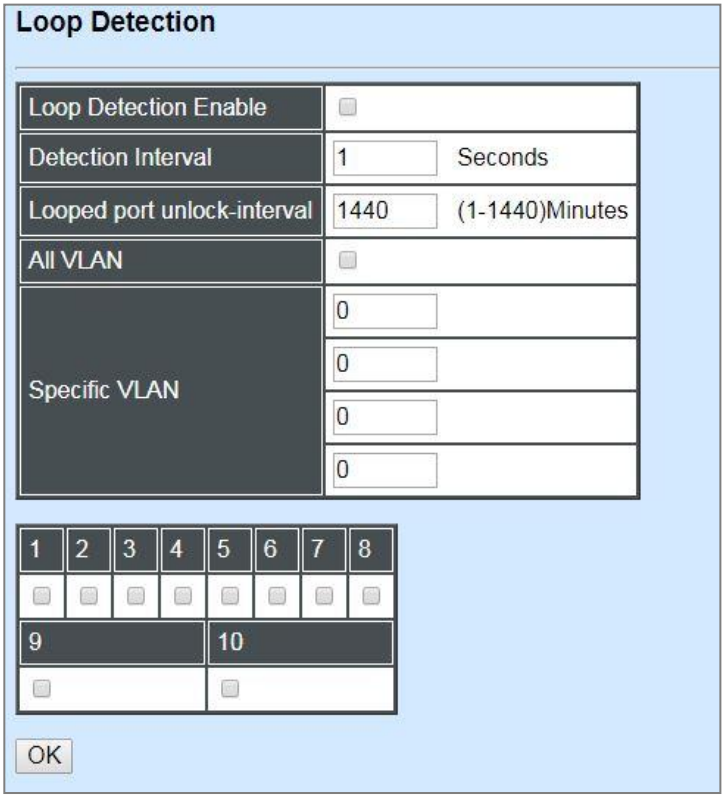
1. It blocks the relevant port to prevent broadcast storms. In other words, the system stops forwarding all the traffic via the looped port. However, the system will process the loop detection packet received on the looped port.
2. It slowly blinks the LED of looped port in orange.
3. It periodically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

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

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

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

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



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

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

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

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

60* "Looped port unlock-interval" ≧ 10* "Detection Interval"

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

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

***NOTE:** When All VLAN 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.

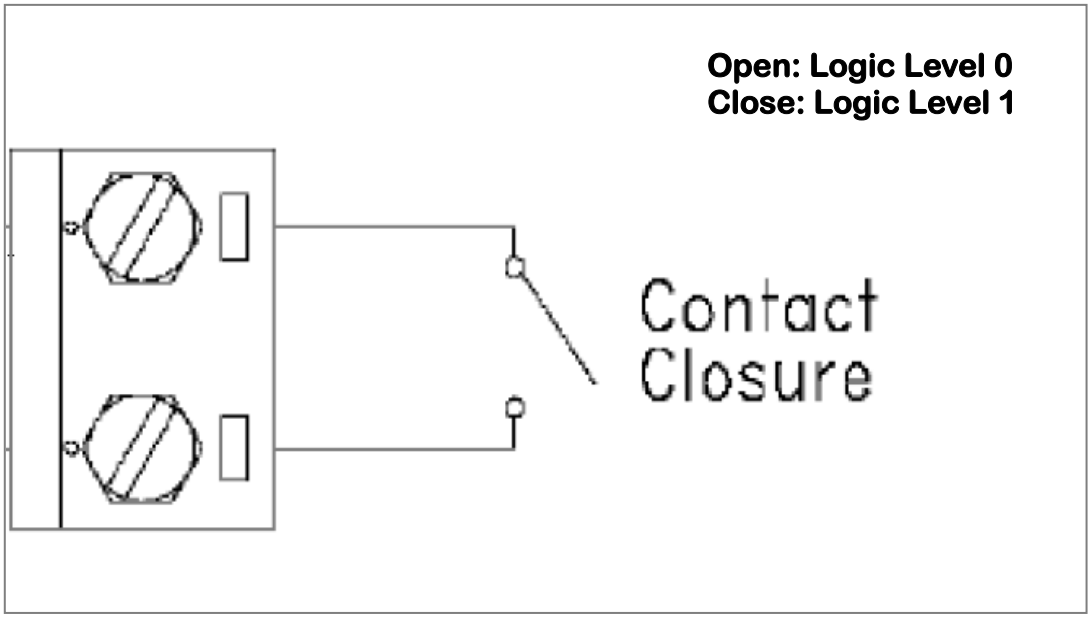
***NOTE:** The configured "Specific VLAN" takes effect when All VLAN check-box is unchecked.*

Port No.: 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) is not allowed to be enabled on the same port at the same time.*

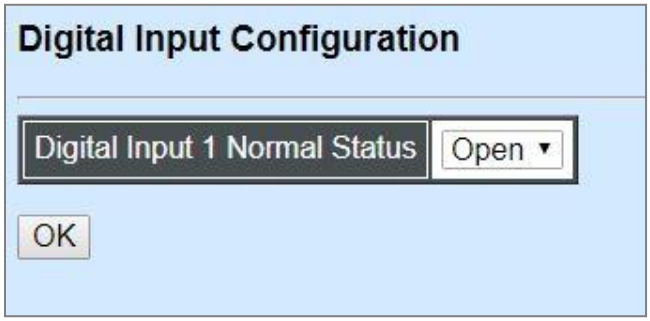
4.4.16 Digital Input Configuration

The DI (Digital Input) with a dry contact is a voltage-free connector that is used to decide whether the trigger occurs or not by detecting its open/close status. Refer to the following figure for the DI configuration.



4.4.16.1 Digital Input Configuration

To set up digital input function, select the option **Digital Input Config** from the **Switch Management** menu and then the following screen page appears.



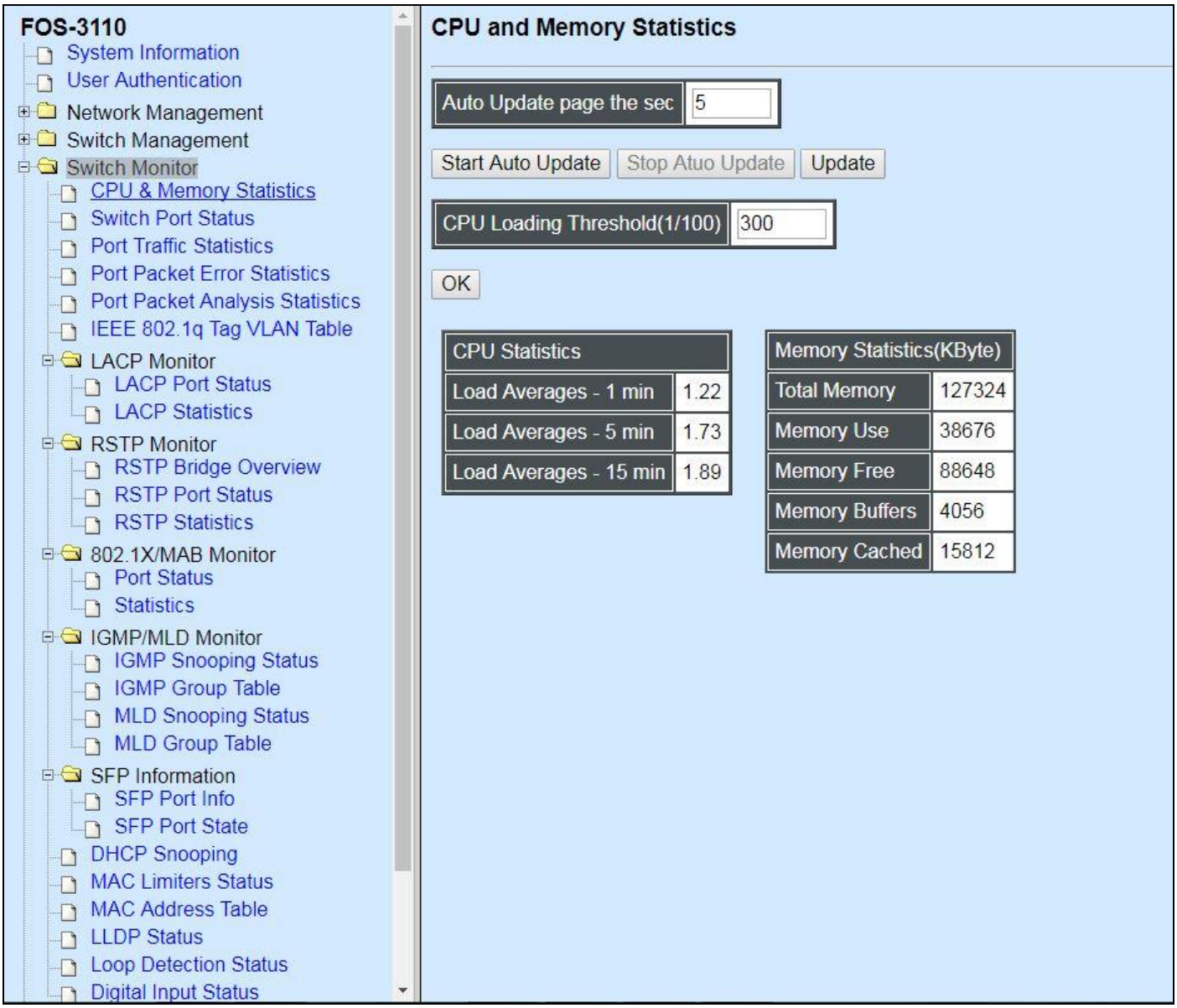
There is one Digital Input Normal Status option is shown on the screen page. Normal Status refers to where the contact remains in one state unless actuated. The contact can either be normally open until closed by operation of the switch, or normally closed and opened by the switch action. You may choose either “Open” or “Close” as the normal status of electrical circuit by clicking this pull-down menu.

Note: *Digital Input event log can be seen both in the Even Log webpage under the System Utility Menu and SNMP trap (Digital Input Start trap is enabled) if the alarm is activated.*

Digital Input-1 Normal Status: Set up the normal status between “Open” or “Close” status for the digital input of the Managed Switch. Click **OK** to save the setting.

4.5 Switch Monitor

Switch Monitor allows users to monitor the real-time operation status of the Managed Switch. Users may monitor the port link-up status or traffic counters for maintenance or diagnostic purposes. Select the folder **Switch Monitor** from the **Main Menu** and then several options and folders will be displayed for your selection



1. **CPU & Memory Statistics:** Manually or automatically update statistics of CPU & Memory and view them.

2. **Switch Port Staus:** View current port media type, port state, etc.

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

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

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

6. **IEEE802.1q Tag VLAN Table:** View the IEEE802.1q Tag VLAN Table of the Managed Switch.

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

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

9. **802.1X/MAB Monitor:** View port status and Statistics.

10. **IGMP/MLD Monitor:** View-only field that shows IGMP status and Groups table.

11. **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..

12. **DHCP Snooping:** View the DHCP learning table, etc..

13. **MAC Limiters Status:** View the status of MAC limiting configuration.

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

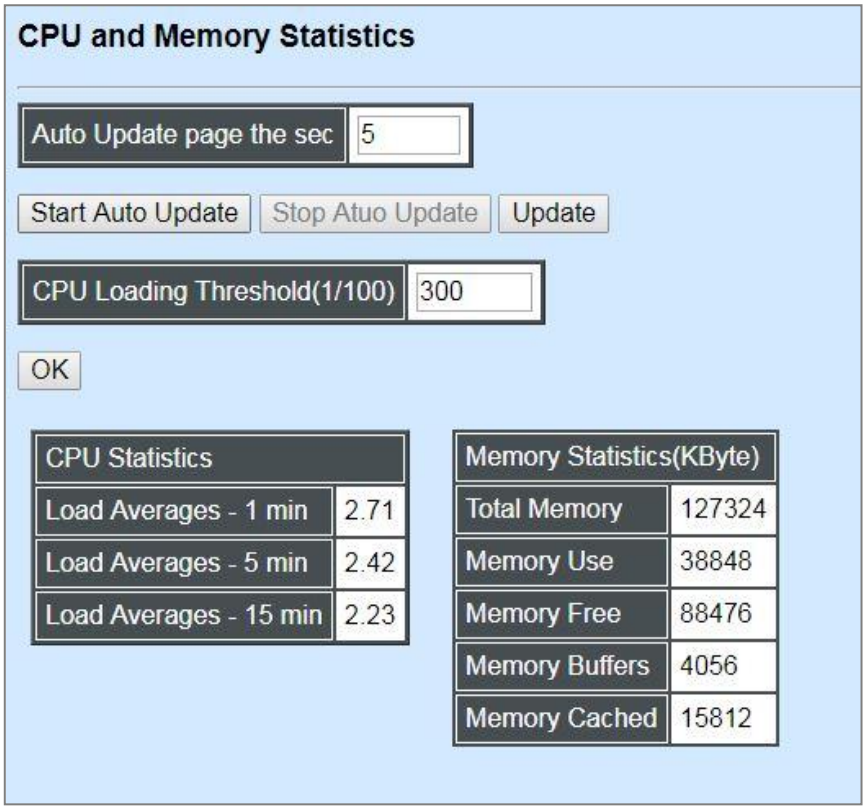
15. **LLDP Status:** View the TLV information sent by the connected device with LLDP-enabled.

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

17. **Digital Input Status:** View the current Digital Input and alarm status of the Managed Switch.

4.5.1 CPU and Memory Statistics

CPU & Memory Statistics is to manually or automatically update statistics of CPU and Memory. Click "**CPU & Memory Statistics**" and the following screen appears.



Auto Update page the sec: Automatically updates statistics of CPU & Memory at a specified interval in seconds.

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.

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.

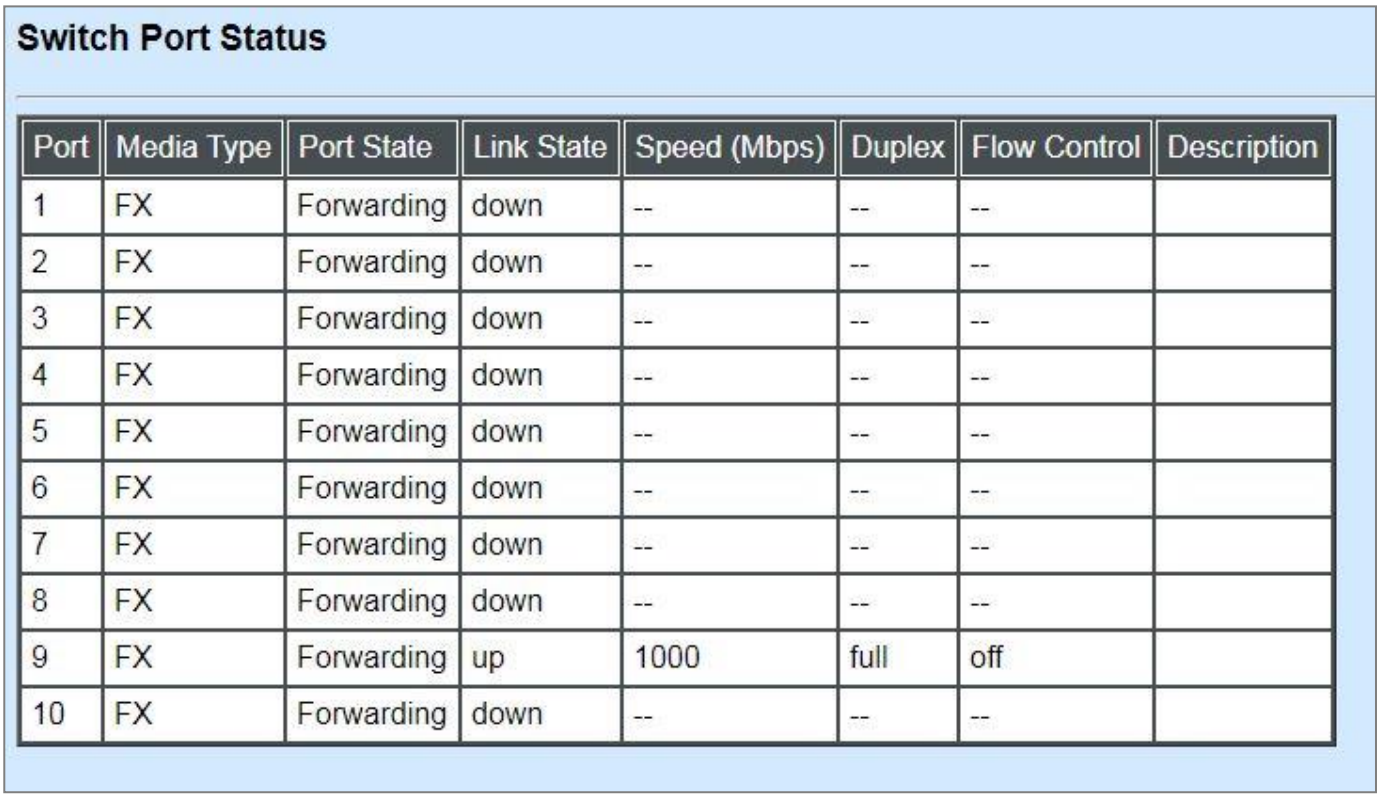
Memory Free: The memory in kilobytes that is idle.

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.

4.5.2 Switch Port Status

In order to view the real-time port status of the Managed Switch, select **Switch Port State** from the **Switch Monitor** menu and then the following screen page appears.



Switch Port Status

Port	Media Type	Port State	Link State	Speed (Mbps)	Duplex	Flow Control	Description
1	FX	Forwarding	down	--	--	--	
2	FX	Forwarding	down	--	--	--	
3	FX	Forwarding	down	--	--	--	
4	FX	Forwarding	down	--	--	--	
5	FX	Forwarding	down	--	--	--	
6	FX	Forwarding	down	--	--	--	
7	FX	Forwarding	down	--	--	--	
8	FX	Forwarding	down	--	--	--	
9	FX	Forwarding	up	1000	full	off	
10	FX	Forwarding	down	--	--	--	

Port Number: The number of the port.

Media Type: The media type of the port, either TX or FX.

Port State: This shows each port's state which can be Disabled, Blocking/Listening, Learning or Forwarding.

Disabled: A port in this state does not participate in frame relay or the operation of the Spanning Tree Algorithm and Protocol if any.

Blocking: A Port in this state does not participate in frame relay; thus, it prevents frame duplication arising from multiple paths existing in the active topology of Bridged LAN.

Learning: A port in this state prepares to participate in frame relay. Frame relay is temporarily disabled in order to prevent temporary loops, which may occur in a Bridged LAN during the lifetime of this state as the active topology of the Bridged LAN changes. Learning is enabled to allow information to be acquired prior to frame relay in order to reduce the number of frames that are unnecessarily relayed.

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

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

Speed (Mbps): The current operation speed of ports, which can be 10M, 100M or 1000M.

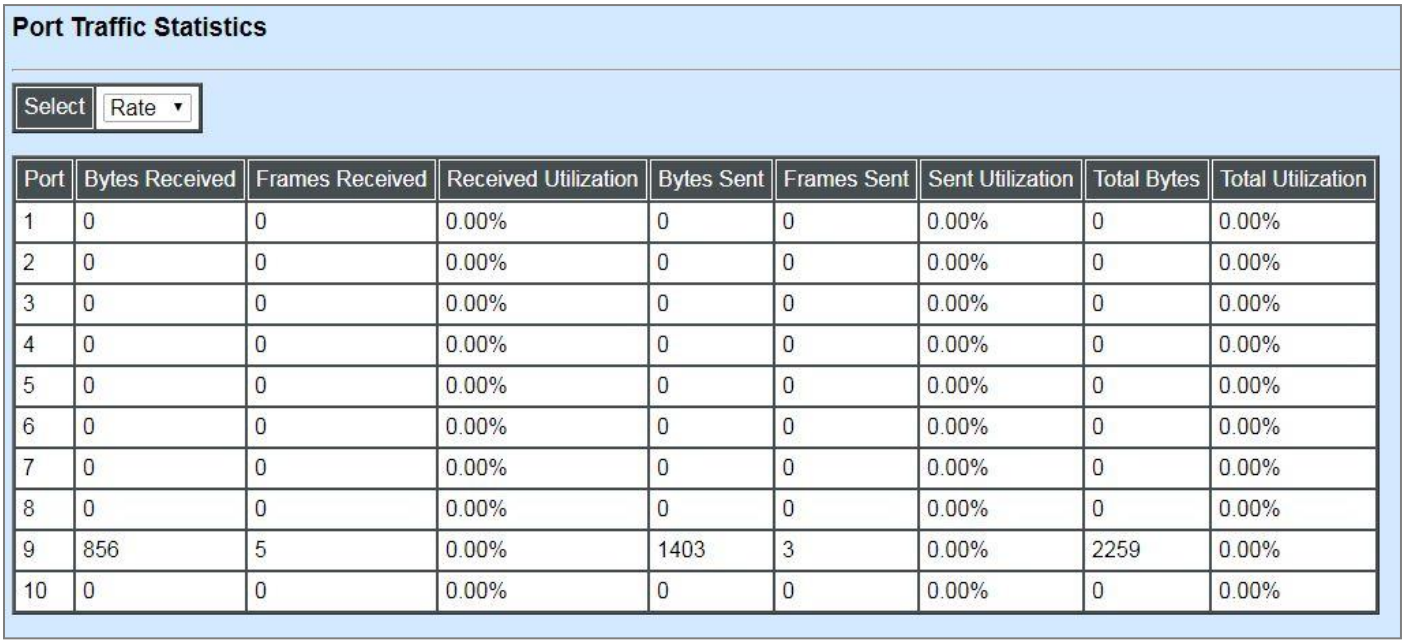
Duplex: The current operation Duplex mode of the port, either Full or Half.

Flow Control: The current state of Flow Control, either on or off.

Description: Display the port description you set up in Port Configuration.

4.5.3 Port Traffic Statistics

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



Port	Bytes Received	Frames Received	Received Utilization	Bytes Sent	Frames Sent	Sent Utilization	Total Bytes	Total Utilization
1	0	0	0.00%	0	0	0.00%	0	0.00%
2	0	0	0.00%	0	0	0.00%	0	0.00%
3	0	0	0.00%	0	0	0.00%	0	0.00%
4	0	0	0.00%	0	0	0.00%	0	0.00%
5	0	0	0.00%	0	0	0.00%	0	0.00%
6	0	0	0.00%	0	0	0.00%	0	0.00%
7	0	0	0.00%	0	0	0.00%	0	0.00%
8	0	0	0.00%	0	0	0.00%	0	0.00%
9	856	5	0.00%	1403	3	0.00%	2259	0.00%
10	0	0	0.00%	0	0	0.00%	0	0.00%

Select: 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.

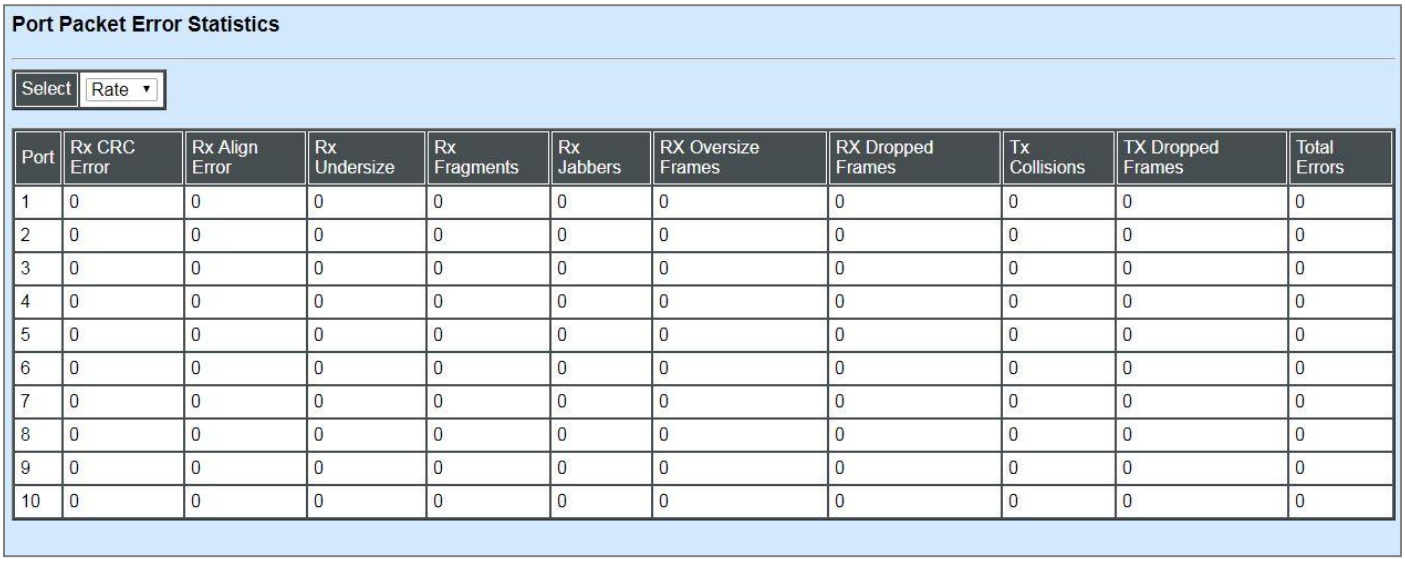
Total Bytes: Total bytes of receiving and sending from current port.

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

Clear All: All port's counter values will be cleared and set back to zero if “Event” option is chosen from **Select** pull-down menu.

4.5.4 Port Packet Error Statistics

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



Port	Rx CRC Error	Rx Align Error	Rx Undersize	Rx Fragments	Rx Jabbers	RX Oversize Frames	RX Dropped Frames	Tx Collisions	TX Dropped Frames	Total Errors
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0

Select: 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 Frames: Undersize frames received.

RX Fragments Frames: Fragments frames received.

RX Jabber Frames: Jabber frames received.

RX Oversize Frames: Oversize frames received.

RX Dropped Frames: Drop frames received.

TX Collision: Each port’s Collision frames.

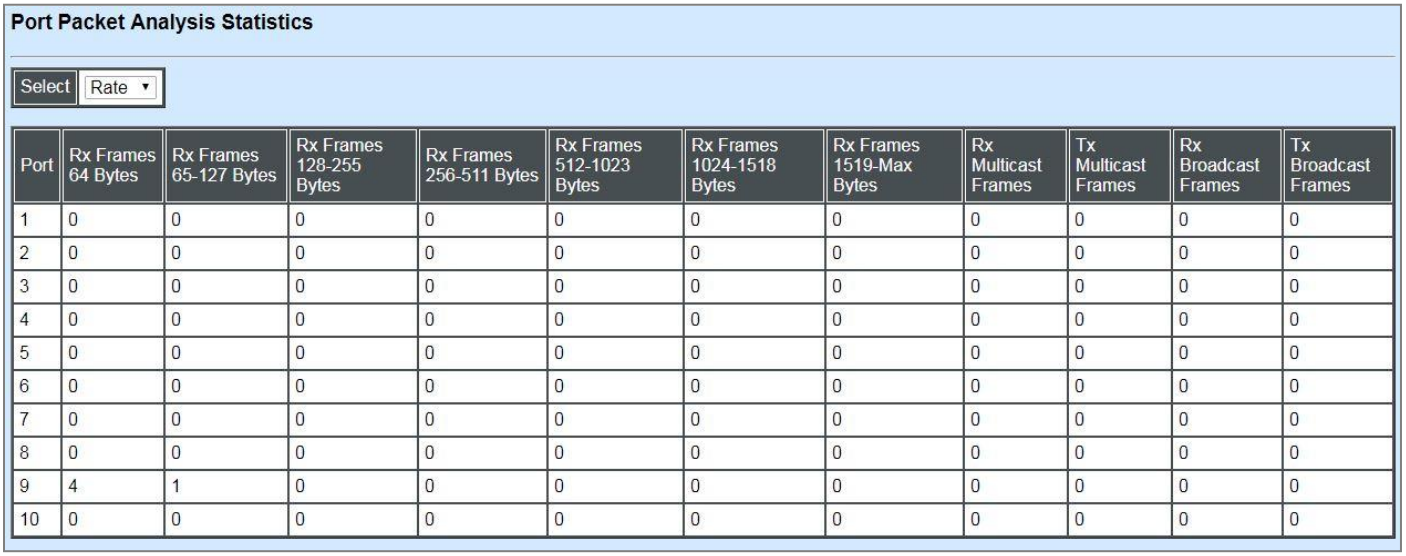
TX Dropped Frames: Drop frames sent.

Total Errors: Total error frames received.

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

4.5.5 Port Packet Analysis Statistics

Port Packet Analysis Statistics Mode Counters allow users to view the port analysis history of the Managed Switch. Event mode counters are calculated since the last time that counter was reset or cleared. Select **Port Packet Analysis Statistics** from the **Switch Monitor** menu and then the following screen page appears.



Port	Rx Frames 64 Bytes	Rx Frames 65-127 Bytes	Rx Frames 128-255 Bytes	Rx Frames 256-511 Bytes	Rx Frames 512-1023 Bytes	Rx Frames 1024-1518 Bytes	Rx Frames 1519-Max Bytes	Rx Multicast Frames	Tx Multicast Frames	Rx Broadcast Frames	Tx Broadcast Frames
1	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0
9	4	1	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0

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

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.

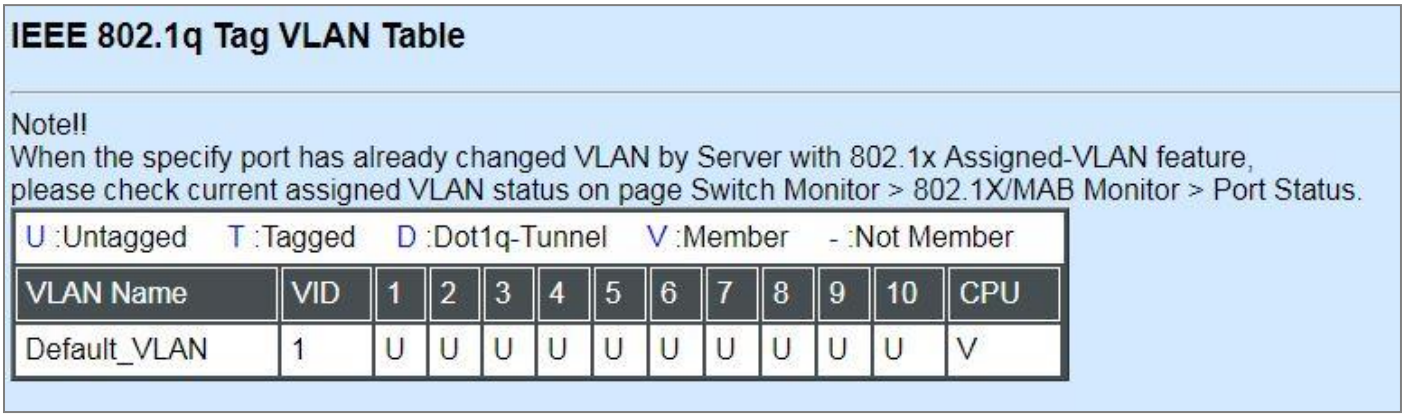
RX Broadcast Frames: Good broadcast frames received.

TX Broadcast Frames: Good broadcast packets sent.

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

4.5.6 IEEE 802.1q Tag VLAN Table

Select **IEEE 802.1q Tag VLAN Table** from the **Switch Monitor** menu and then the following screen page appears.

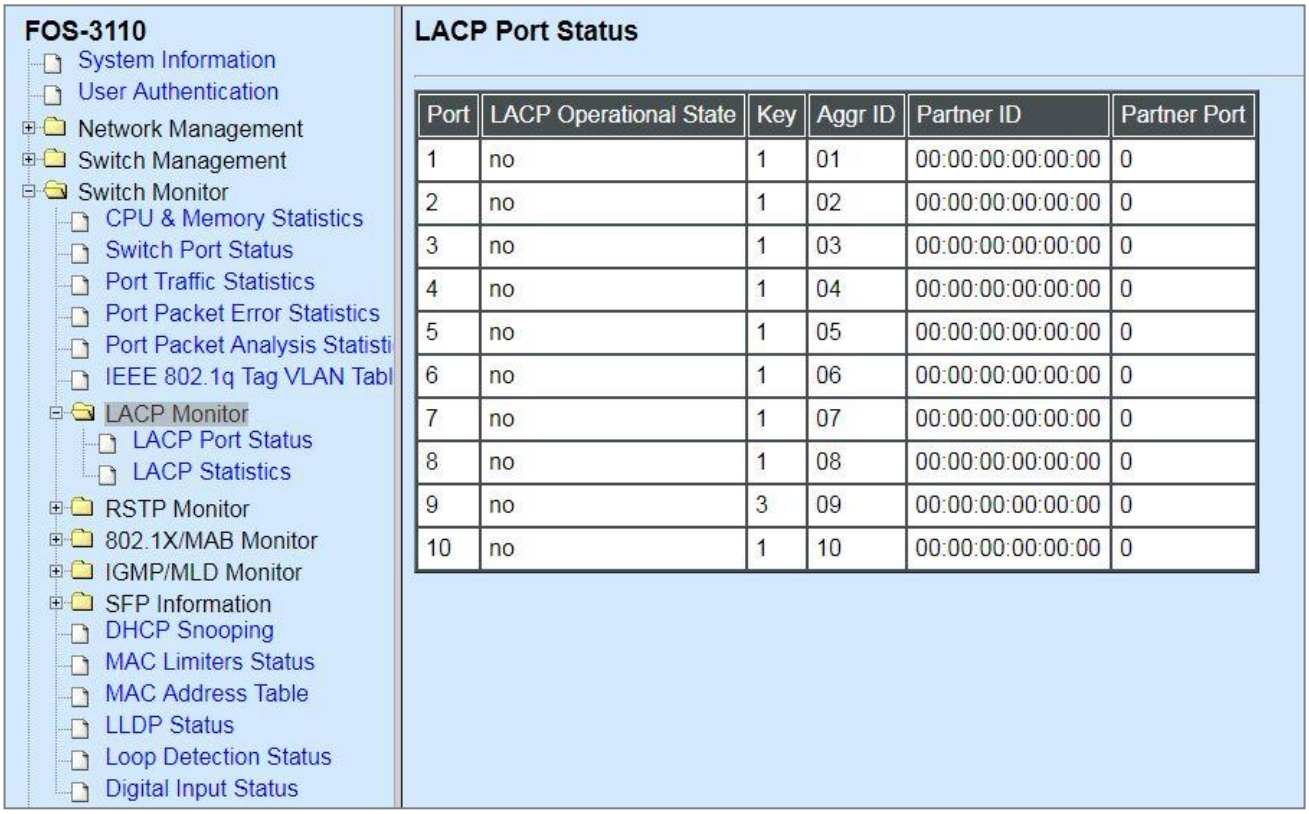


VLAN Name: View-only filed that shows the VLAN name.

VID: View-only filed that shows the VID.

4.5.7 LACP Monitor

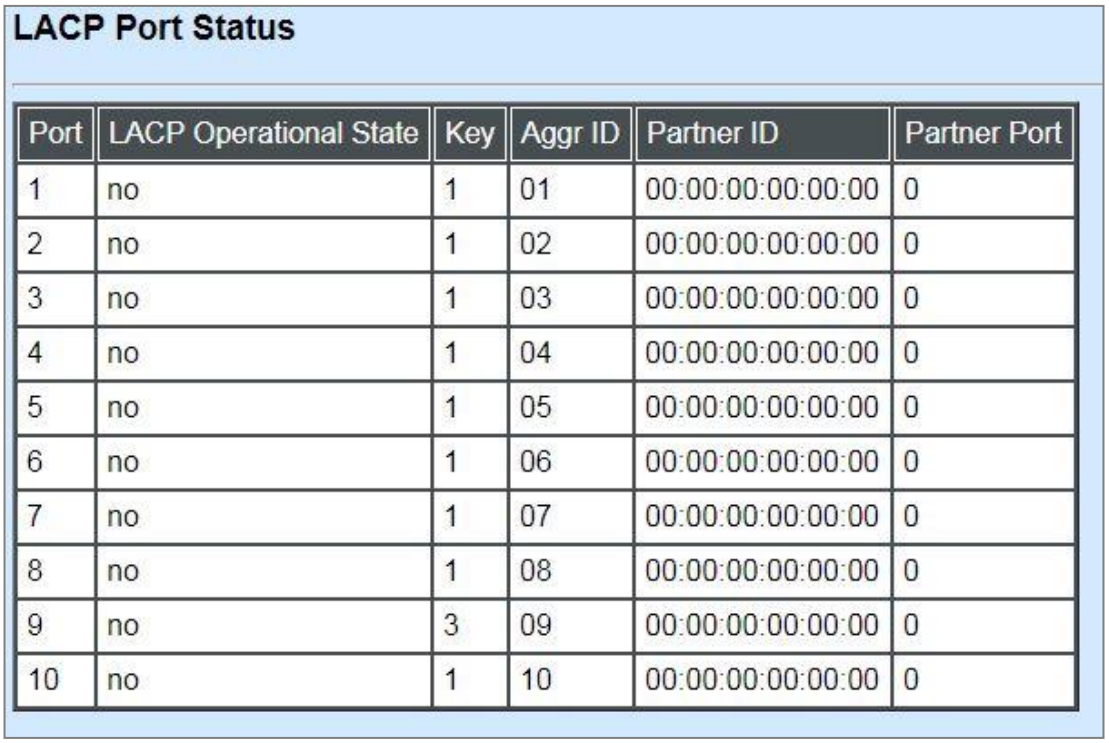
Click the **LACP Monitor** folder and then two options within this folder will be displayed.



Port	LACP Operational State	Key	Aggr ID	Partner ID	Partner Port
1	no	1	01	00:00:00:00:00:00	0
2	no	1	02	00:00:00:00:00:00	0
3	no	1	03	00:00:00:00:00:00	0
4	no	1	04	00:00:00:00:00:00	0
5	no	1	05	00:00:00:00:00:00	0
6	no	1	06	00:00:00:00:00:00	0
7	no	1	07	00:00:00:00:00:00	0
8	no	1	08	00:00:00:00:00:00	0
9	no	3	09	00:00:00:00:00:00	0
10	no	1	10	00:00:00:00:00:00	0

4.5.7.1 LACP Port Status

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



Port	LACP Operational State	Key	Aggr ID	Partner ID	Partner Port
1	no	1	01	00:00:00:00:00:00	0
2	no	1	02	00:00:00:00:00:00	0
3	no	1	03	00:00:00:00:00:00	0
4	no	1	04	00:00:00:00:00:00	0
5	no	1	05	00:00:00:00:00:00	0
6	no	1	06	00:00:00:00:00:00	0
7	no	1	07	00:00:00:00:00:00	0
8	no	1	08	00:00:00:00:00:00	0
9	no	3	09	00:00:00:00:00:00	0
10	no	1	10	00:00:00:00:00:00	0

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

Port Number: The number of the port.

LACP Operational State: The current operational state of LACP

Key: The current operational key for the LACP group.

Aggr ID: The ID of the LACP group.

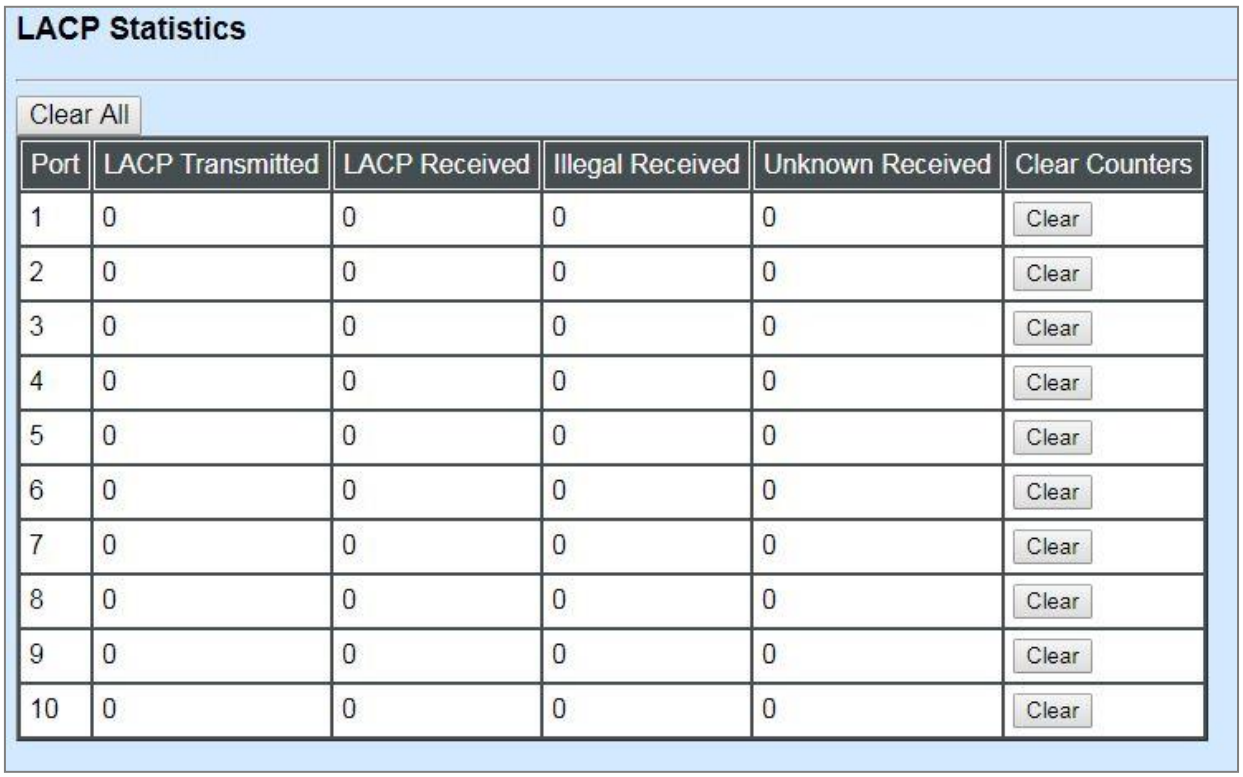
In LACP mode, link aggregation control protocol data unit (LACPDU) is used for exchanging information among LACP-enabled devices. After LACP is enabled on a port, the port sends LACPDUs to notify the remote system of its system LACP priority, system MAC address, port LACP priority, port number and operational key. Upon receipt of an LACPDU, the remote system compares the received information with the information received on other ports to determine the ports that can operate as selected ports. This allows the two systems to reach an agreement on the states of the related ports when aggregating ports, link aggregation control automatically assigns each port an operational key based on its rate, duplex mode and other basic configurations. In an LACP aggregation group, all ports share the same operational key; in a manual or static LACP aggregation, the selected ports share the same operational key.

Partner ID: The ID (MAC address) of the partner port

Partner Port: The corresponding port numbers that connect to the partner switch in LACP mode.

4.5.7.2 LACP Statistics

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



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

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

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

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

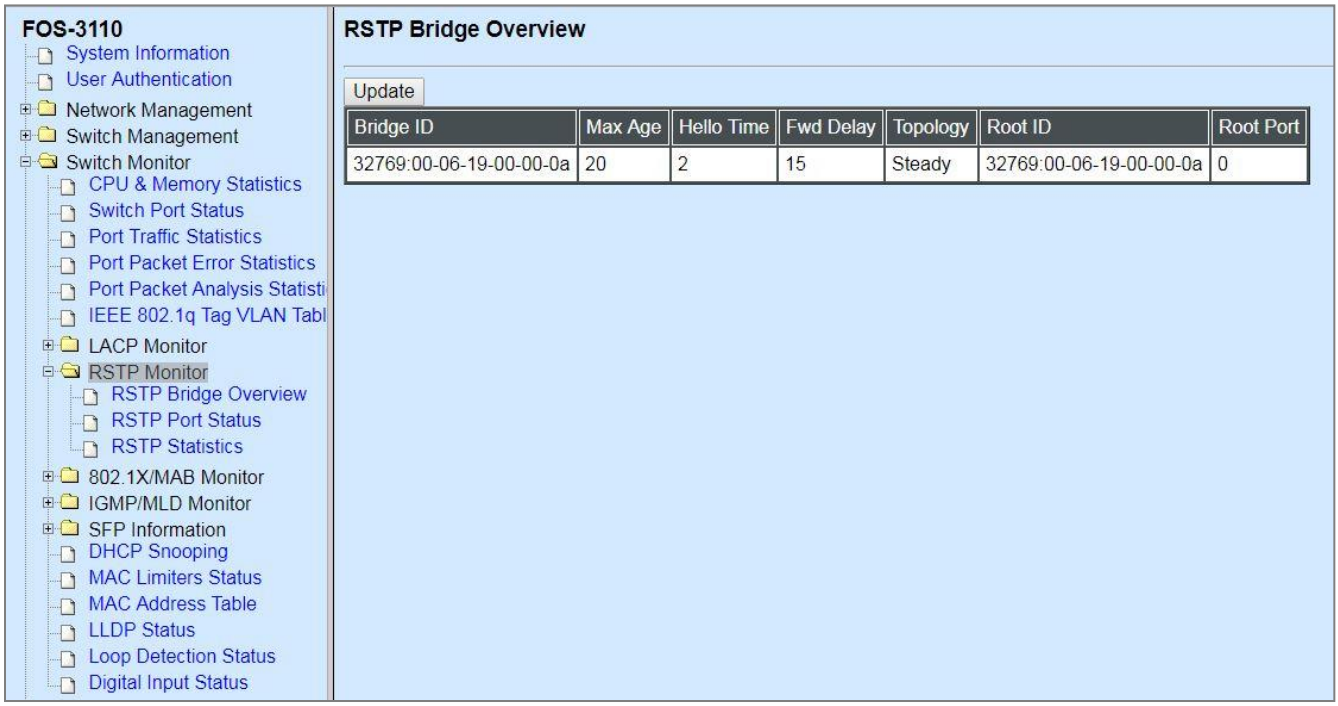
Unknown Received: The current unknown packets received from the port.

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

Clear All: Clear the statistics of all ports.

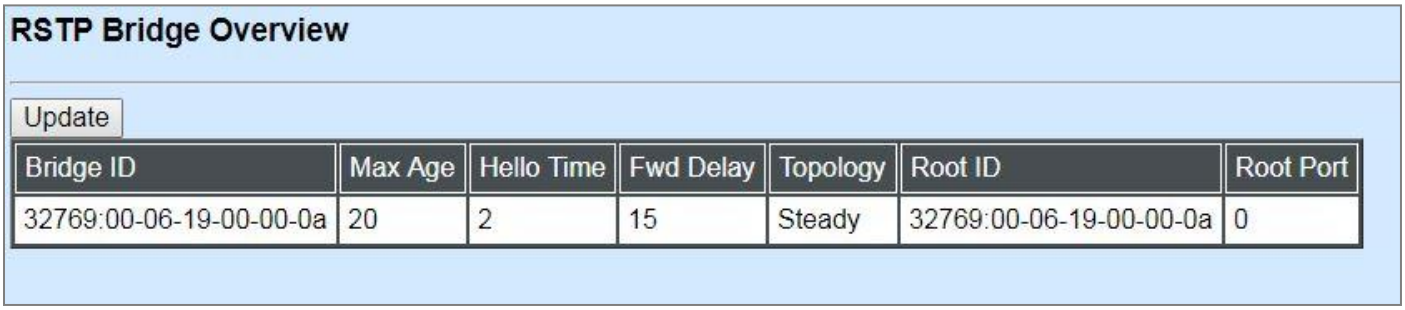
4.5.8 RSTP Monitor

Click the **RSTP Monitor** folder and then three options within this folder will be displayed.



4.5.8.1 RSTP Bridge Overview

RSTP Bridge Overview allows users to view a list of RSTP brief information, such as Bridge ID, topology status and Root ID. Select **RSTP Bridge Overview** from the **RSTP Monitor** menu and then the following screen page appears.



In this webpage, you can find the following information about RSTP bridge:

Update: Update the current status.

Bridge ID: RSTP Bridge ID of the Managed Switch

Max Age: Max Age setting of the Managed Switch.

Hello Time: Hello Time setting of the Managed Switch.

Forward Delay: The Managed Switch's setting of Forward Delay Time.

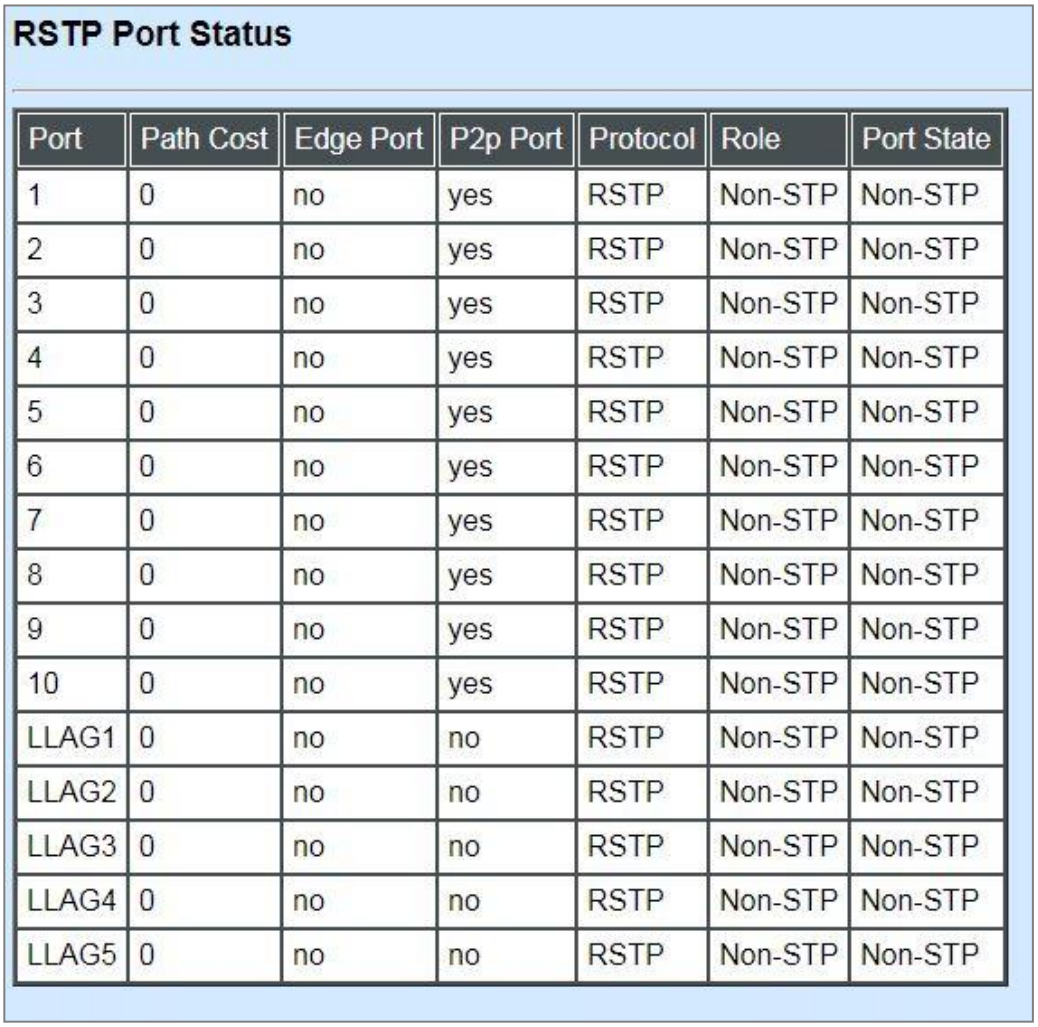
Topology: The state of the topology.

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

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

4.5.8.2 RSTP Port Status

RSTP Port Status allows users to view a list of all RSTP ports' information. Select **RSTP Port Status** from the **RSTP Monitor** menu and then the following screen page appears.



RSTP Port Status

Port	Path Cost	Edge Port	P2p Port	Protocol	Role	Port State
1	0	no	yes	RSTP	Non-STP	Non-STP
2	0	no	yes	RSTP	Non-STP	Non-STP
3	0	no	yes	RSTP	Non-STP	Non-STP
4	0	no	yes	RSTP	Non-STP	Non-STP
5	0	no	yes	RSTP	Non-STP	Non-STP
6	0	no	yes	RSTP	Non-STP	Non-STP
7	0	no	yes	RSTP	Non-STP	Non-STP
8	0	no	yes	RSTP	Non-STP	Non-STP
9	0	no	yes	RSTP	Non-STP	Non-STP
10	0	no	yes	RSTP	Non-STP	Non-STP
LLAG1	0	no	no	RSTP	Non-STP	Non-STP
LLAG2	0	no	no	RSTP	Non-STP	Non-STP
LLAG3	0	no	no	RSTP	Non-STP	Non-STP
LLAG4	0	no	no	RSTP	Non-STP	Non-STP
LLAG5	0	no	no	RSTP	Non-STP	Non-STP

In this webpage, you can find the following information about RSTP status:

Port Number: The number of the port.

Path Cost: The Path Cost of the port.

Edge Port: "Yes" is displayed if the port is the Edge port connecting to an end station and does not receive BPDU.

P2p Port: "Yes" is displayed if the port link is connected to another STP device.

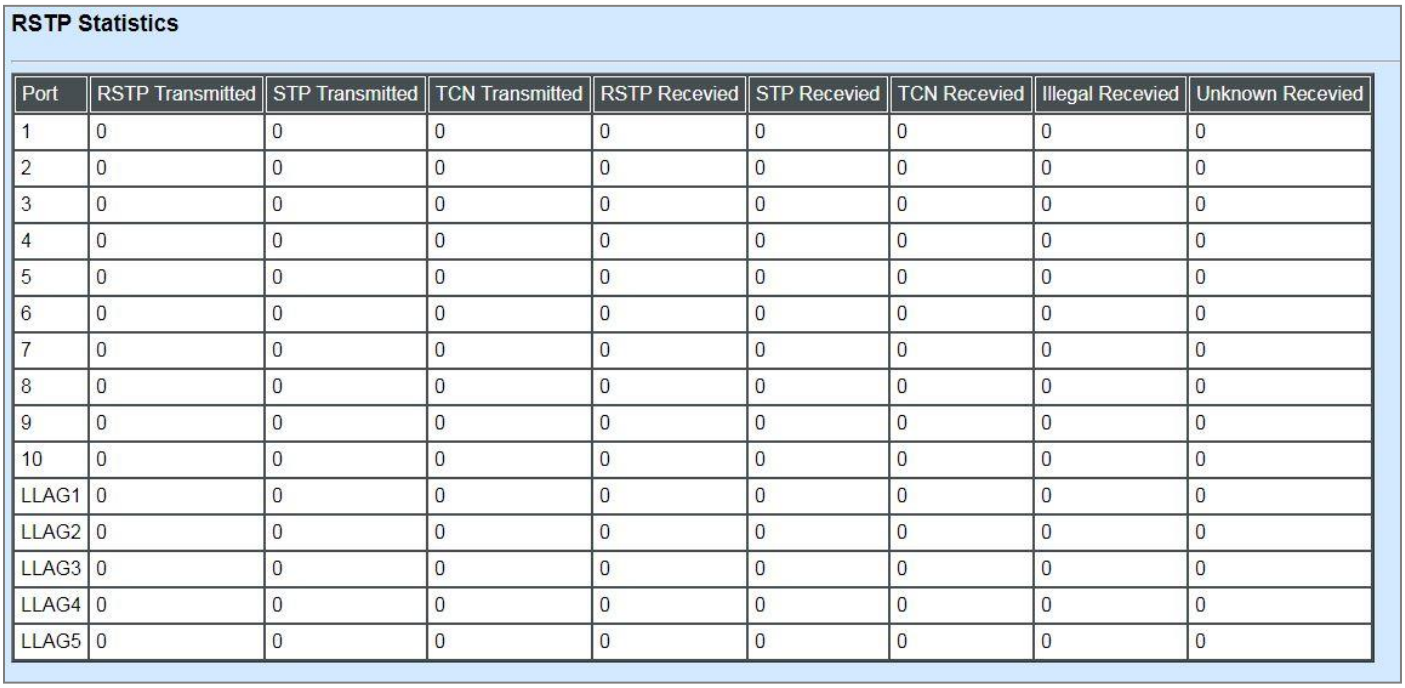
Protocol: Display RSTP or STP.

Role: Display the Role of the port (non-STP, forwarding or blocked).

Port State: Display the state of the port (non-STP, forwarding or blocked).

4.5.8.3 RSTP Statistics

In order to view the real-time RSTP statistics status of the Managed Switch, select **RSTP Statistics** from the **RSTP Monitor** menu and then the following screen page appears.


RSTP Statistics

Port	RSTP Transmitted	STP Transmitted	TCN Transmitted	RSTP Recevied	STP Recevied	TCN Recevied	Illegal Recevied	Unknown Recevied
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
LLAG1	0	0	0	0	0	0	0	0
LLAG2	0	0	0	0	0	0	0	0
LLAG3	0	0	0	0	0	0	0	0
LLAG4	0	0	0	0	0	0	0	0
LLAG5	0	0	0	0	0	0	0	0

Port Number: The number of the port.

RSTP Transmitted: The total transmitted RSTP packets from current port.

STP Transmitted: The total transmitted STP packets from current port.

TCN Transmitted: The total transmitted TCN (Topology Change Notification) packets from current port.

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

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

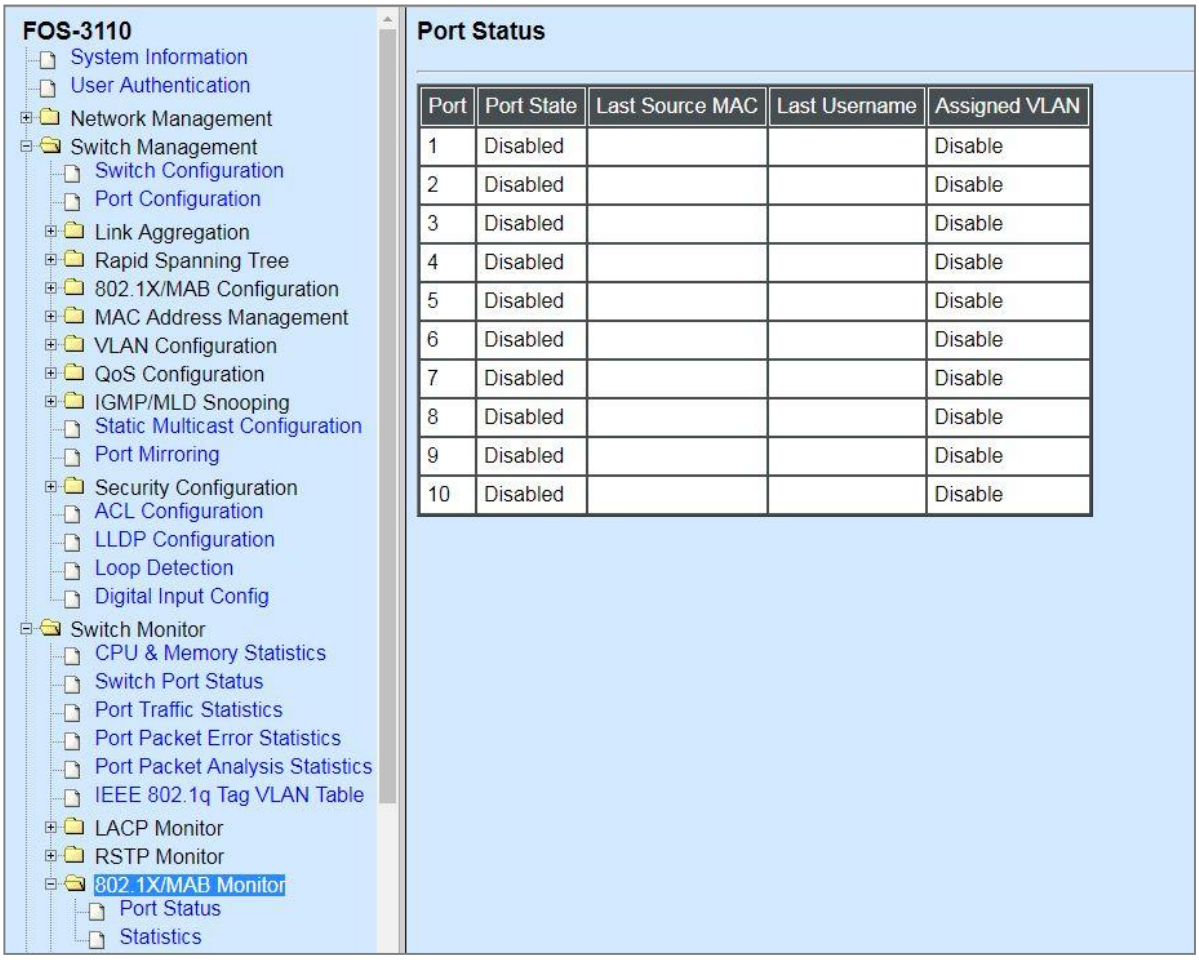
TCN Received: The total received TCN packets from current port.

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

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

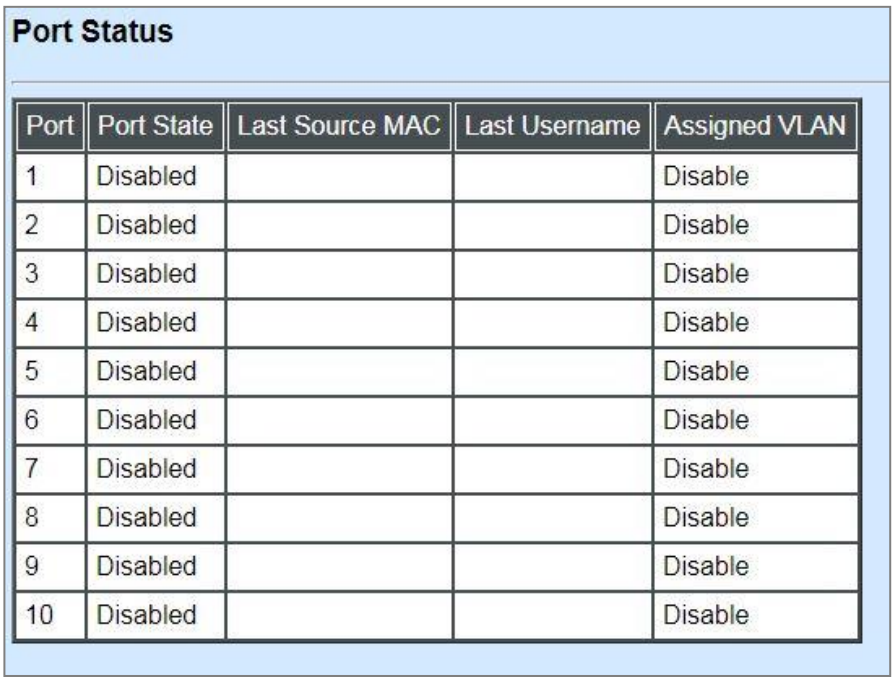
4.5.9 802.1X/MAB Monitor

Click the **802.1X/MAB Monitor** folder and then two options within this folder will be displayed.



4.5.9.1 802.1X/MAB Port Status

Port Status allows users to view a list of all 802.1x ports' information. Select **port status** from the **802.1x/MAB Monitor** menu and then the following screen page appears.



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

Port: The number of the port.

Port State: Display the number of the port 802.1x link state LinkDown or LinkUp.

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

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

Assigned VLAN: Display the VLAN assigned by 802.1xServer

4.5.9.2 802.1X/MAB Statistics

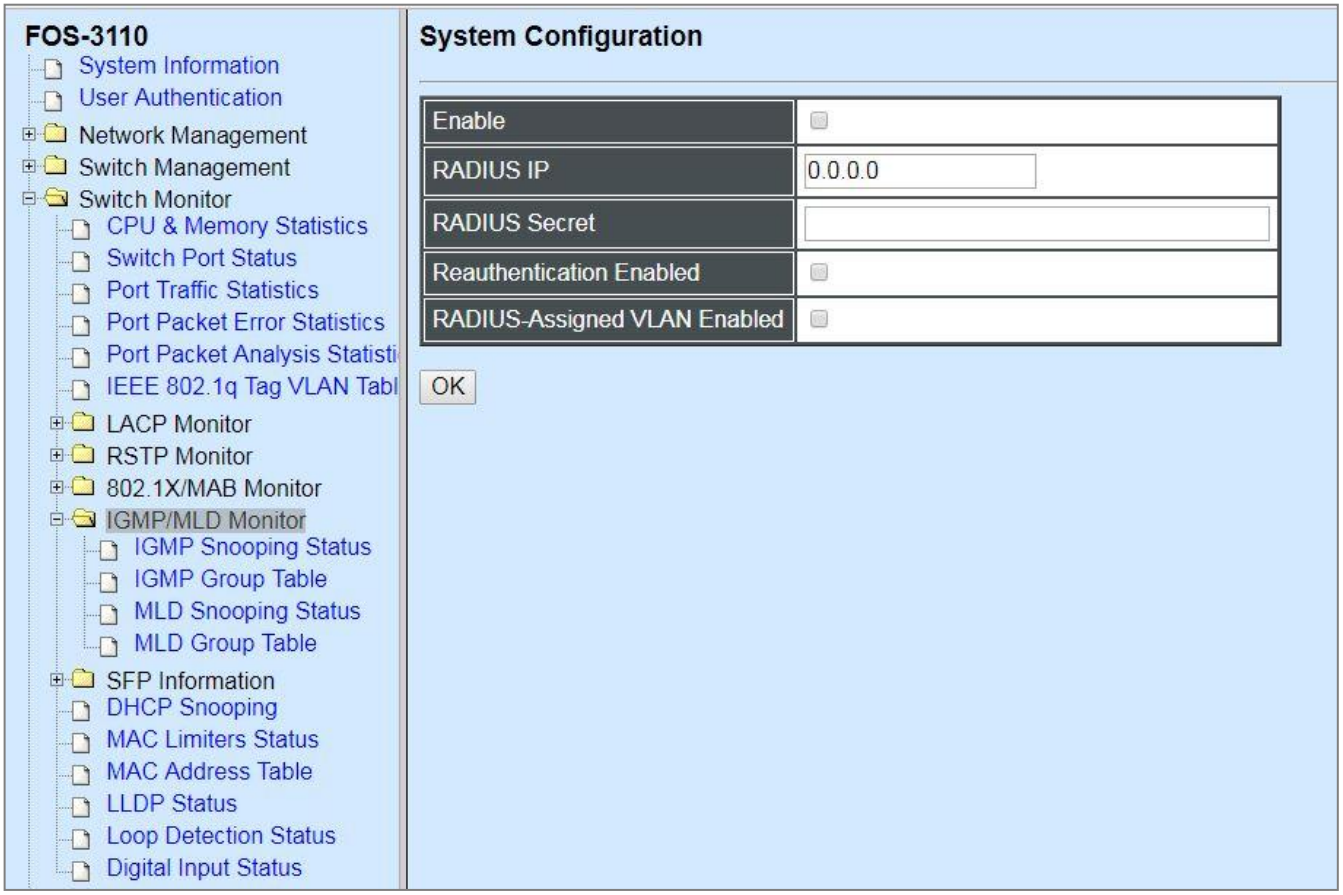
In order to view the real-time 802.1X port statistics status of the Managed Switch, select **Statistics** from the **802.1x/MAB Monitor** menu and then the following screen page shows up.

Statistics

Port	Rx Total	Rx Response ID	Rx Response	Rx Start	Rx Logoff	Rx Invalid Type	Rx Invalid Length	Rx Access Challenges	Rx Other Requests	Rx Auth. Successes	Rx Auth. Failures	Tx Total	Tx Request ID	Tx Request	Tx Responses
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

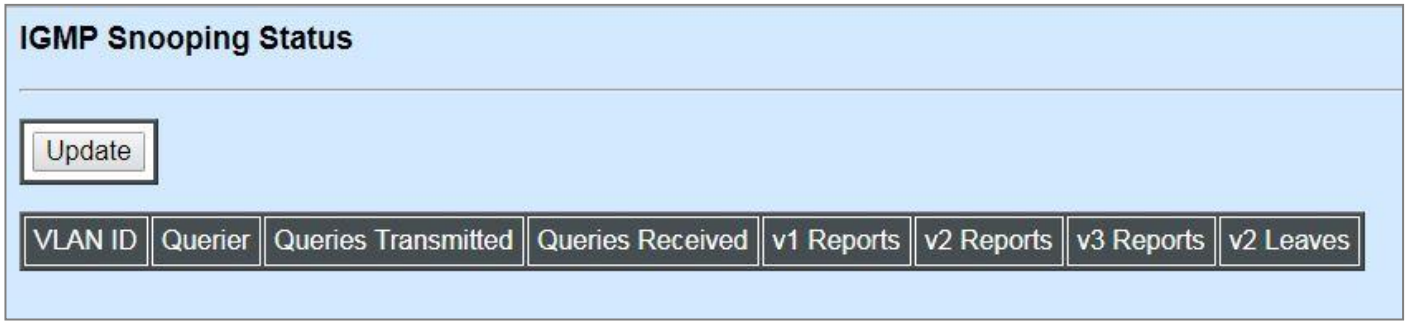
4.5.10 IGMP/MLD Monitor

Click the **IGMP/MLD Monitor** folder and then four options within this folder will be displayed.



4.5.10.1 IGMP Snooping Status

IGMP Snooping Status allows users to view a list of IGMP queries' information in VLAN(s) such as VLAN ID, Querier and Queries Transmitted/Received packets. Select **IGMP Snooping Status** from the **IGMP/MLD Monitor** menu and then the following screen page appears.



Update: Click "Update" to update the 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 IGMP general queries transmitted will be sent to IGMP hosts.

Queries Received: The total received IGMP general queries from IGMP querier.

v1 Reports: IGMP Version 1 reports.

v2 Reports: IGMP Version 2 reports.

v3 Reports: IGMP Version 3 reports.

v2 Leaves: IGMP Version 2 leaves.

4.5.10.2 IGMP Group Table

In order to view the real-time IGMP multicast group status of the Managed Switch, select **IGMP Group Table** from the **IGMP/MLD Monitor** menu and then the following screen page appears.

Update: Click “Update” to update the 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.

4.5.10.3 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 **MLD Snooping Status** from the **IGMP/MLD Monitor** menu and then the following screen page appears.

Update: Click "Update" to update the MLD snooping status.

VLAN ID: VID of the specific VLAN.

Querier: The state of MLD querier in the VLAN.

Queries Transmitted: The total MLD general queries transmitted will be sent to MLD hosts.

Queries Received: The total received MLD general queries from MLD querier.

v1 Reports: MLD Version 1 reports.

v2 Reports: MLD Version 2 reports.

Done: MLD dones

4.5.10.4 MLD Group Table

In order to view the real-time MLD multicast group status of the Managed Switch, select **MLD Group Table** from the **IGMP/MLD Monitor** menu and then the following screen page appears.

Update: Click “Update” to update the MLD group table.

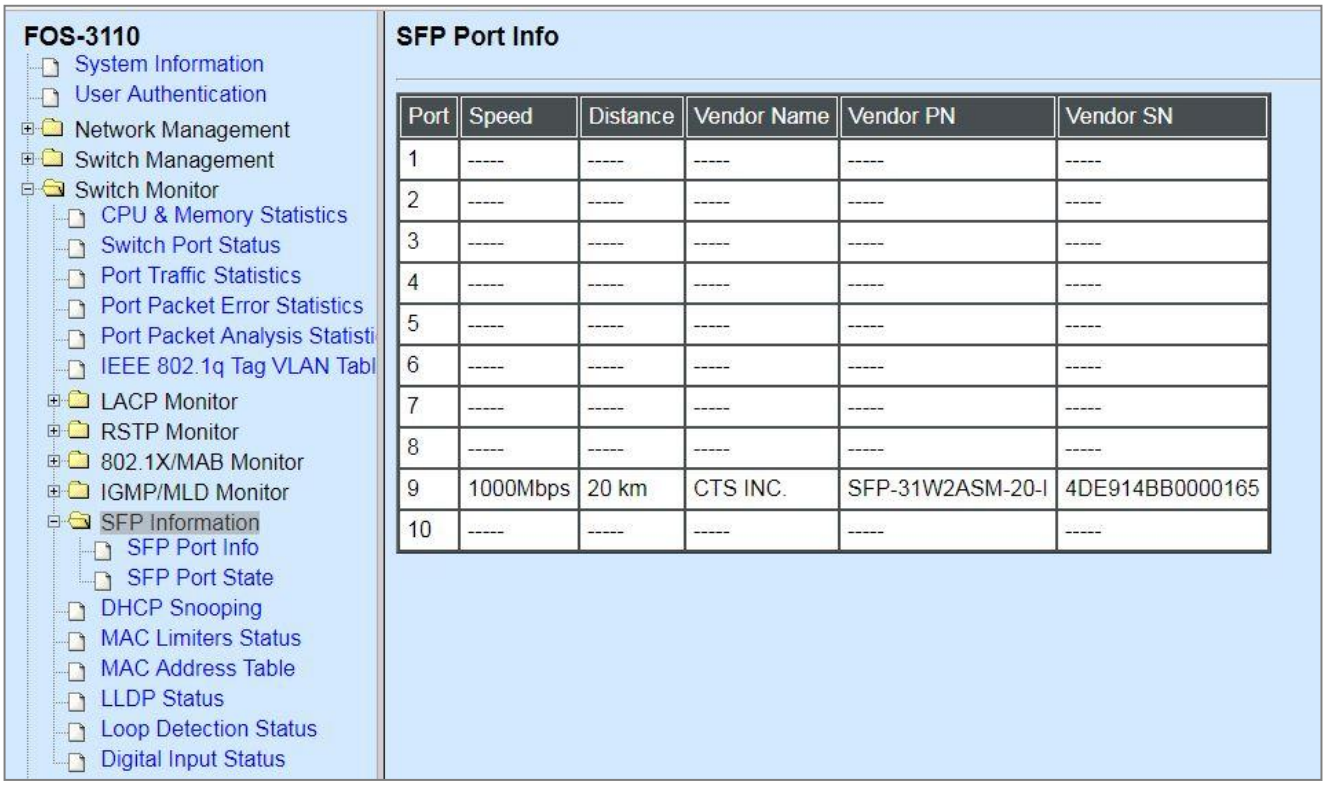
VLAN ID: VID of the specific VLAN

Group: The multicast IP address of MLD querier.

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

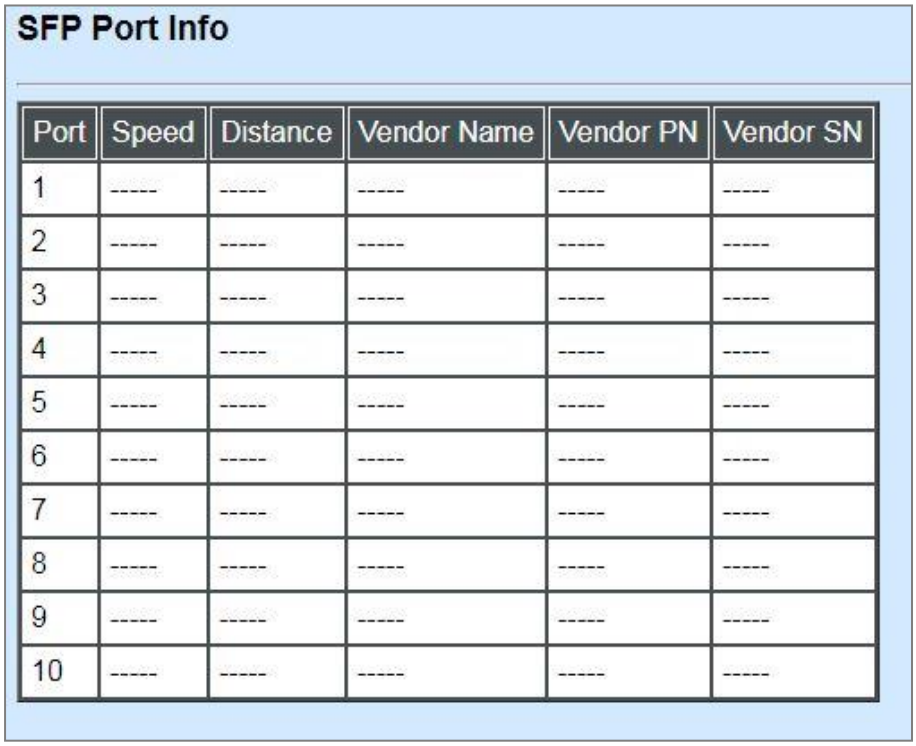
4.5.11 SFP Information

Click the **SFP Information** folder and then two options within this folder will be displayed.



4.5.11.1 SFP Port Info

SFP Port Info displays each port's slide-in SFP Transceiver information e.g. the speed of transmission, the distance of transmission, vendor Name, vendor PN, vendor SN, etc. Select **SFP Port Info** from the **SFP Information** menu and then the following screen page appears.



Port: The number of the port.

Speed: Data rate of the slide-in SFP Transceiver.

Distance: Transmission distance of the slide-in SFP Transceiver.

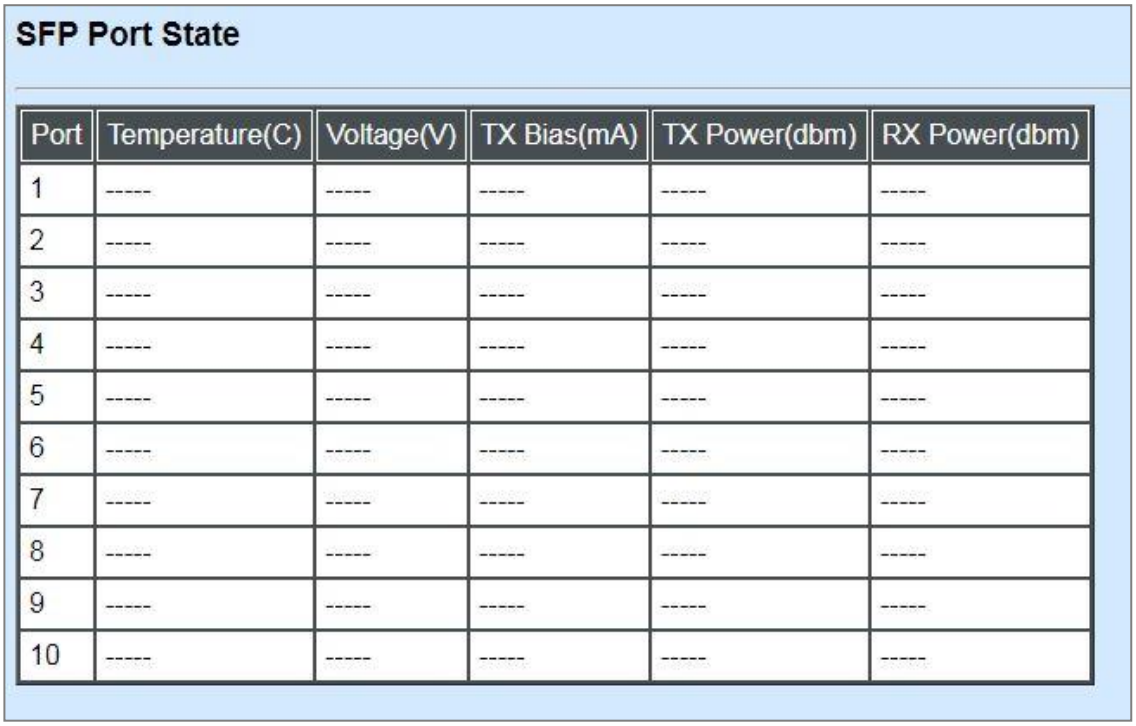
Vendor Name: Vendor name of the slide-in SFP Transceiver.

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

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

4.5.11.2 SFP Port State

SFP Port State displays each port's slide-in SFP Transceiver information e.g. the currently detected temperature, voltage, TX Bias, etc.. Select **SFP Port State** from the **SFP Information** menu and then the following screen page appears.



Port: The number of the SFP module slide-in port.

Temperature (C): The operation temperature of slide-in SFP module currently detected.

Voltage (V): The operation voltage of slide-in SFP module currently detected.

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

TX Power (dbm): The optical transmission power of slide-in SFP module currently detected.

RX Power (dbm): The optical receiving power of slide-in SFP module currently detected.

4.5.12 DCHP Snooping

DHCP Snooping displays the Managed Switch's DHCP Snooping table. Select **DHCP Snooping** from the **Switch Monitor** menu and then the following screen page appears.

Update: Click "Update" to update the DHCP snooping table.

Cli Port: View-only field that shows where the DHCP client binding port is.

Srv Port:.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.

CliIP Addr: View-only field that shows client IP address.

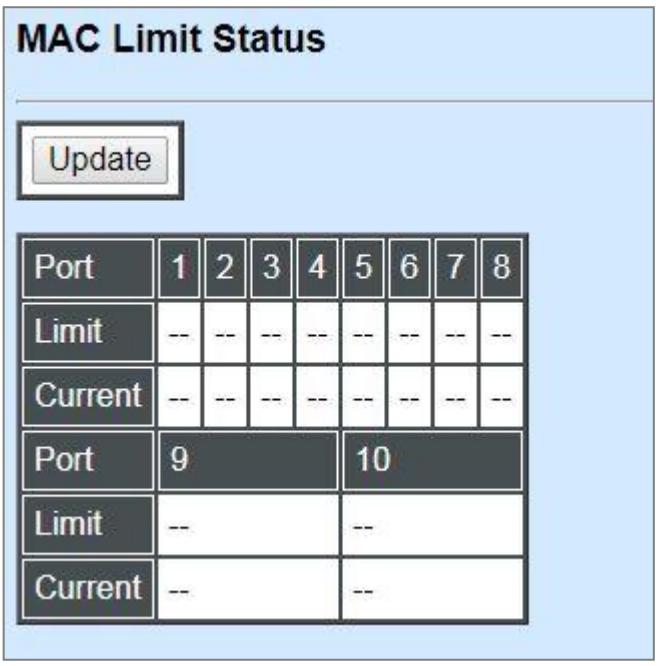
Cli MAC Addr: View-only field that shows client MAC address.

SrvIPAddr: View-only field that shows DHCP server IP address.

TimeLeft: View-only field that shows DHCP client lease time.

4.5.13 MAC Limiters Status

MAC Limiters Status displays the valid MAC Limit Status of each port.



Update: Click “Update” to update the MAC Limiters status.

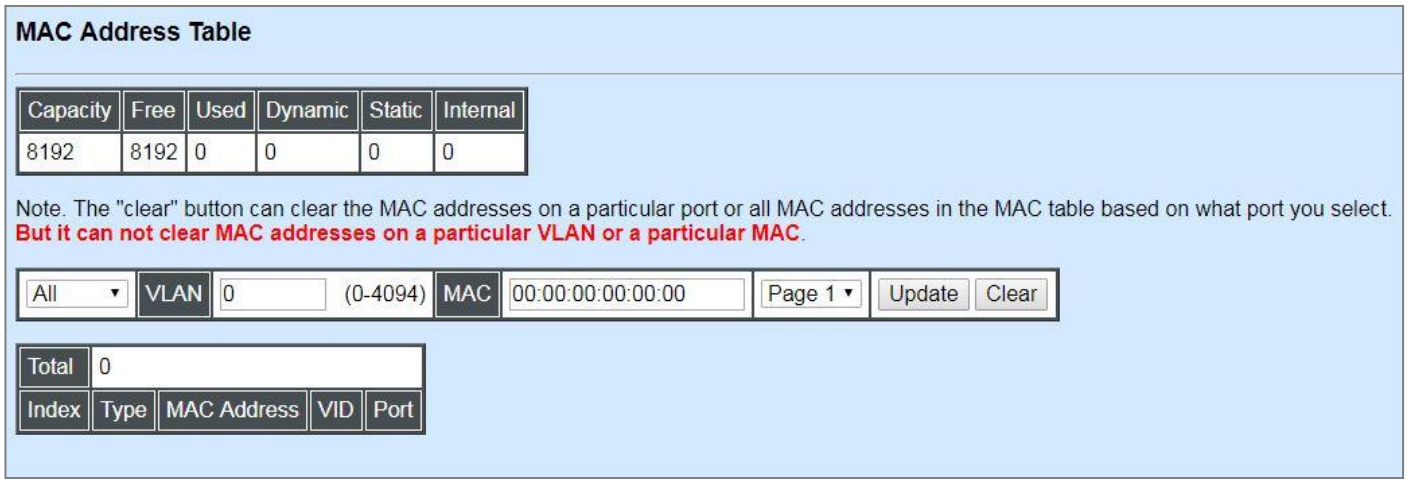
Port: The number of each port.

Limit: The MAC address threshold configured.

Current: The current number of MAC address.

4.5.14 MAC Address Table

MAC Address Table displays MAC addresses learned when MAC Address Learning is enabled.



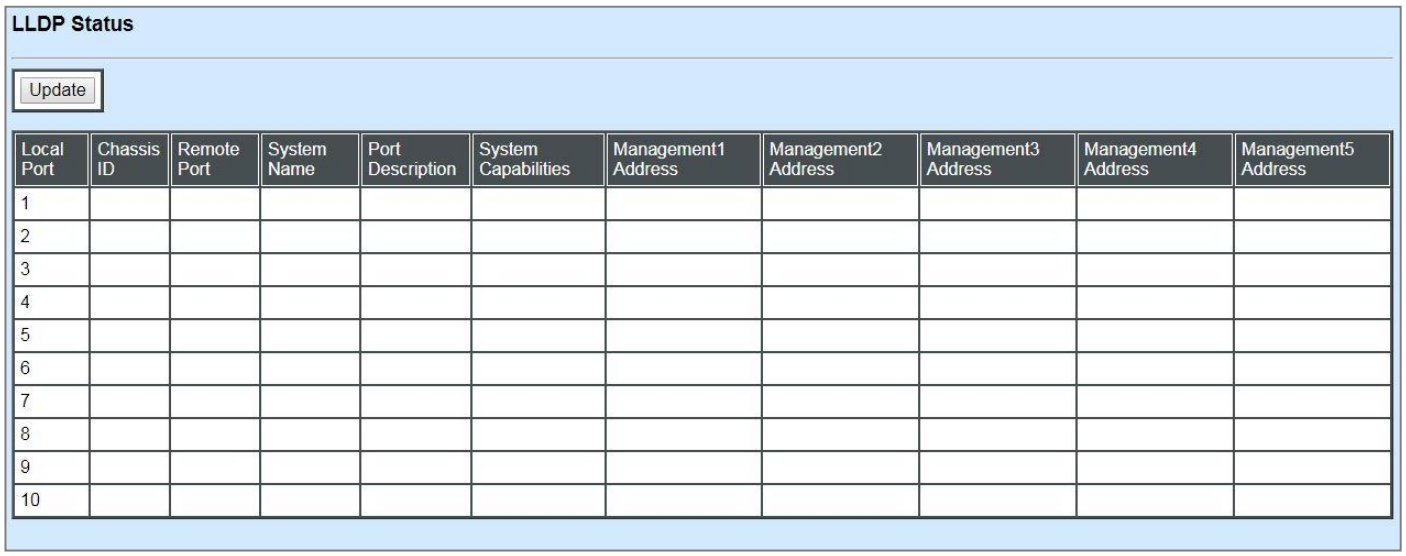
The table above shows the MAC addresses learned from each port of the Managed Switch.

Click **Update** to update the MAC Address Table.

Click **Clear** to clear the MAC Address table for the specified port(s).

4.5.15 LLDP Status

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



Click **"Update"** to update the LLDP Status table.

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

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

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

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

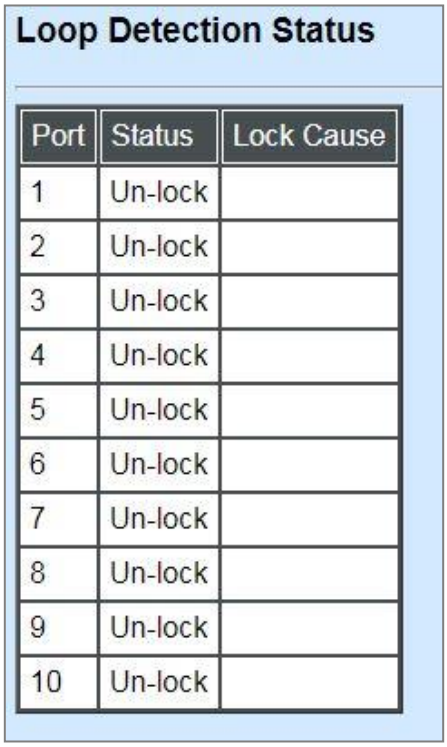
Port Description: View-only field that shows the port description of the remote port.

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

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

4.5.16 Loop Detection Status

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

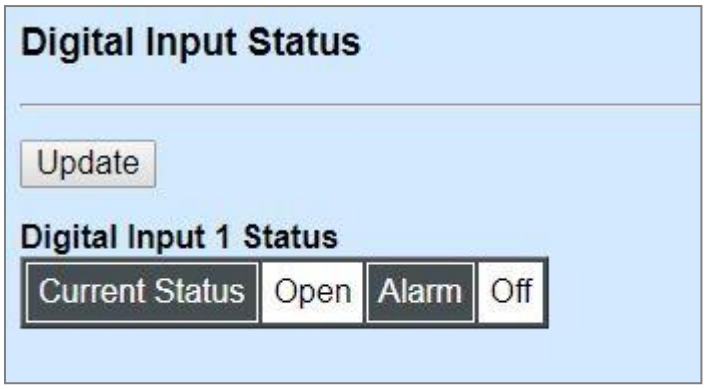


Status: View-only filed that shows the loop status of each port.

Lock Cause: View-only filed that shows the cause why the port is locked.

4.5.17 Digital Input Status

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



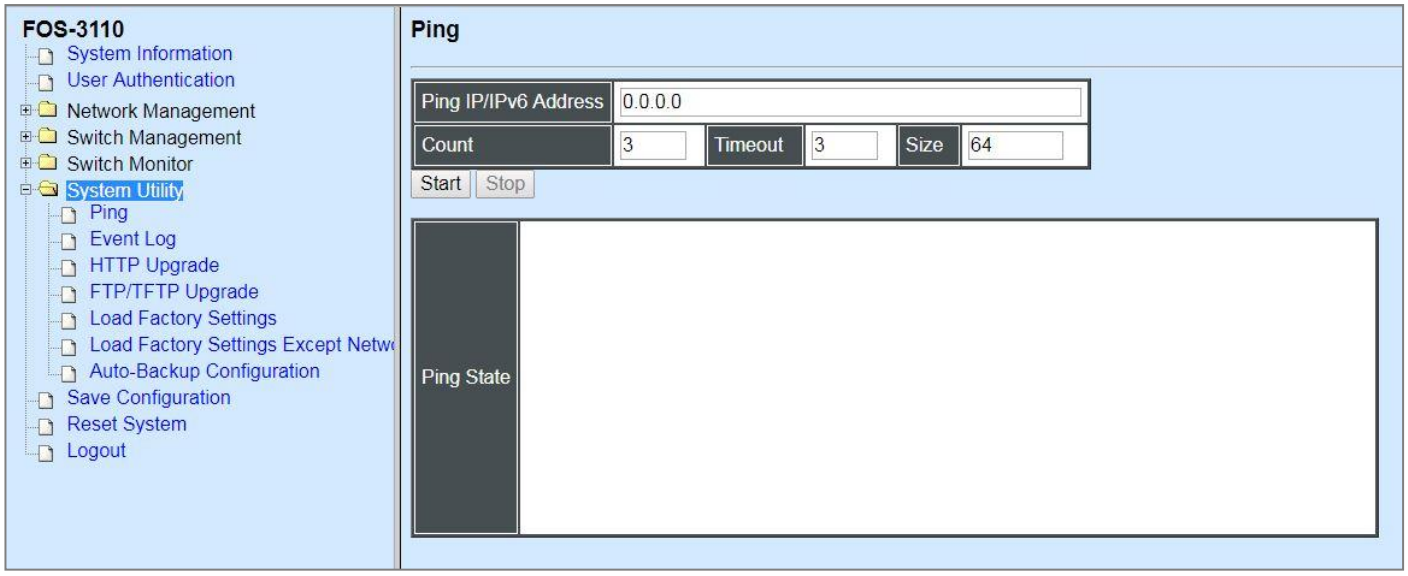
Click **Update** to update the digital input and alarm status.

Current Status: View-only field that shows the current status of Digital Input 1.

Alarm: View-only field that shows the current alarm status.

4.6 System Utility

System Utility allows users to easily operate and maintain the system. Select the folder **System Utility** from the **Main Menu** and then the following screen page appears.



1. **Ping:** Ping can help you test the network connectivity between the Managed Switch and the host. You can also specify count s, timeout and size of the Ping packets.

2. **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.

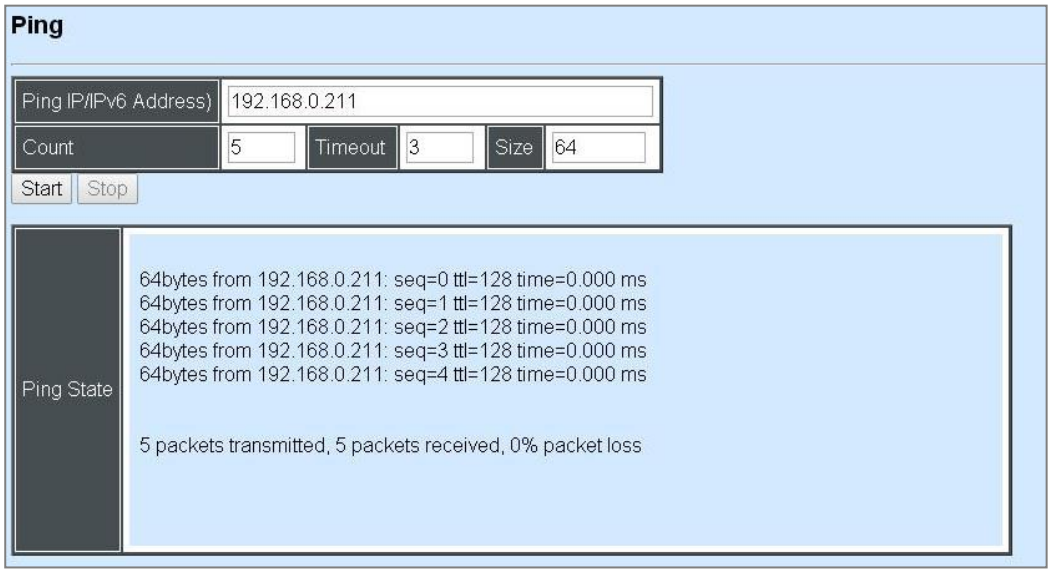
3. **HTTP/FTP/TFTP Upgrade:** This allows users to update the latest firmware, save current configuration or restore previous configuration to the Managed Switch.

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

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

4.6.1 Ping

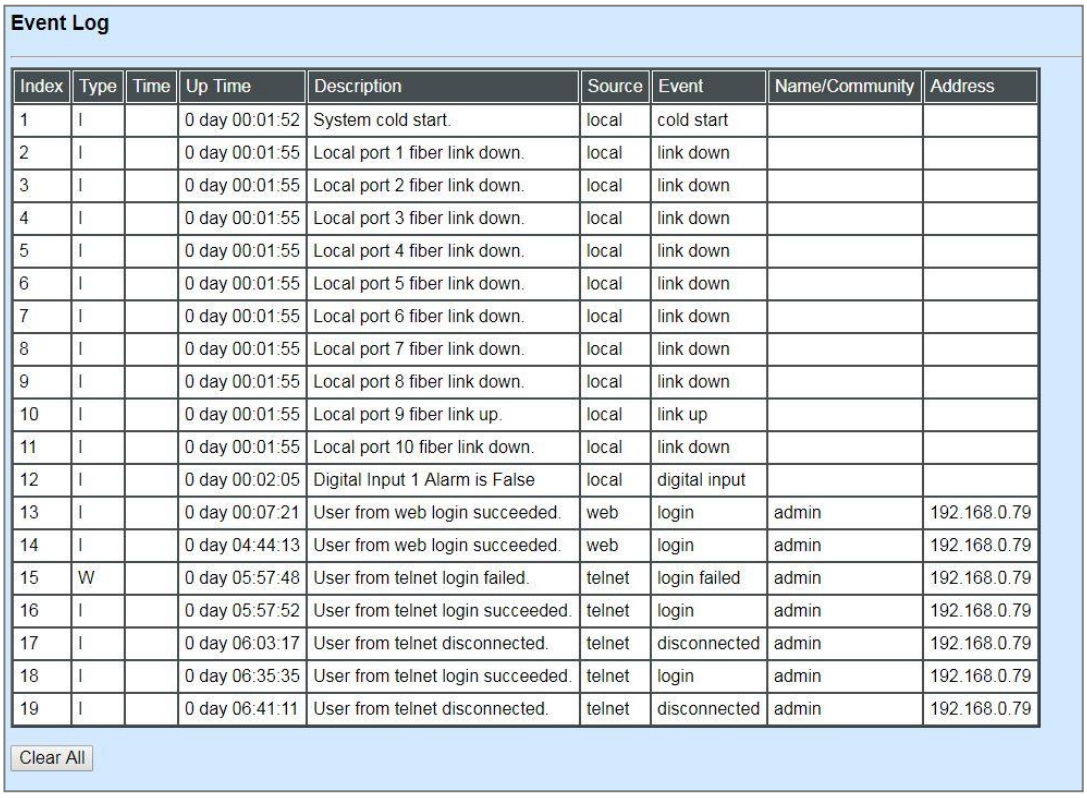
Ping can help you test the network connectivity between the Managed Switch and the host. Select **Ping** from the **System Utility** menu and then the following screen page appears.



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

4.6.2 Event Log

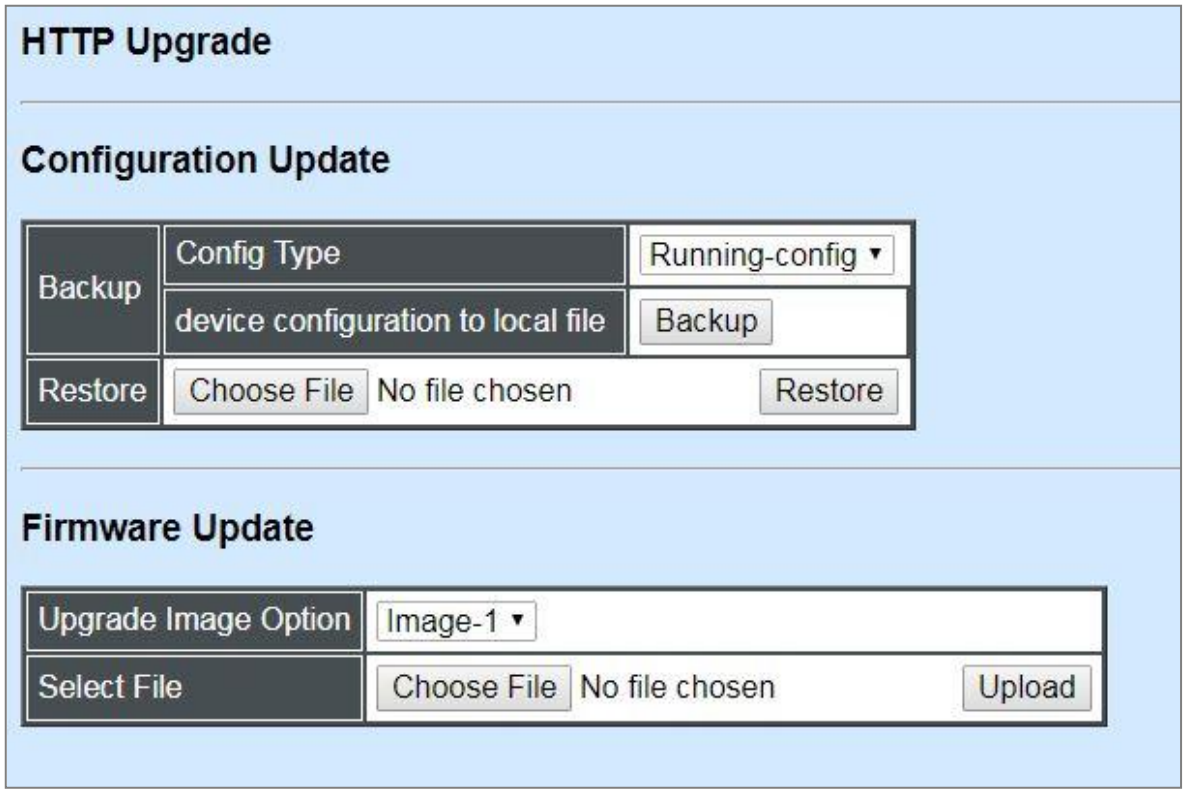
Event log keeps a record of switch-related information, such as user login, logout timestamp and so on. Select **Event Log** from the **System Utility** menu and then the following screen page appears. All event logs will be cleared when system reset occurs.



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

4.6.3 HTTP Upgrade

Users may save or restore their configuration and update their firmware. Select **HTTP Upgrade** from the **System Utility** menu and then the following screen page appears.



The related parameter description of the configuration update is as follows:

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 factory setting.
- **Start-up-config:** Back up the data same as last saved data.

Device Configuration to Local File: Click **Backup** to begin download the configuration file to your PC.

Restore: Click **Choose File** to select the designated data and then click **Restore**.

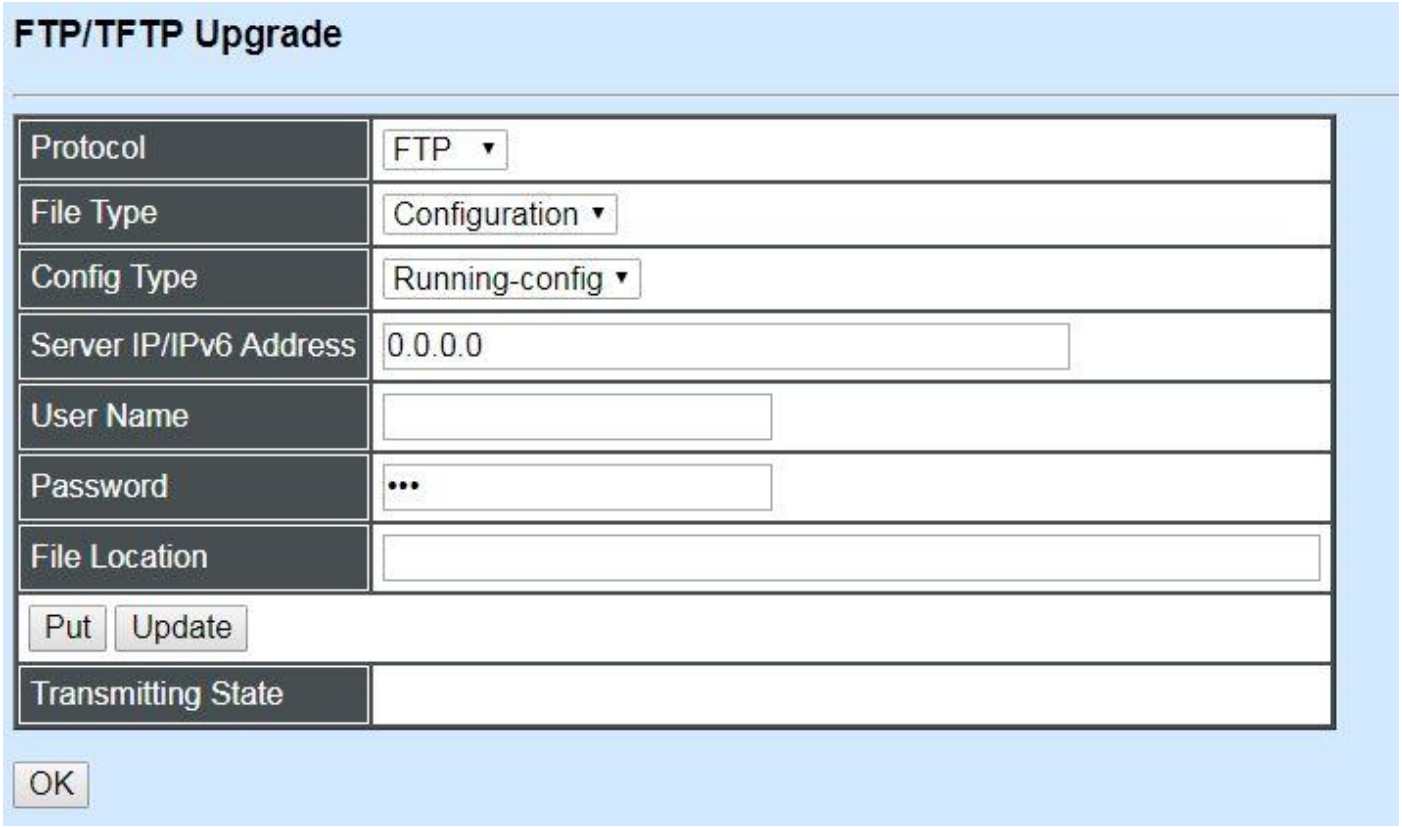
The related parameter description of the firmware update is as follows:

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 **Upload.**

4.6.4 FTP/TFTP Upgrade

The Managed Switch has both built-in TFTP and FTP clients. Users may save or restore their configuration and update their firmware. Select **FTP/TFTP Upgrade** from the **System Utility** menu and then the following screen page appears.



Protocol: Select the preferred protocol, either FTP or TFTP.

File Type: Select the type o file to process, either Firmware or Configuration.

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 IP/IPv6 Address: Enter the specific IP/IPv6 address of the FTP/TFTP file server.

User Name: Enter the specific username to access the FTP file server.

Password: Enter the specific password to access the FTP file server.

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

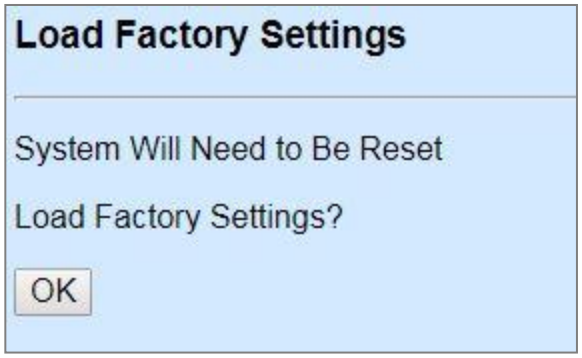
Click **Update** to start the download process and receive files from the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind the user.

Click **Put** 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.

4.6.5 Load Factory Settings

Load Factory Setting 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 **Load Factory Setting** from the **System Utility** menu and then the following screen page appears.

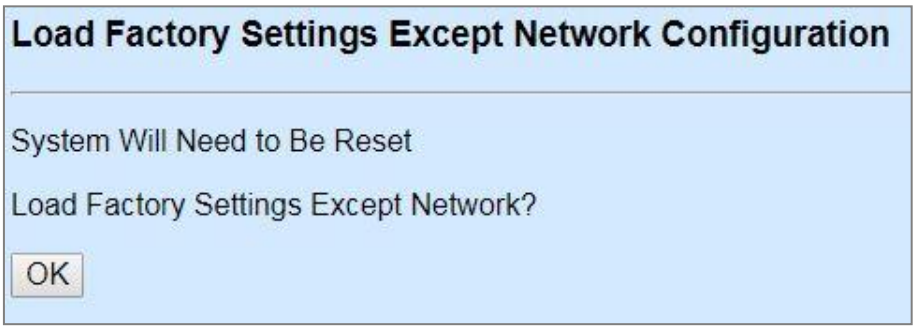


Click **OK** to start loading factory settings.

4.6.6 Load Factory Settings Except Network Configuration

Load Factory Settings Except Network Configuration 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.

Select **Load Factory Setting Except Network Configuration** from the **System Utility** menu, the following screen page shows up.

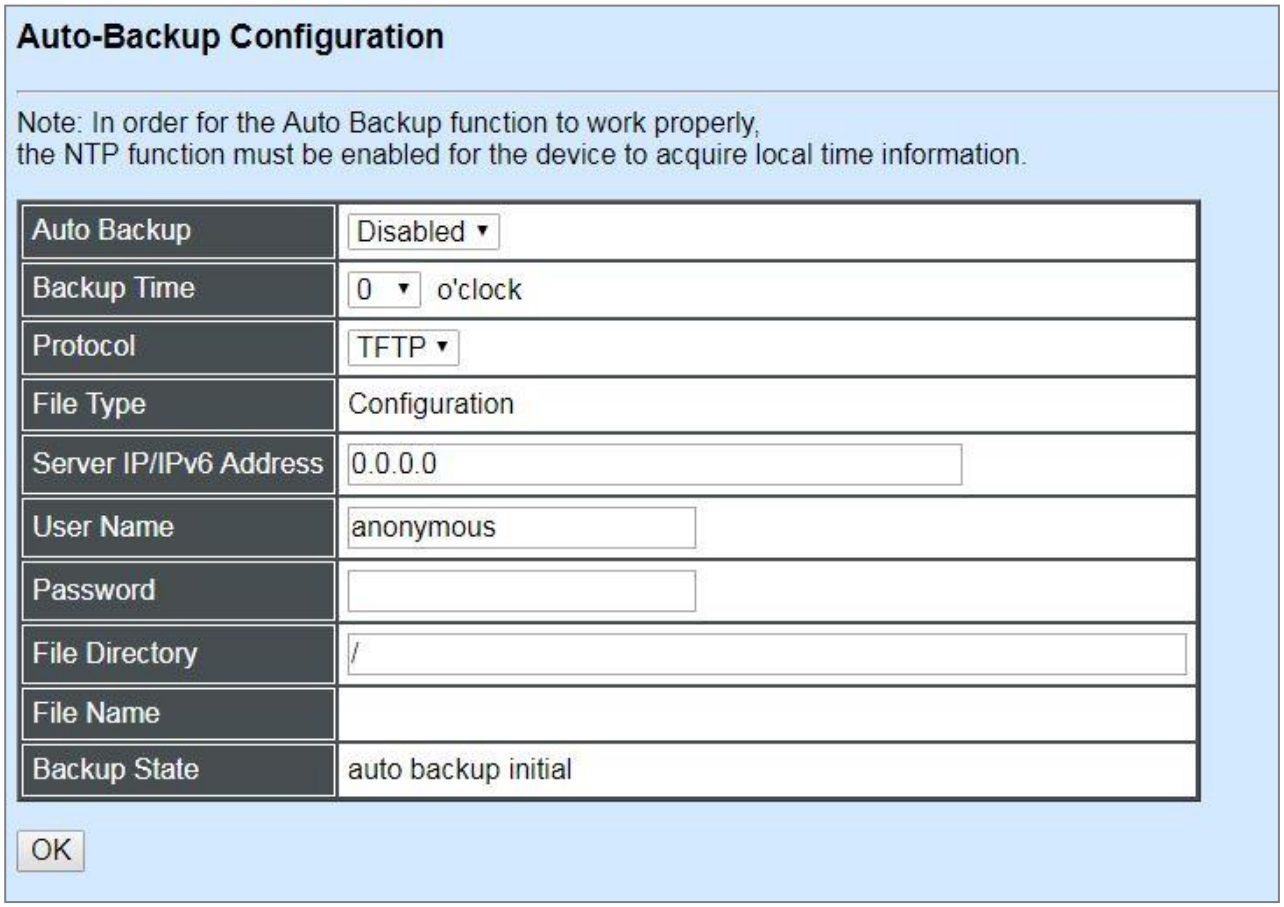


Click **OK** to start loading factory settings except network configuration.

4.6.7 Auto-Backup Configuration

In FOS-3110, 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 configuration** function to do this backup automatically and periodically. It is useful to prevent the loss of user's important configuration if they forget to do the backup, or help do the file comparison if any error occurs. Please note that the device's NTP function must be enabled as well in order to obtain the correct local time.

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



Auto Backup: 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 IP/IPv6 Address: Set up the IP/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.

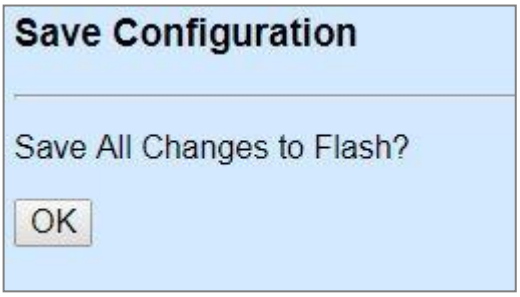
File Name: The filename assigned to the auto- backup configuration files. The format of filename generated automatically is as follows:

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

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

4.7 Save Configuration

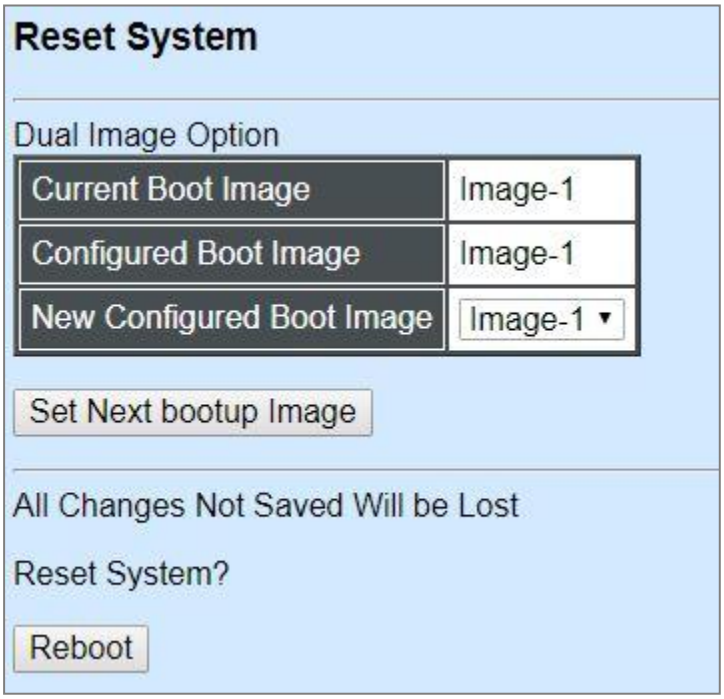
In order to save the configuration permanently, users need to save configuration first before resetting the Managed Switch. Select **Save Configuration** from the the Main Menu and then the following screen page appears.



Click **OK** to save the configuration.

4.8 Reset System

To reboot the system, please select **Reset System** from the Main 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

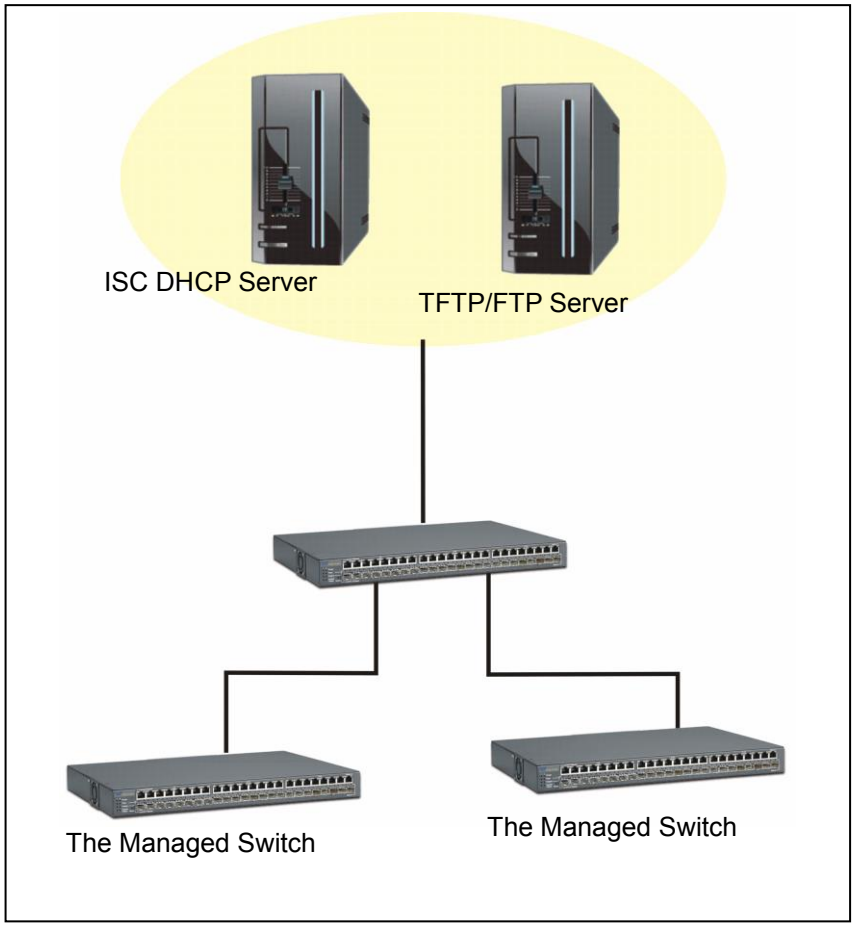
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the Managed Switch that you purchased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

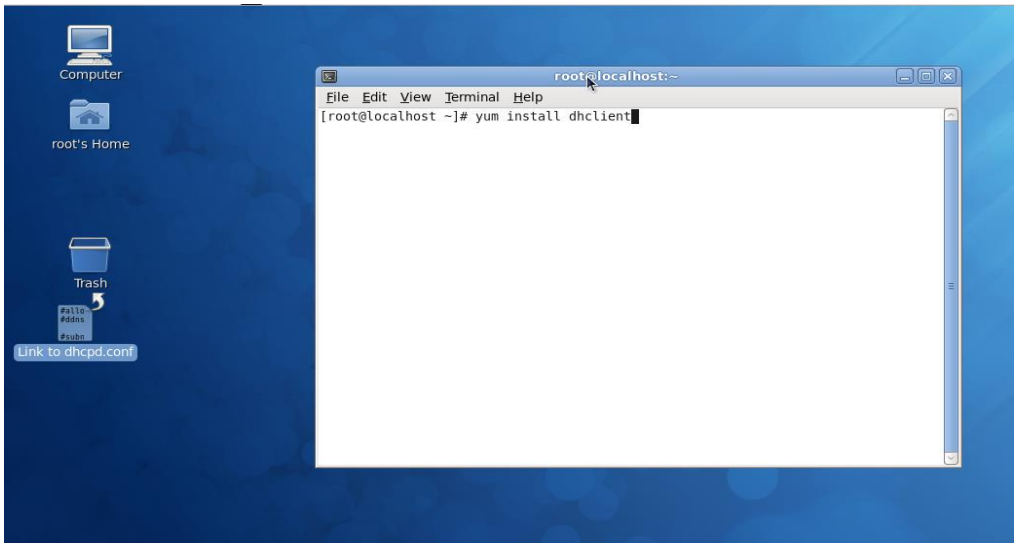
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Topology Example

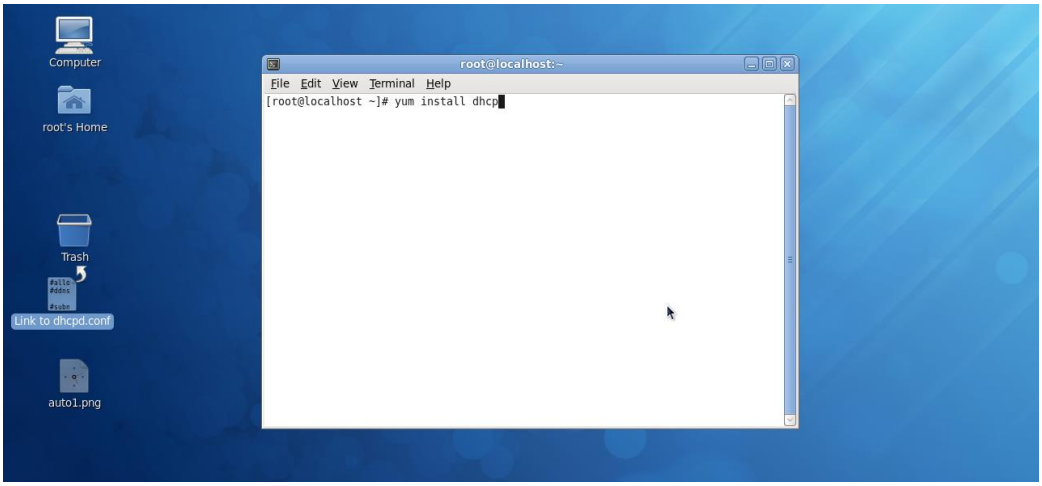
Step 2. Set up Auto Provision Server

- **Update DHCP Client**



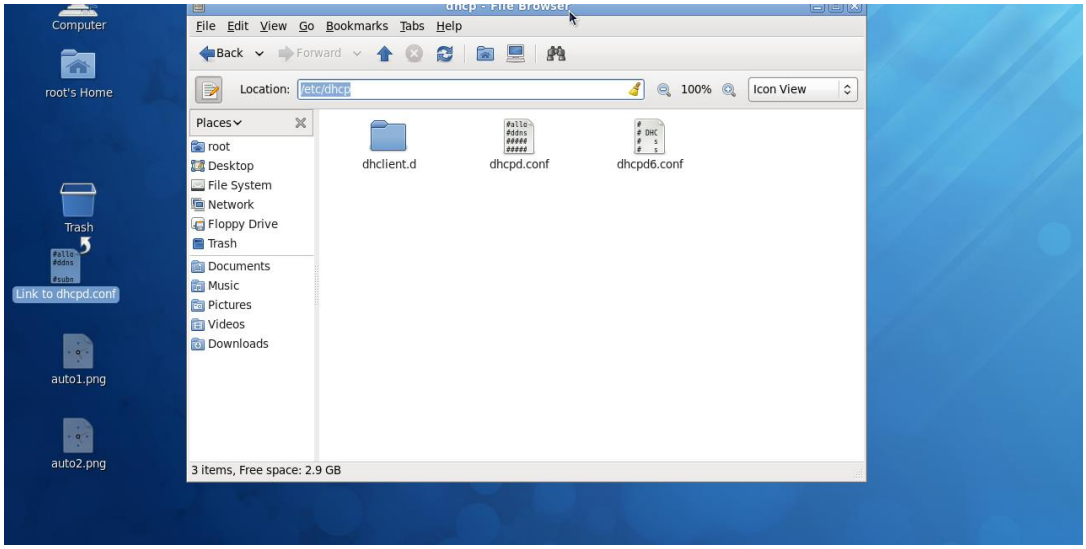
Linux Fedora 12 supports “yum” function by default. First of all, update DHCP client function by issuing “yum install dhclient” command.

- **Install DHCP Server**



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

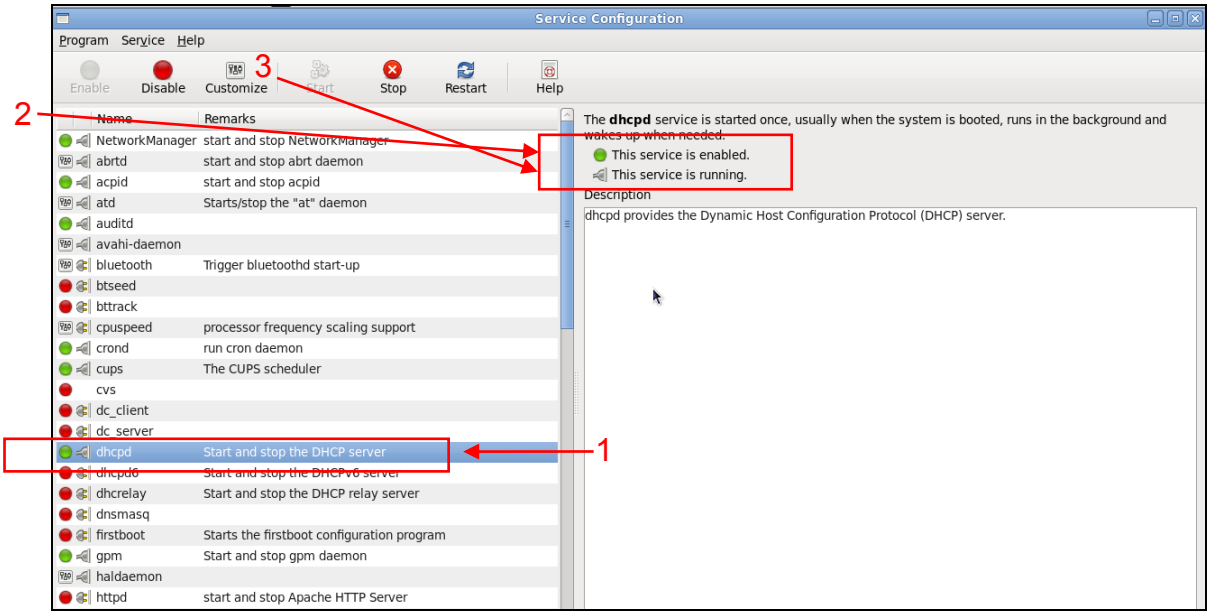
- **Copy dhcpd.conf to /etc/dhcp/ directory**



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

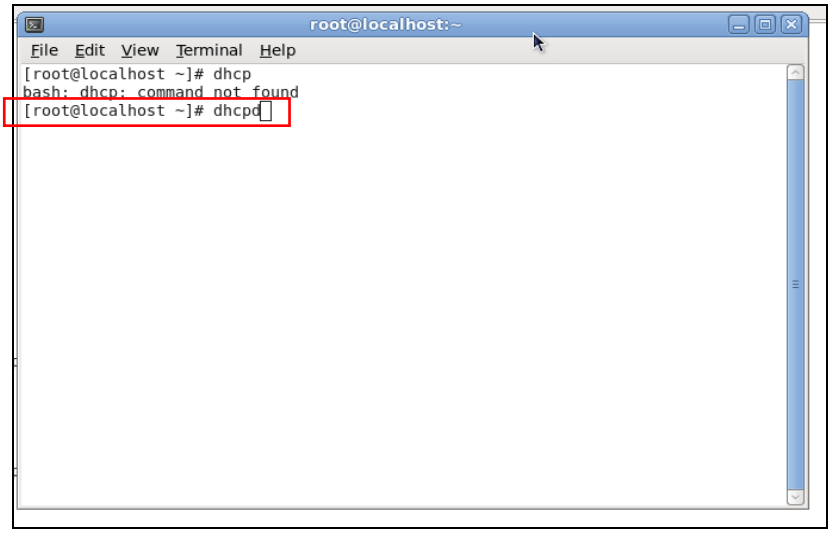
Please note that each vendor has their own way to define auto provisioning. Make sure to use the file provided by the vendor.

- **Enable and run DHCP service**



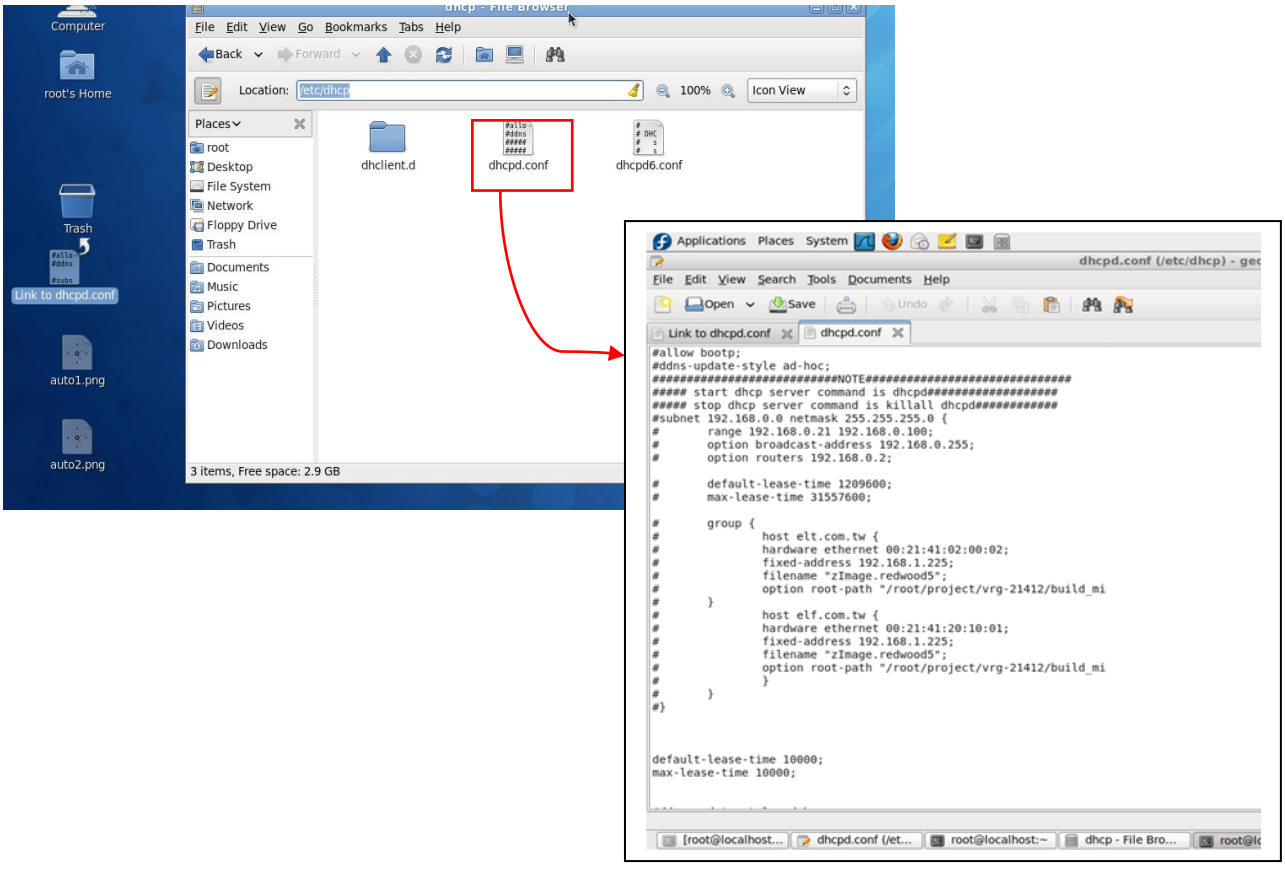
1. Choose dhcpd.
2. Enable DHCP service.
3. Start running DHCP service.

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



Step 3. Modify dhcpd.conf file

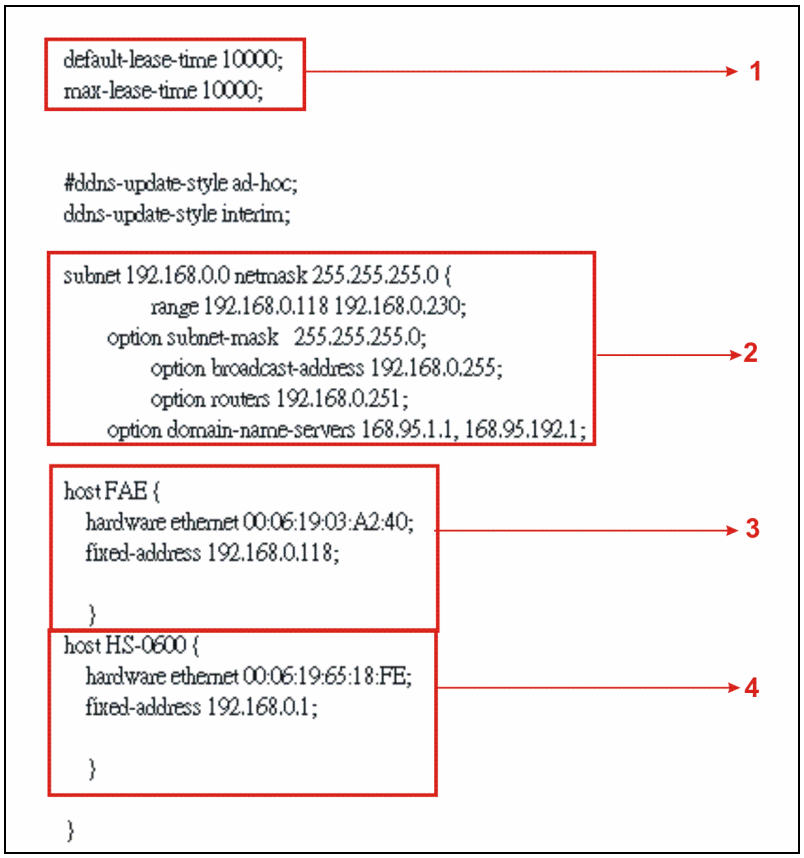
- **Open dhcpd.conf file in /etc/dhcp/ directory**



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.

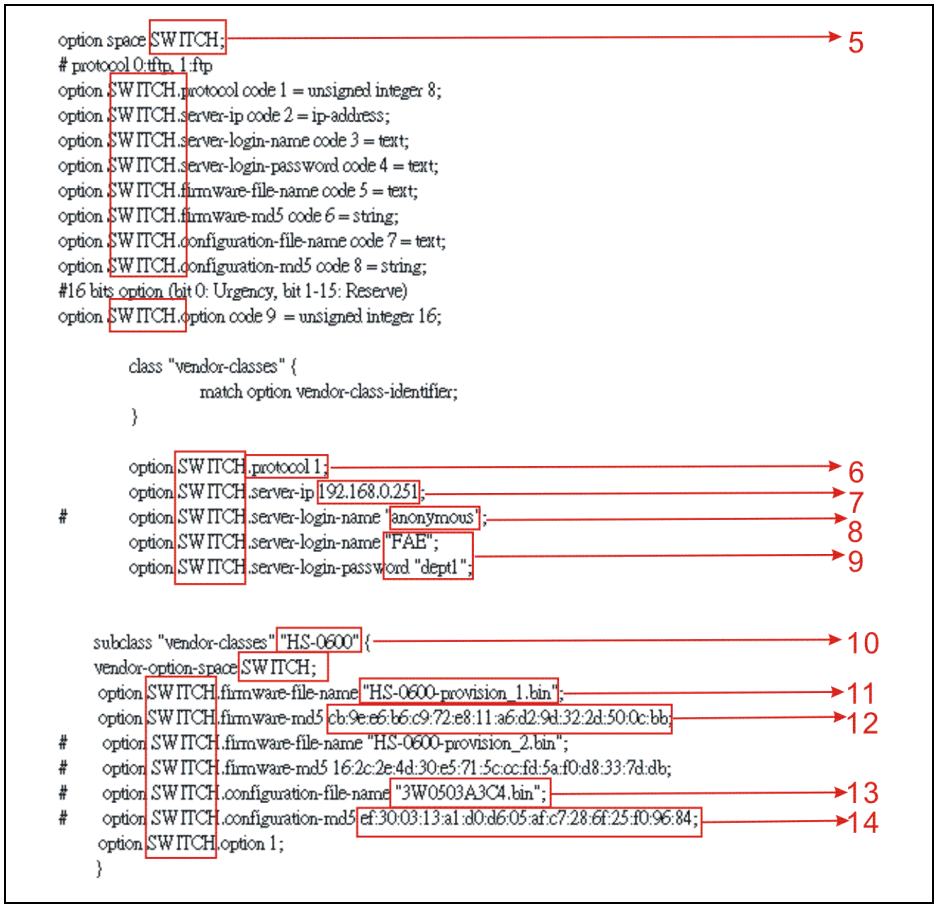
   Default lease time: If a client does not request a specific IP lease time, the server will assign a default lease time value.

   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.

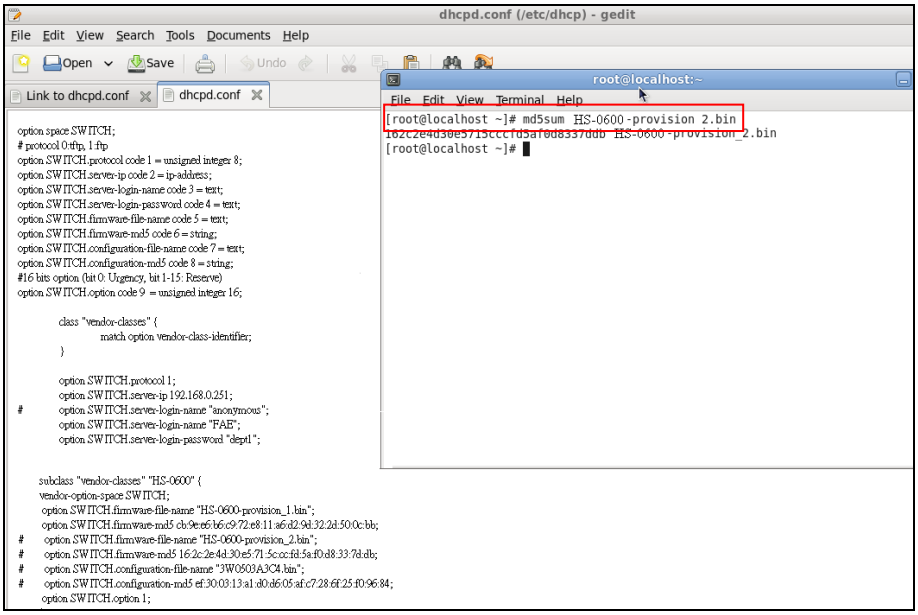
4. Map a host's MAC address to a fixed IP address. Use the same format to create multiple MAC-to-IP address bindings.



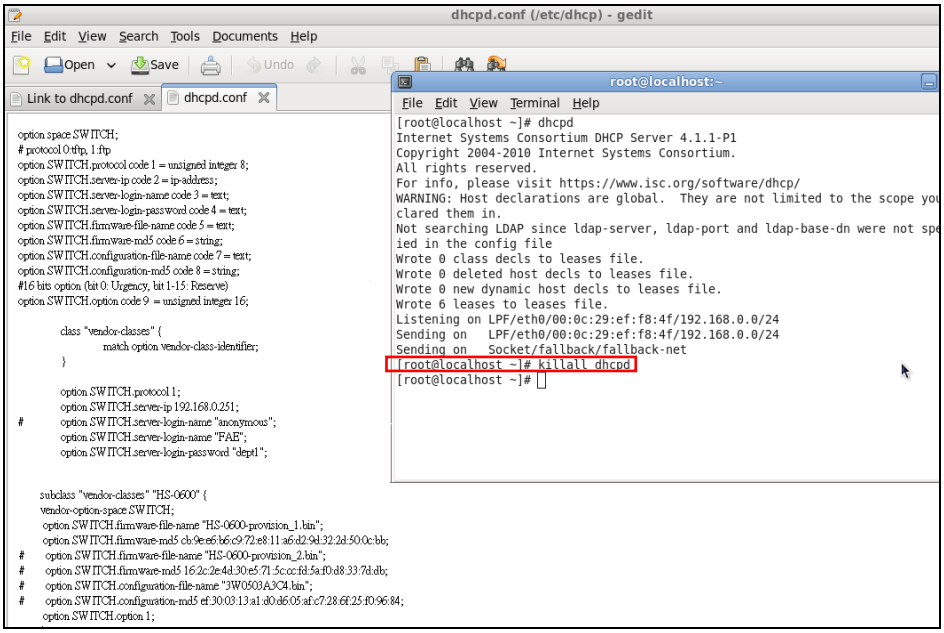
5. This value is configurable and can be defined by users.
6. Specify the protocol used (Protocol 1: FTP; Protocol 0: TFTP).
7. Specify the FTP or TFTP IP address.
8. Login TFTP server anonymously (TFTP does not require a login name and password).
9. Specify FTP Server login name and password.
10. Specify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

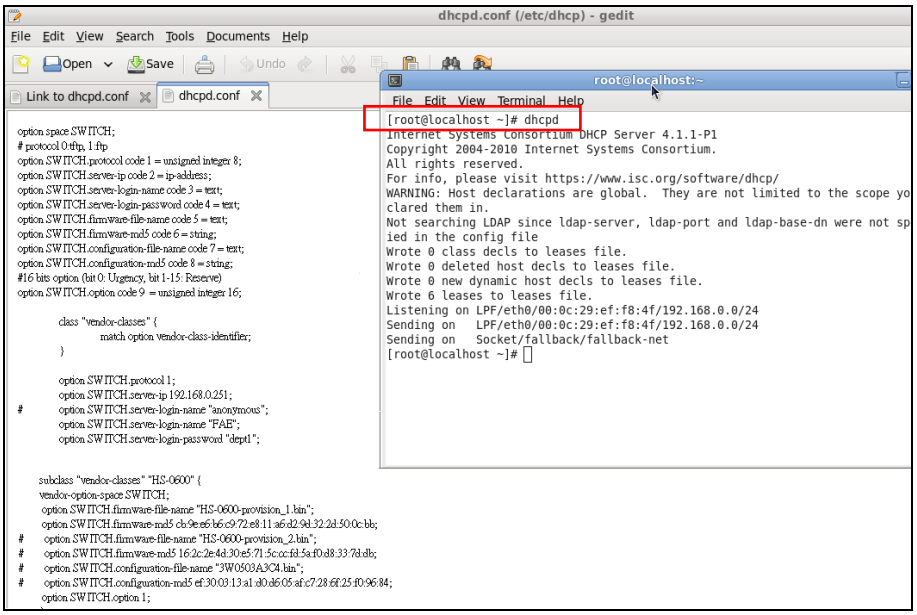
NOTE 1: *The text beginning with a pound sign (#) will be ignored by the DHCP server. For example, in the figure shown above, firmware-file-name "HS-0600-provision_2.bin" and firmware-md5 (line 5 & 6 from the bottom) will be ignored. If you want DHCP server to process these two lines, remove pound signs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

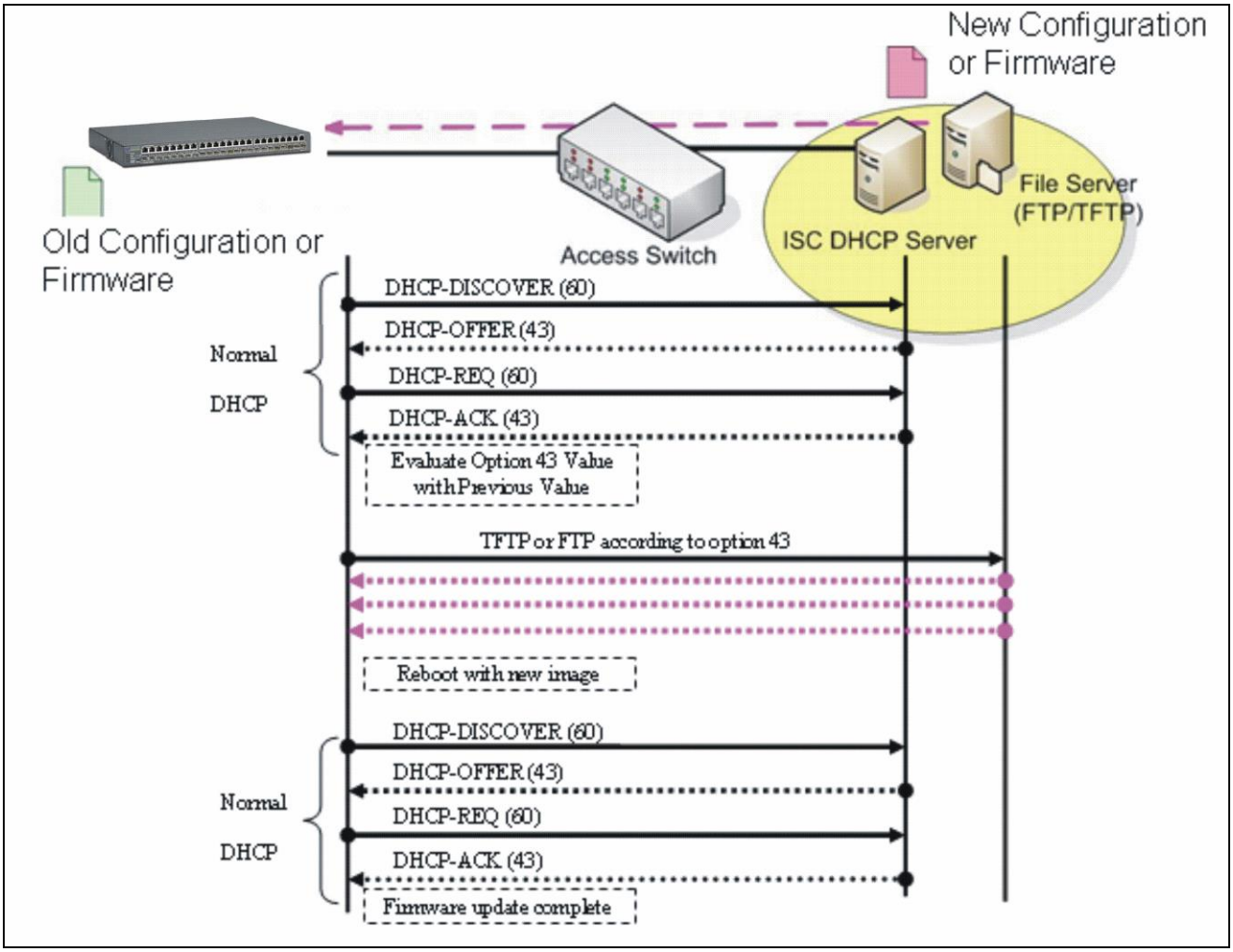
Step 5. Place a copy of Firmware and Configuration File in TFTP/FTP

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.

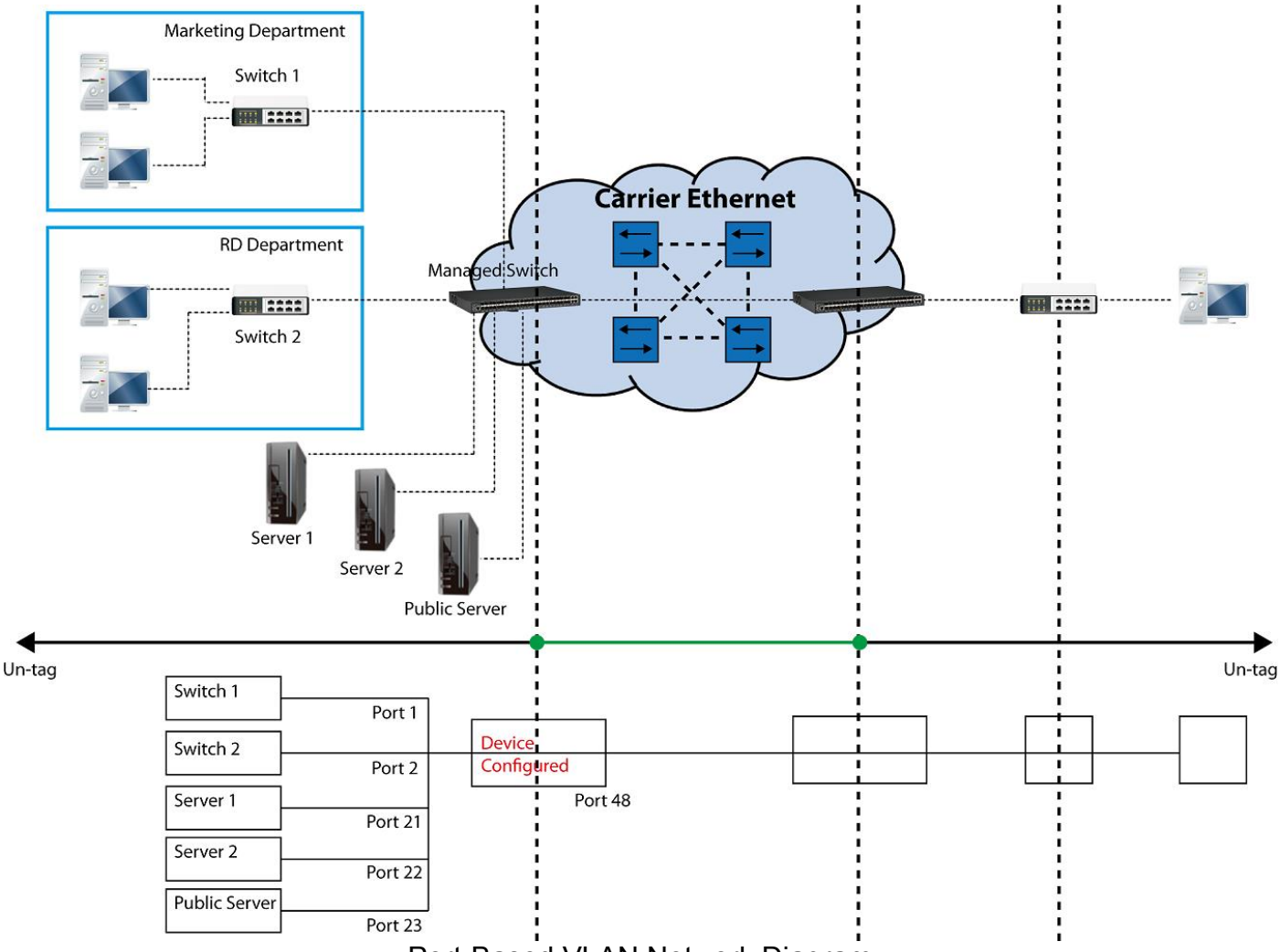
The Managed Switch supports Port-based VLAN implementation and IEEE 802.1Q standard tagging mechanism that enables the switch to differentiate frames based on a 12-bit VLAN ID (VID) field. Besides, the Managed Switch also provides double tagging function. The IEEE 802.1Q double tagging VLAN is also referred 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:

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.

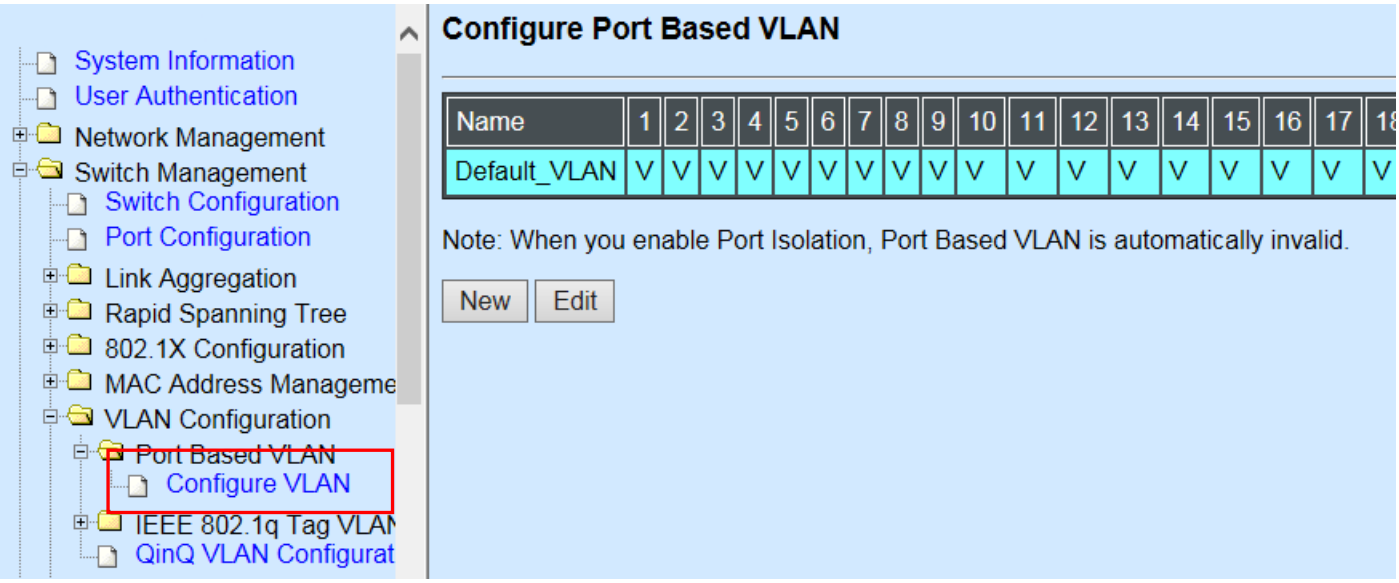
VLAN Name	Member ports
Marketing	1, 21, 23, 48
RD	2, 22, 23, 48

CLI Configuration:

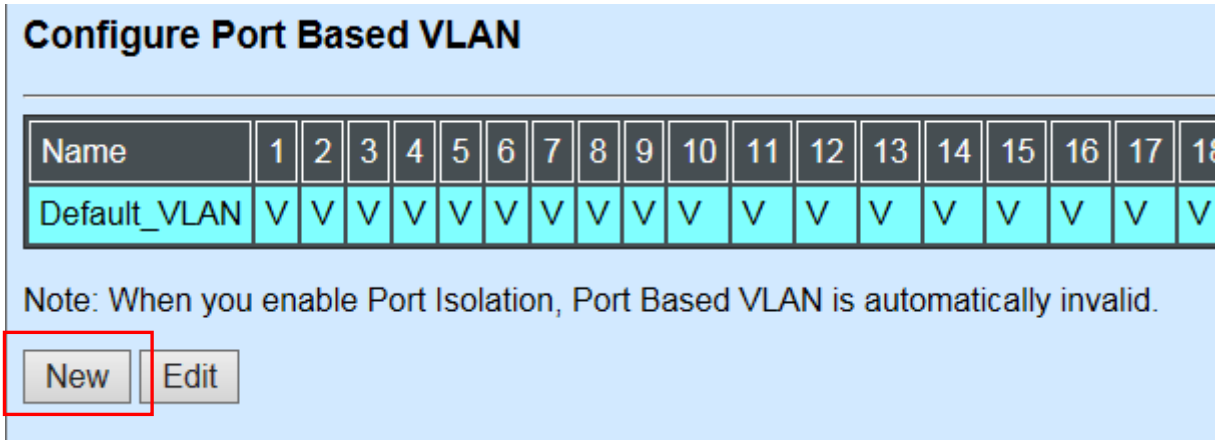
Steps…	Commands…
1. Enter Global Configuration mode.	SWH> enable Password: SWH# config SWH(config)#
2. Create port-based VLANs “Marketing” and “RD”	SWH(config)# vlan port-based Marketing OK ! SWH(config)# vlan port-based RD OK !
3. Select port 1, 21, 23 and 48 to configure.	SWH(config)# interface 1,21,23,48 SWH(config-if-1,21,23,48)#
4. Assign the ports to the port-based VLAN “Marketing”.	SWH(config-if-1,21,23,48)# vlan port-based Marketing OK !
5. Return to Global Configuration mode, and select port 2, 22, 23 and 48 to configure.	SWH(config-if-1,21,23,48)# exit SWH(config)# interface 2,22,23,48 SWH(config-if-2,22,23,48)#
6. Assign the ports to the port-based VLAN “RD”.	SWH(config-if-2,22,23,48)# vlan port-based RD OK !
7. Return to Global Configuration mode, and show currently configured port-based VLAN membership.	SWH(config-if-2,22,23,48)# exit SWH(config)# show vlan port-based When you enable Port Isolation, Port Based VLAN is automatically invalid. ========== Port Based VLAN : ========== Name Port Member ---------- ---------- Default_VLAN 1-48,CPU Marketing 1,21,23,48 RD 2,22,23,48 *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:

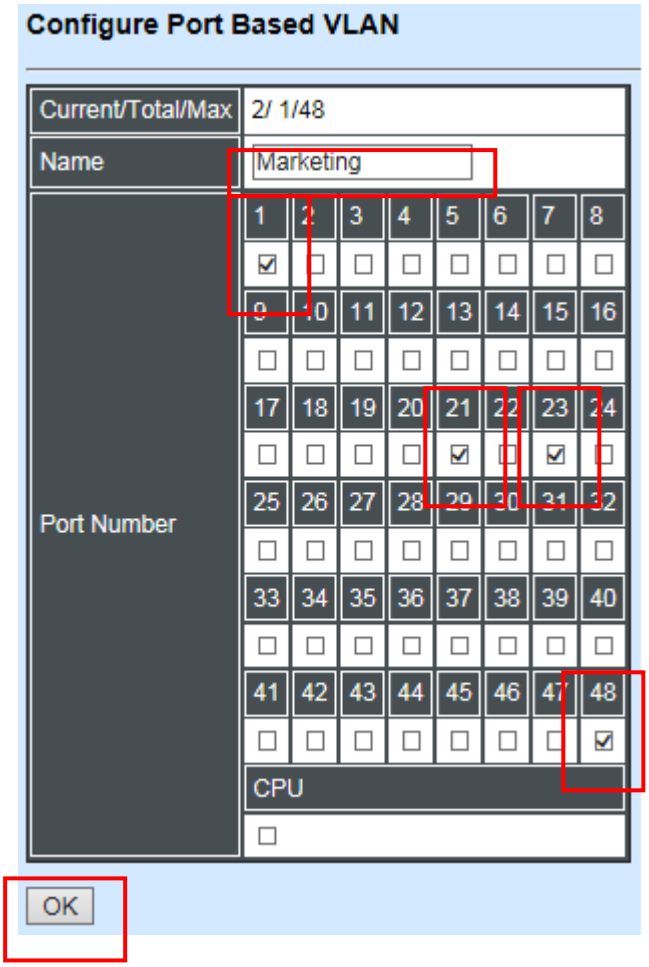
1. **Select “Configure VLAN” option in Port Based VLAN menu.**
   Switch Management>VLAN Configuration>Port Based VLAN>Configure VLAN



2. **Click "New" to add a new Port-Based VLAN**
   Switch Management>VLAN Configuration>Port Based VLAN>Configure VLAN

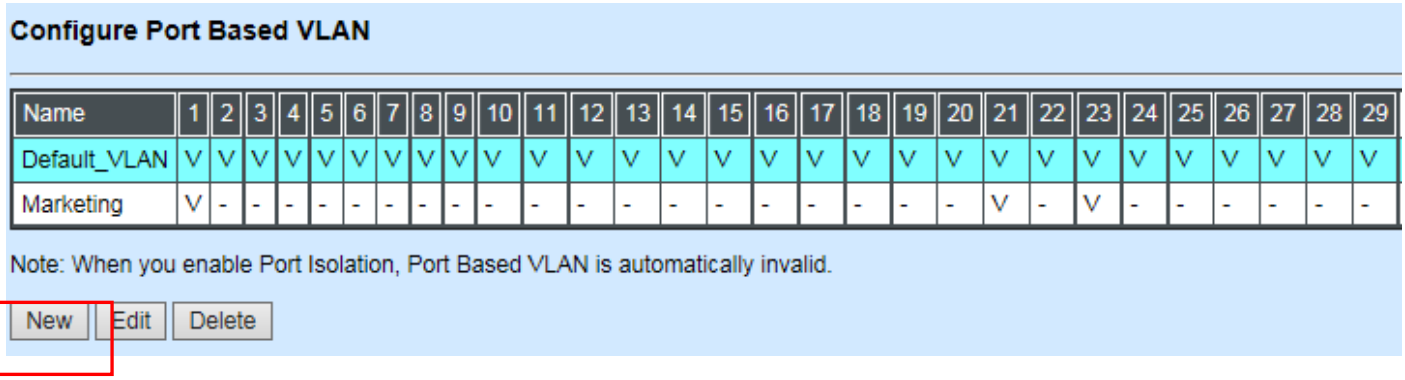


3. **Add Port 1, 21, 23 and 48 in a group and name it to "Marketing".**
   Switch Management>VLAN Configuration>Port Based VLAN>Configure VLAN

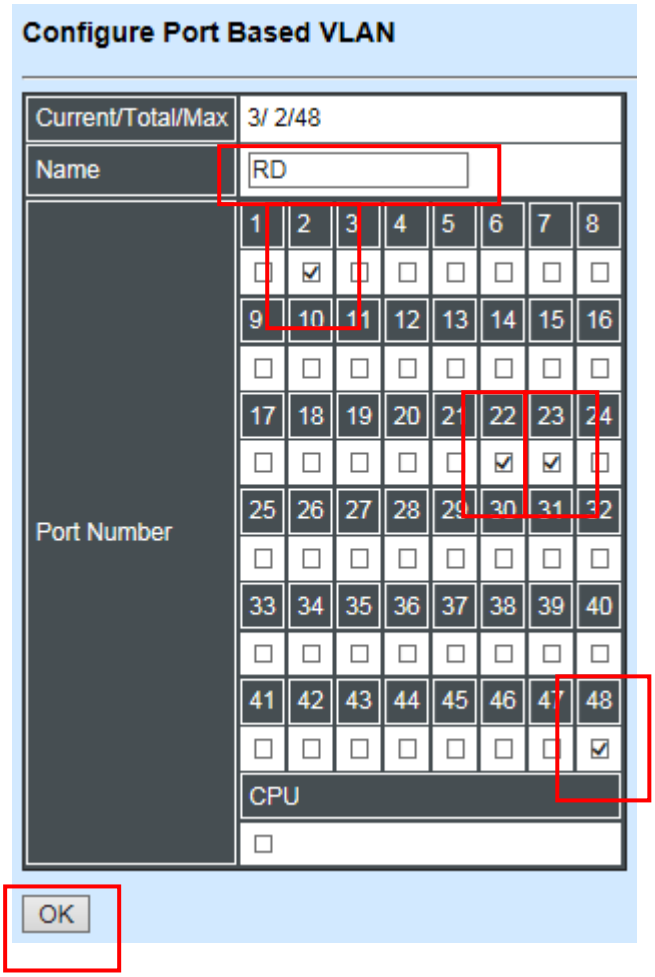


Click “OK” to apply the settings.

4. **Click “New” to add a new Port-Based VLAN**
   Switch Management>VLAN Configuration>Port Based VLAN>Configure VLAN

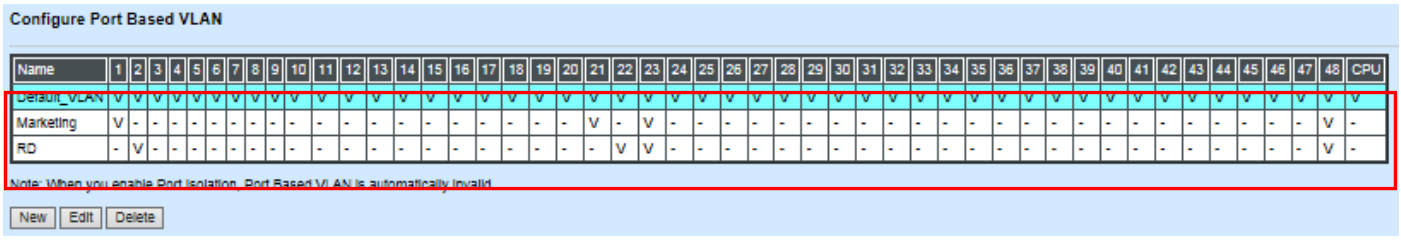


5. **Add Port 2, 22, 23 and 48 in a group and name it to "RD".**
   Switch Management>VLAN Configuration>Port Based VLAN>Configure VLAN



   Click "OK" to apply the settings.

6. **Check Port-Based VLAN settings.**
   Switch Management>VLAN Configuration>Port Based VLAN>Configure 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 48.

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 48.

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 48.

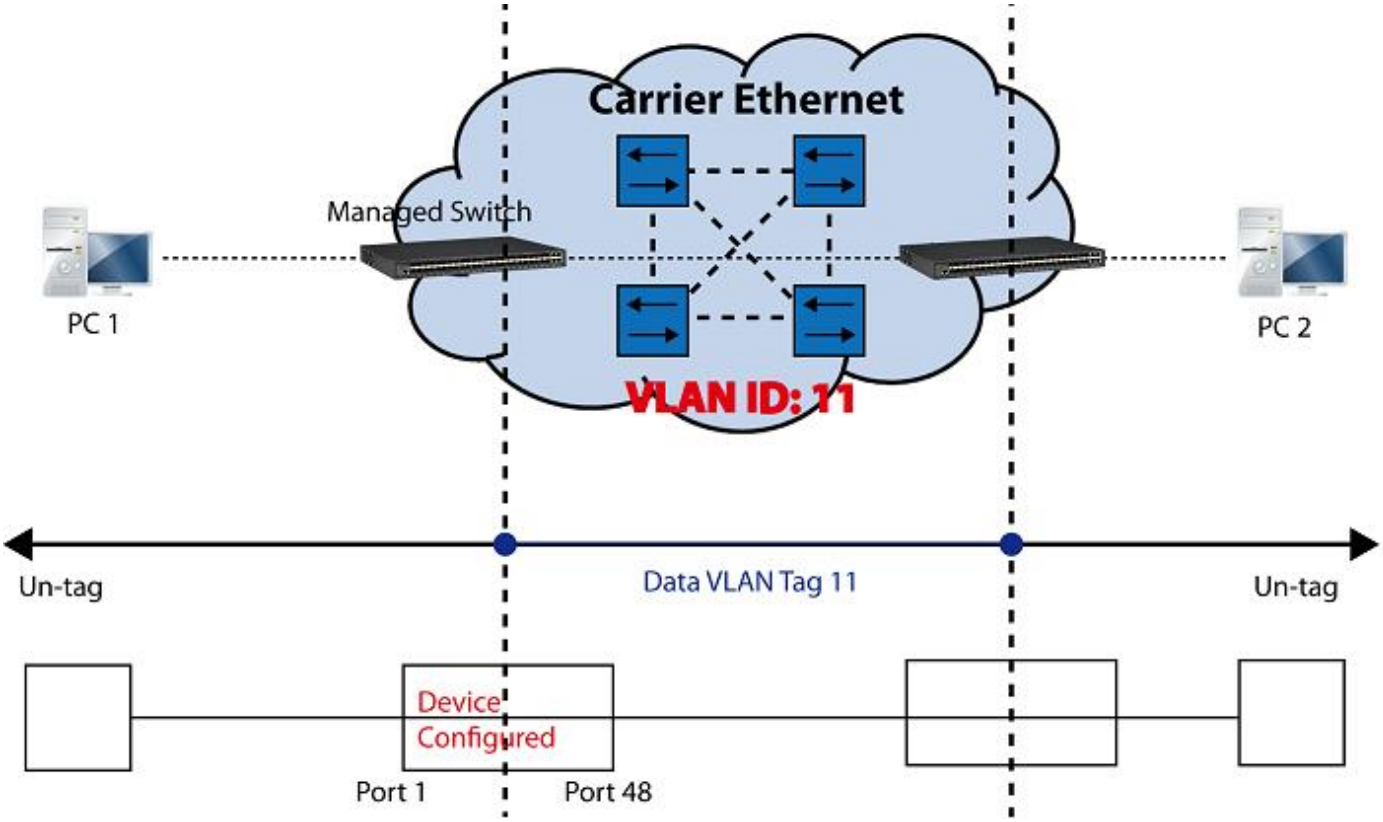
4. A tagged packet with any permissible VID arrives at Port 2

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 48.

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

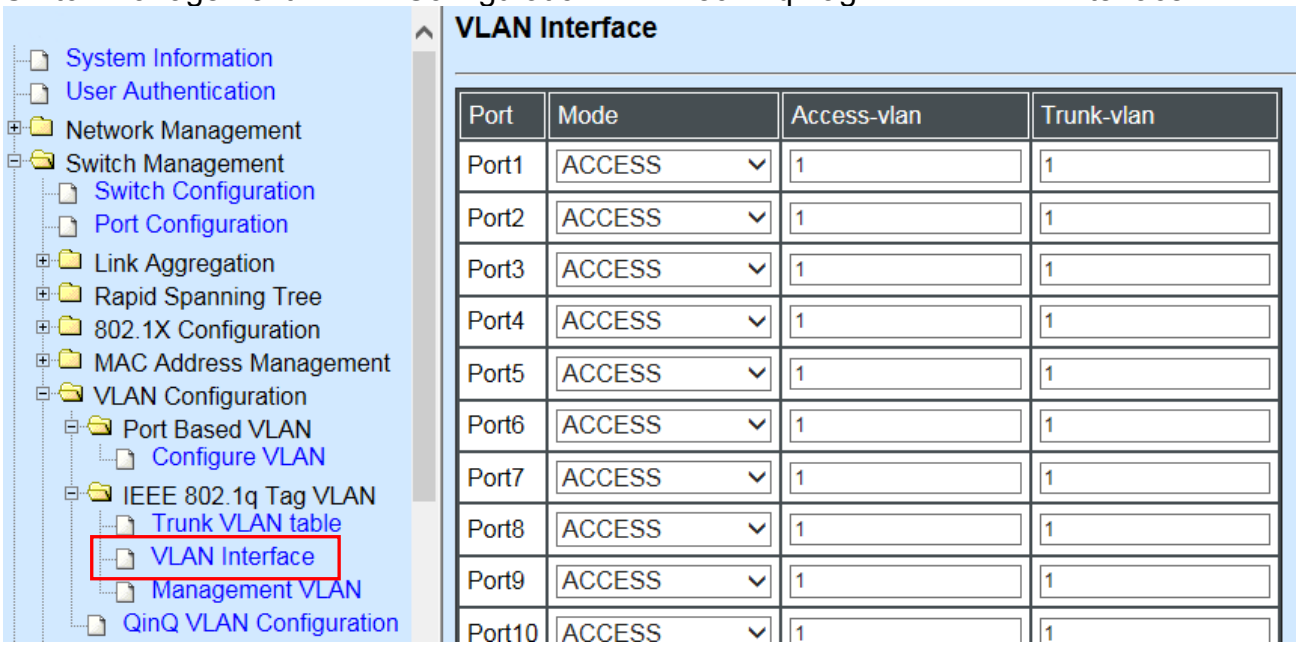
CLI Configuration:

Steps…	Commands…
1. Enter Global Configuration mode.	SWH> enable Password: SWH# config SWH(config)#
2. Create VLAN 11 and assign Port 1 and Port 48 to VLAN 11.	SWH(config)# interface 1,48 SWH(config-if-1,48)# vlan dot1q-vlan trunk-vlan 11 OK ! SWH(config-vlan-11)# exit
3. Name VLAN 11 to DataVLAN.	SWH(config)# vlan dot1q-vlan 11 SWH(config-vlan-11)# name DataVLAN OK ! SWH(config-vlan-11)# exit
4. Show currently configured dot1q VLAN membership.	FOS-3148-1A(config)# show vlan dot1q-vlan trunk-vlan ========== Configure Trunk VLAN : ==========

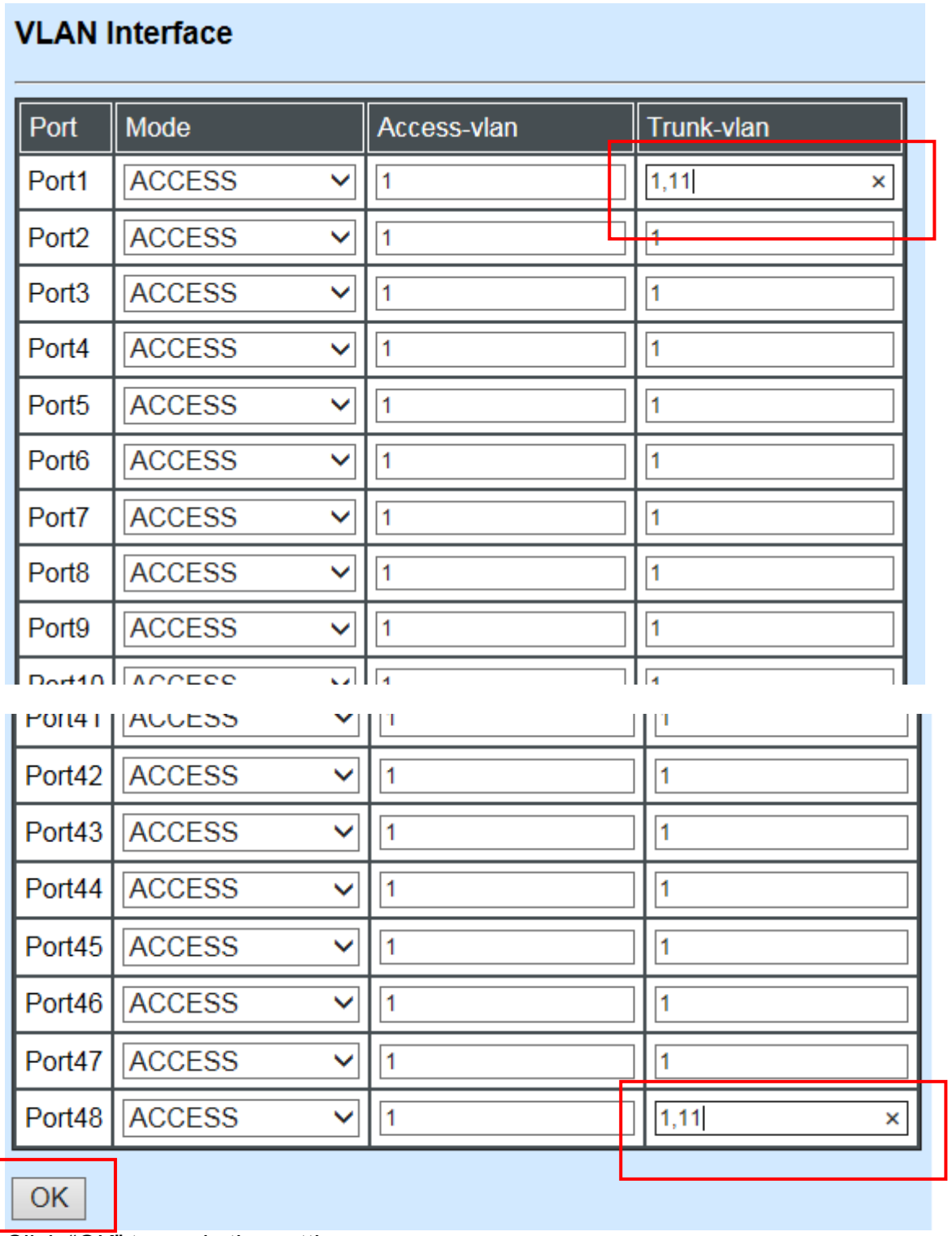
	CPU VLAN ID : 1 Management Priority : 0 VLAN Name VLAN 1 8 41 48 CPU ---------- ---- -------- -------- -------- --- Default_VLAN 1 VVVVVVVV … VVVVVVVV V DataVLAN 11 V------- -------V - *NOTE: By default, all ports are member ports of the Default_VLAN. Before removing the Default_VLAN from the VLAN table, 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.*
5. Set Port 48 to trunk mode.	SWH(config)# interface 48 SWH(config-if-48)# vlan dot1q-vlan mode trunk OK ! SWH(config-if-48)# exit
6. Change Port 1's Access VLAN to "11".	SWH(config)# interface 1 SWH(config-if-1)# vlan dot1q-vlan access-vlan 11 OK ! SWH(config-if-1)# exit
7. Show currently configured VLAN tag settings.	SWH(config)# show vlan interface ========== IEEE 802.1q Tag VLAN Interface : ========== Port Access-vlan User Priority Port VLAN Mode Trunk-vlan ---- ---------- ------------- ------------ ---------- 1 11 0 access 1,11 2 1 0 access 1 3 1 0 access 1 . . . 45 1 0 access 1 46 1 0 access 1 47 1 0 access 1 48 1 0 trunk 1,11

Web Management Configuration:

1. Select "VLAN Interface" option in IEEE 802.1Q Tag VLAN menu.
Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>VLAN Interface

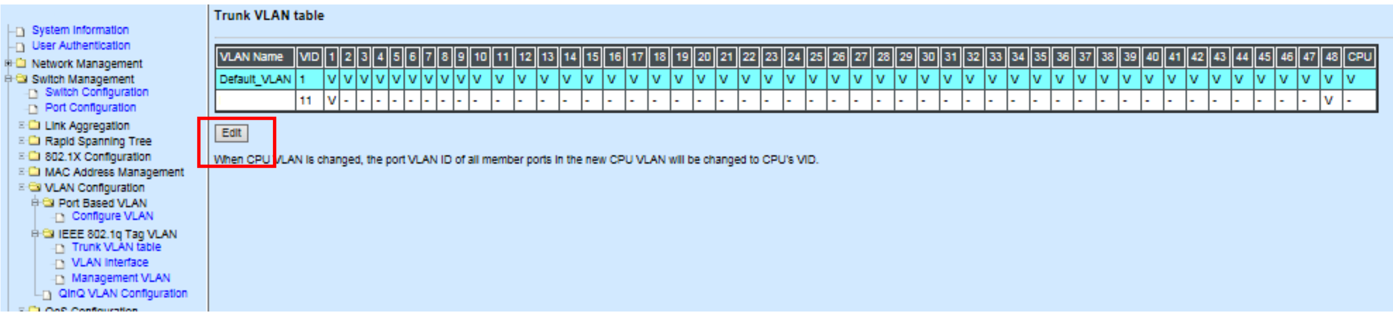


2. **Create a new Data VLAN 11 that includes Port 1 and Port 48 as members.**
   Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>VLAN INterface

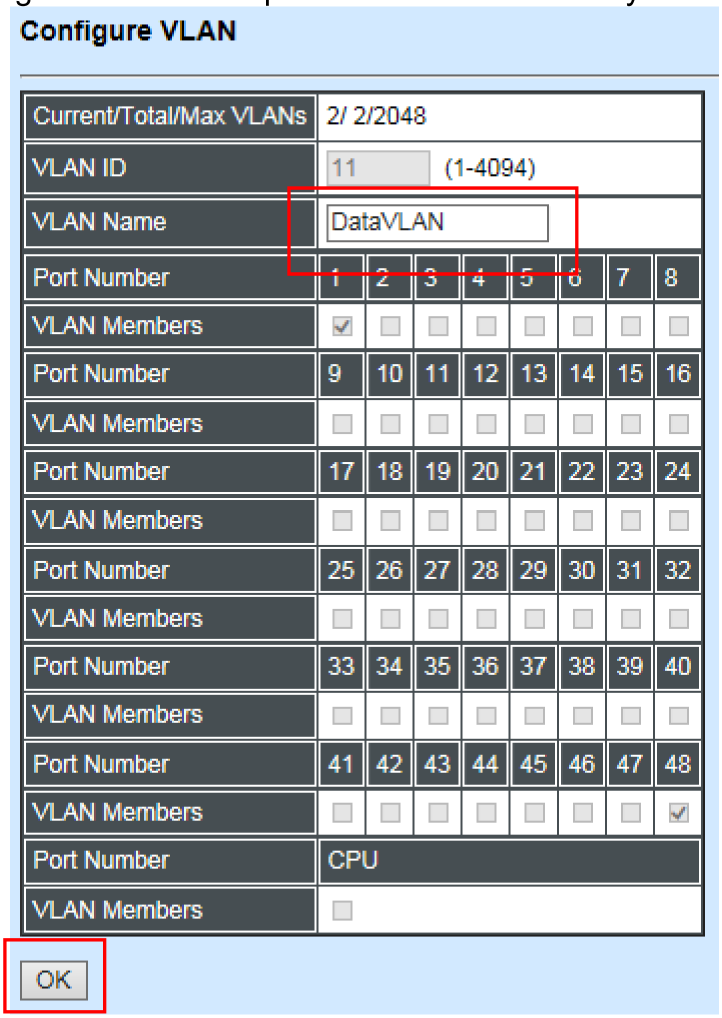


   Click “OK” to apply the settings.

3. **Edit a name for new Trunk VLAN 11 that includes Port 1 and 48 as member ports.**
   Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>Trunk VLAN table

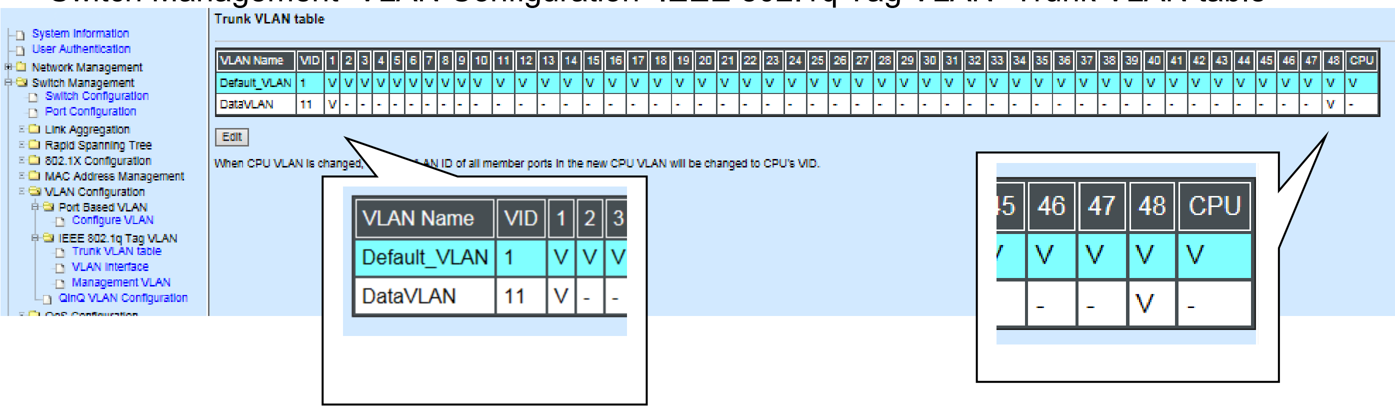


Click **"Edit"**, the following screen shows up. The VLAN Name is only the editable item.

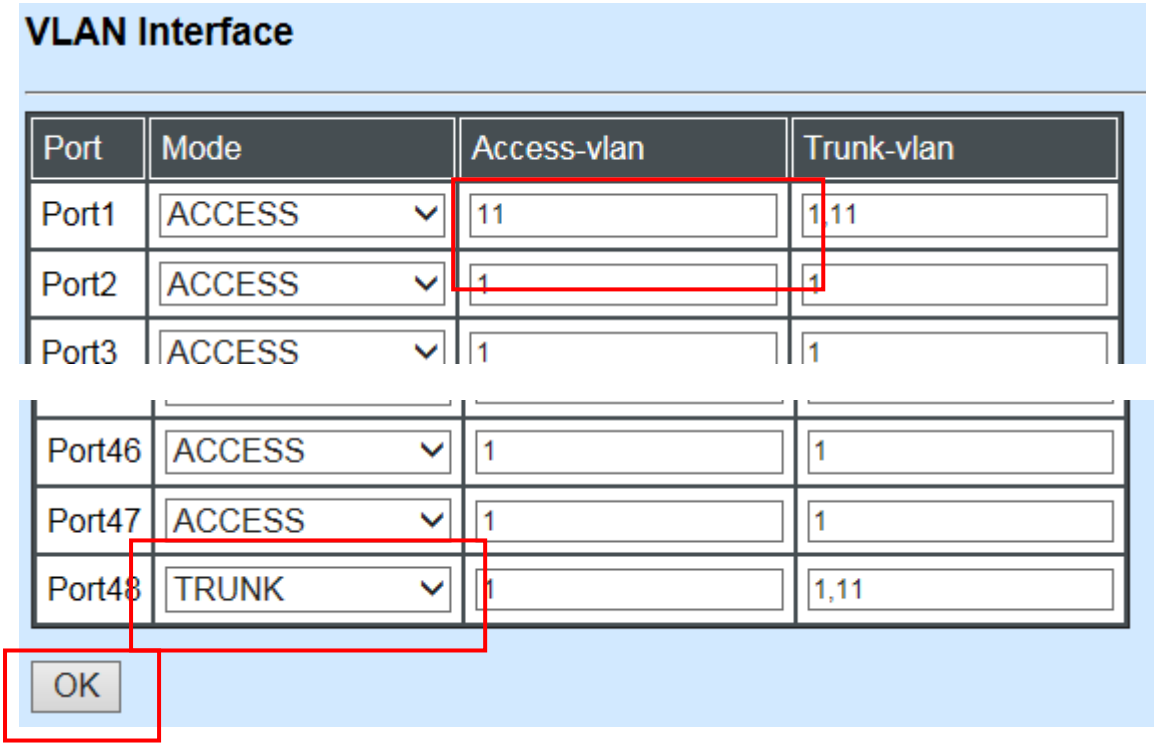


Click "OK" to apply the settings.

4. **Check Trunk VLAN 11 settings.**
Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>Trunk VLAN table



5. **Change Port 1's Access VLAN to 11, and set Port 48 to trunk mode.**
   Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN> VLAN Interface



   Click "OK" to apply the settings.

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 48 is set 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.

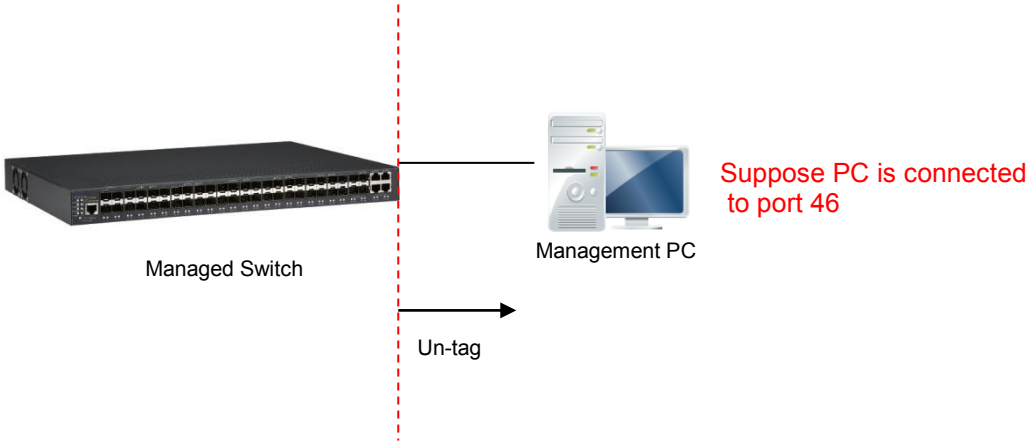
III. Management VLAN

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):

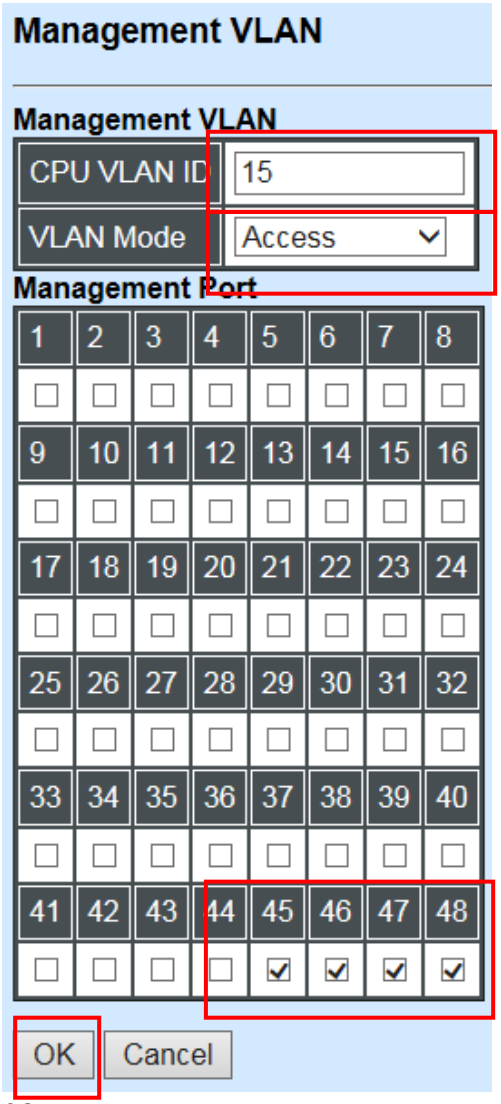
Supposed that we have the default Management VLAN whose VLAN ID is 1 for all ports, we can create new Management VLANs as required. This example is to demonstrate how to set up Management VLAN from 15 to 20 on specified ports under Access mode.

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

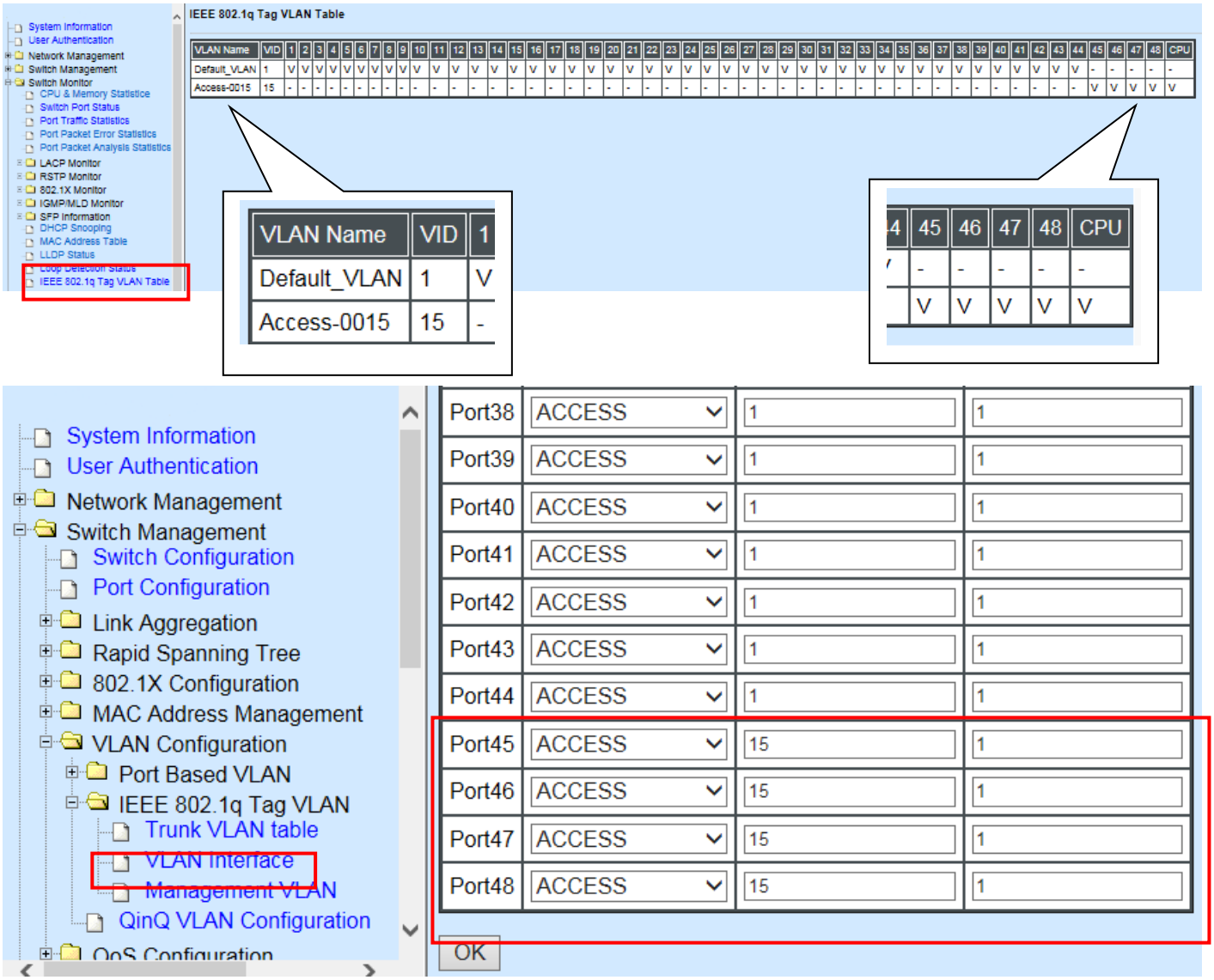
1. **Change the Management default VLAN 1 into VLAN 15 that includes Port 45, 46, 47 and 48 under Access mode.**



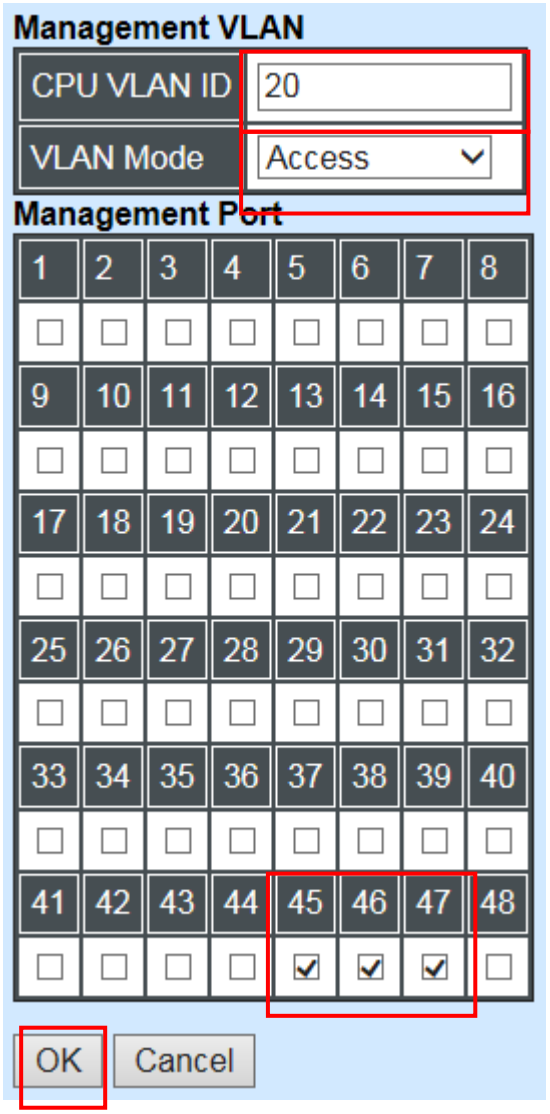
Click “OK” to apply the settings.

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: *After clicking **“OK”**, the checked boxes will soon be emptied because this Management VLAN is for configuration only.*
*To check the current status of Management VLAN, please refer to **IEEE 802.1q Tag VLAN Table or VLAN Interface**.*

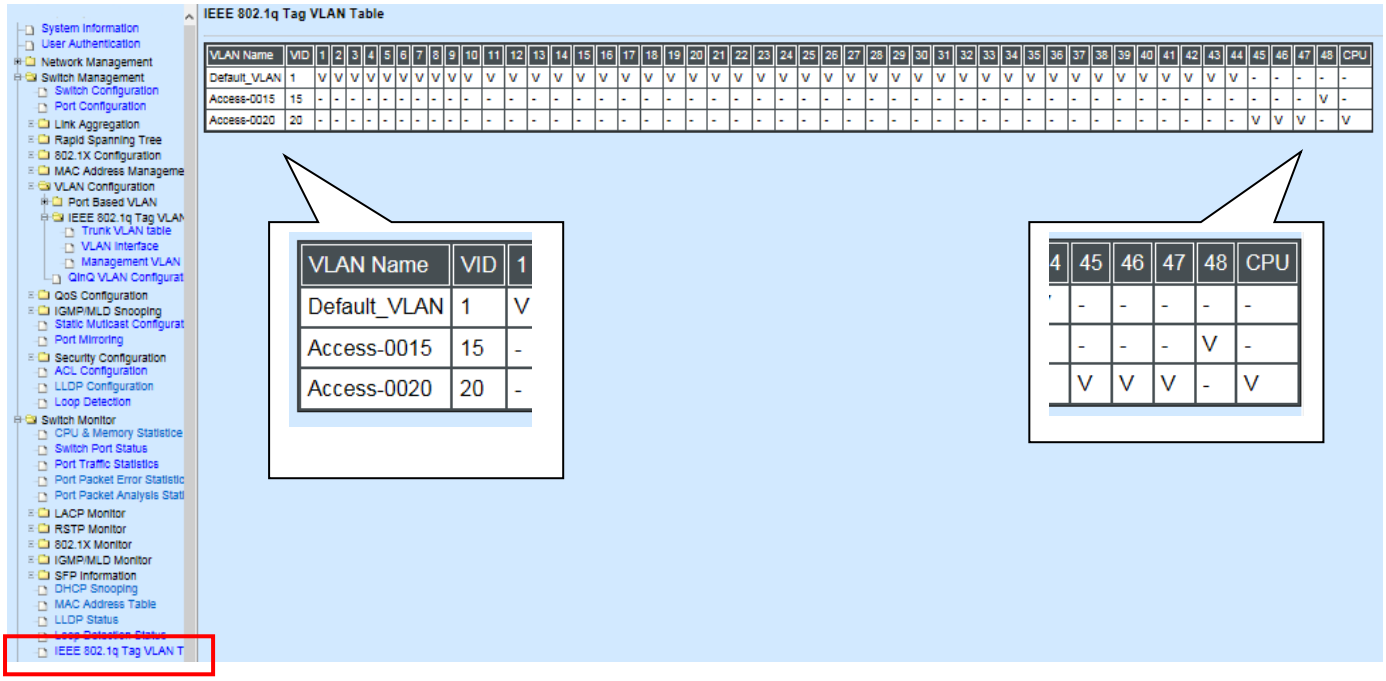

System Information
User Authentication
Network Management
Switch Management
Switch Monitor
CPU & Memory Statistics
Switch Port Status
Port Traffic Statistics
Port Packet Error Statistics
Port Packet Analysis Statistics
LACP Monitor
RSTP Monitor
802.1X Monitor
IGMP/MLD Monitor
SFP Information
DHCP Snooping
MAC Address Table
LLDP Status
Loop Detection Status
IEEE 802.1q Tag VLAN Table
IEEE 802.1q Tag VLAN Table
VLAN Name
VID
Default_VLAN
Access-0015
45
46
47
48
CPU
System Information
User Authentication
Network Management
Switch Management
Switch Configuration
Port Configuration
Link Aggregation
Rapid Spanning Tree
802.1X Configuration
MAC Address Management
VLAN Configuration
Port Based VLAN
IEEE 802.1q Tag VLAN
Trunk VLAN table
VLAN Interface
Management VLAN
QinQ VLAN Configuration
QoS Configuration
Port38 ACCESS 1 1
Port39 ACCESS 1 1
Port40 ACCESS 1 1
Port41 ACCESS 1 1
Port42 ACCESS 1 1
Port43 ACCESS 1 1
Port44 ACCESS 1 1
Port45 ACCESS 15 1
Port46 ACCESS 15 1
Port47 ACCESS 15 1
Port48 ACCESS 15 1
OK

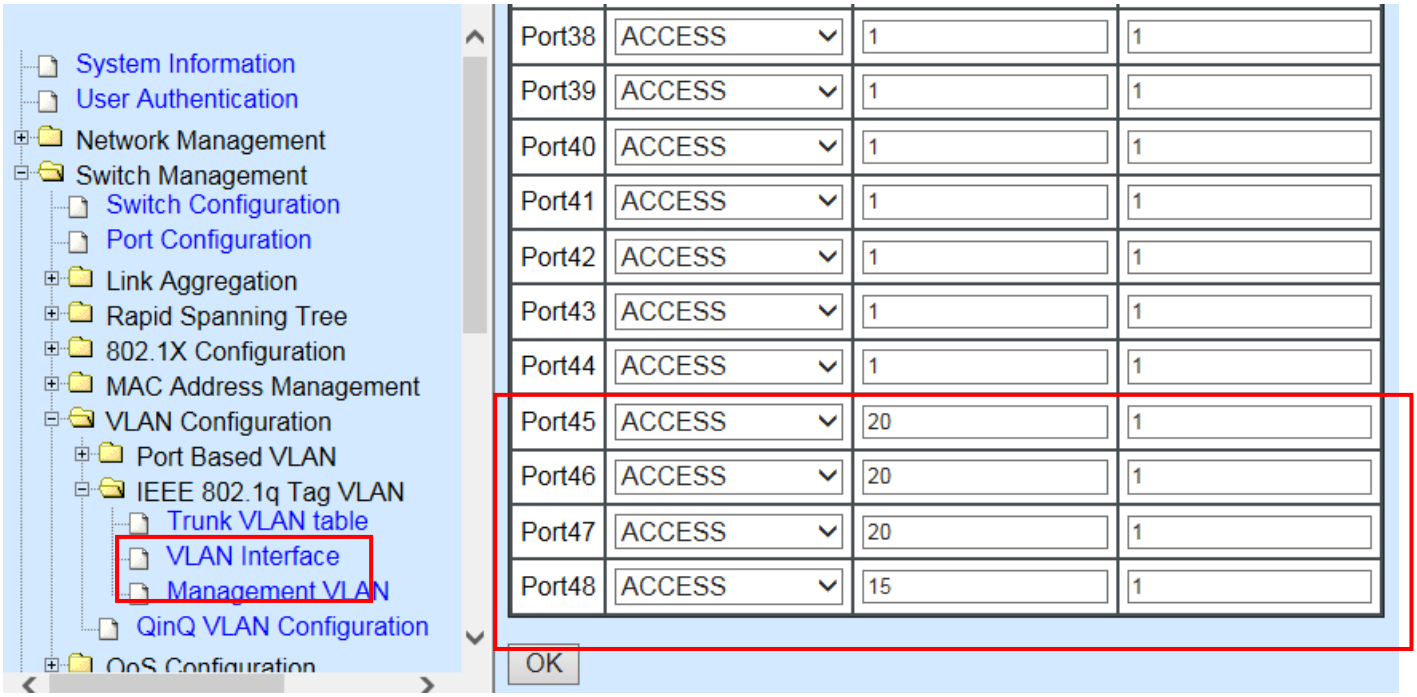
2. Now, change the Management VLAN 15 into VLAN 20 and includes Port 45, 46 and 47 under Access mode (It's necessary to include Port 46 to prevent the disconnection.)



Click "OK" to apply the settings.

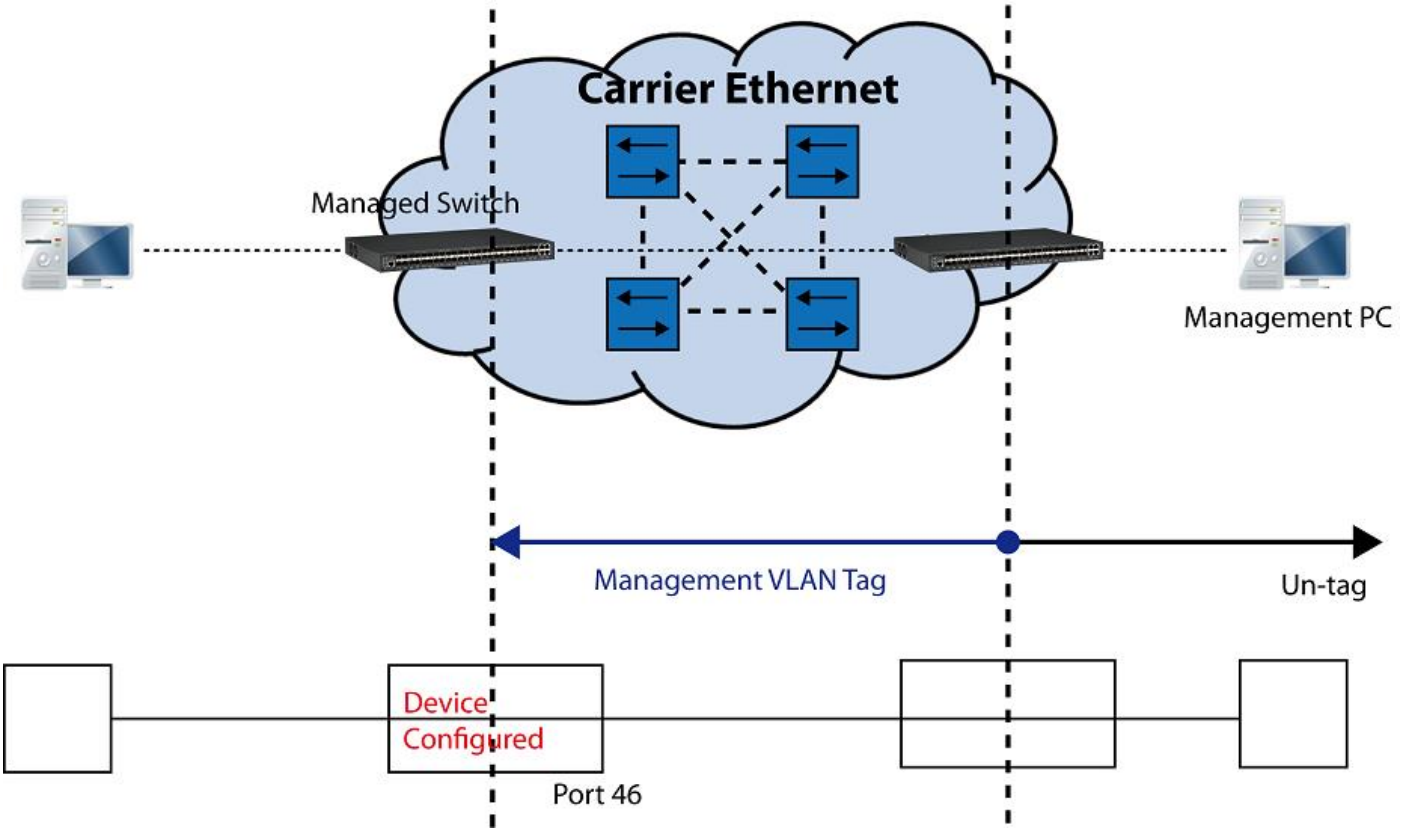
Note: *To check the current status of Management VLAN, please refer to* ***IEEE 802.1q Tag VLAN Table or VLAN Interface****.*


IEEE 802.1q Tag VLAN Table
VLAN Name
VID
Default_VLAN
Access-0015
Access-0020
System Information
User Authentication
Network Management
Switch Management
Switch Configuration
Port Configuration
Link Aggregation
Rapid Spanning Tree
802.1X Configuration
MAC Address Management
VLAN Configuration
Port Based VLAN
IEEE 802.1q Tag VLAN
Trunk VLAN table
VLAN Interface
Management VLAN
QinQ VLAN Configuration
QoS Configuration
IGMP/MLD Snooping
Port Mirroring
Security Configuration
ACL Configuration
LLDP Configuration
Loop Detection
Switch Monitor
CPU & Memory Statistics
Switch Port Status
Port Traffic Statistics
LACP Monitor
RSTP Monitor
802.1X Monitor
IGMP/MLD Monitor
SFP Information
DHCP Snooping
MAC Address Table
LLDP Status
IEEE 802.1q Tag VLAN T


System Information
User Authentication
Network Management
Switch Management
Switch Configuration
Port Configuration
Link Aggregation
Rapid Spanning Tree
802.1X Configuration
MAC Address Management
VLAN Configuration
Port Based VLAN
IEEE 802.1q Tag VLAN
Trunk VLAN table
VLAN Interface
Management VLAN
QinQ VLAN Configuration
QoS Configuration
Port38 ACCESS 1 1
Port39 ACCESS 1 1
Port40 ACCESS 1 1
Port41 ACCESS 1 1
Port42 ACCESS 1 1
Port43 ACCESS 1 1
Port44 ACCESS 1 1
Port45 ACCESS 20 1
Port46 ACCESS 20 1
Port47 ACCESS 20 1
Port48 ACCESS 15 1
OK

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

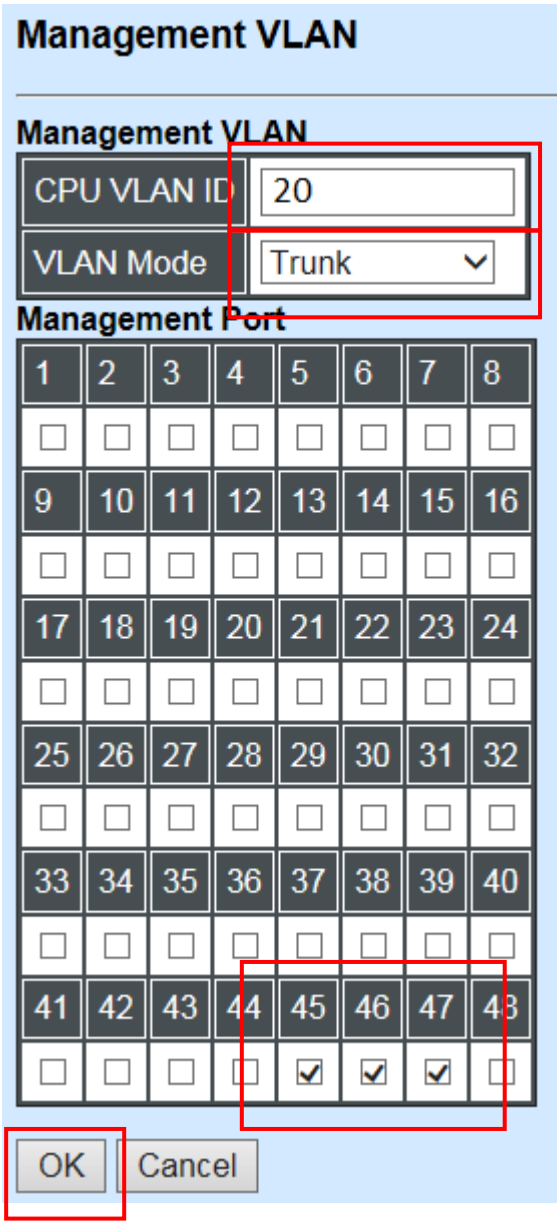
Supposed that the Management PC is remotely connected to Managed Switch Port 46 as shown above while we have a various of existing trunk vlan and the Management VLAN 15 is set on Port 45,46,47,48 and CPU as shown below. We can create new Management VLAN 20 as required. This part is to demonstrate how to set up from Management VLAN 15 to VLAN 20 on specified ports under Trunk mode.

IEEE 802.1q Tag VLAN Table

VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	CPU
Default_VLAN	1	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	-	-	-	-	-
	13	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	-
	14	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	-	-	V	-
	15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	V	V	V	V
	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	V	V	V	-
	17	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	V	V	V	-
	18	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	V	V	V	-
	19	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	V	V	V	-

IEEE 802.1q Tag VLAN Table

1. Change the Management VLAN 15 into VLAN 20 that includes Port 45, 46, 47 under Trunk mode.



Click “OK” to apply the settings.

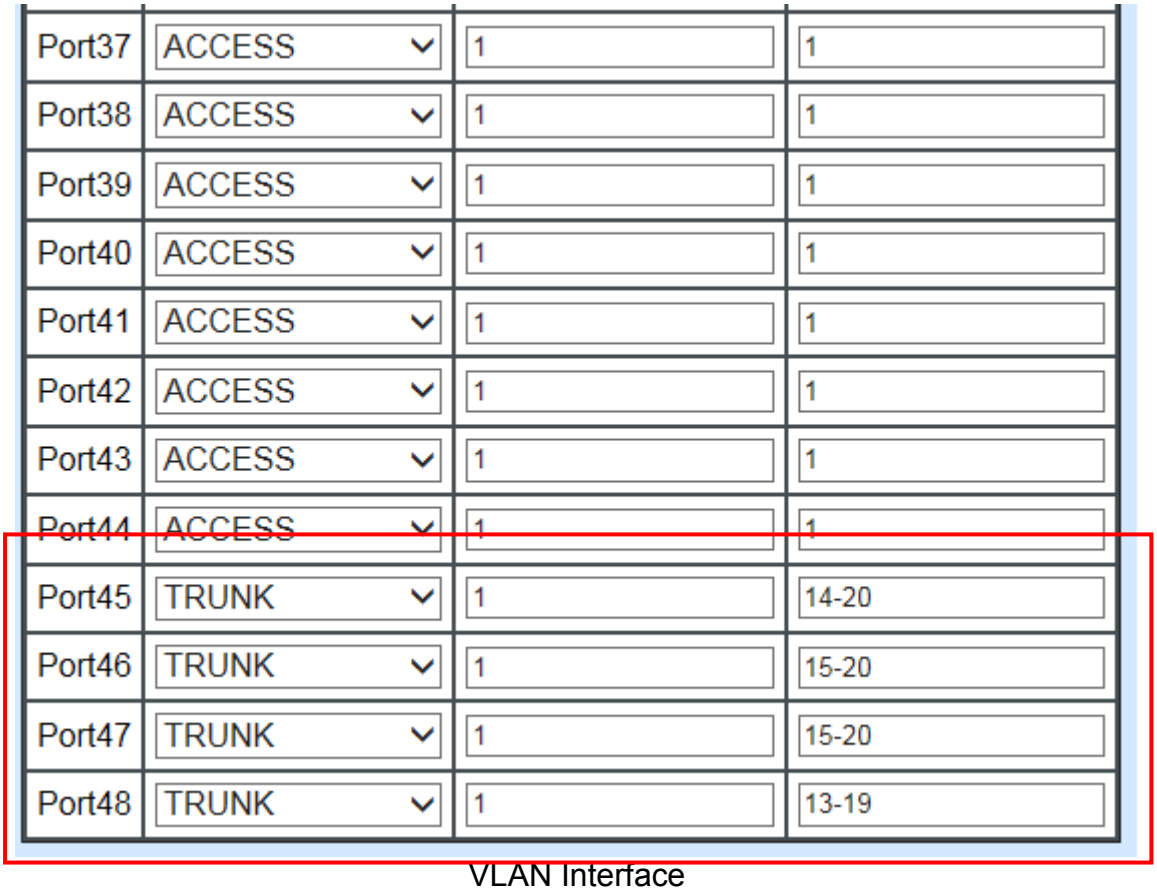
Note1: *Make sure you have correct management VLAN and VLAN Mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you click “OK” to apply.*

Note2: *After clicking **“OK”**, the checked boxes will soon be emptied because this Management VLAN is for configuration only.*
*To check the current status of Management VLAN, please refer to **IEEE 802.1q Tag VLAN Table or VLAN Interface.***

Then, Management VLAN is changing to VLAN 20.

IEEE 802.1q Tag VLAN Table

VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	CPU
Default_VLAN	1	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	-	-	-	-	-
	13	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	-
	14	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	-	-	V	-
	15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	V	V	V	-
	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	V	V	V	-
	17	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	V	V	V	-
	18	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	V	V	V	-
	19	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	V	V	V	-
	20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	V	V	-	V



VLAN Interface

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.

1. Change the Management default VLAN 1 into VLAN 15 that includes Port 45, 46, 47 and 48 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 45-48 to Management port.	Switch(config)# vlan management-vlan 15 management-port 45-48 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 dot1q-vlan tag-vlan ========== Configure Trunk VLAN : ---------- CPU VLAN ID : 15 Management Priority : 0 VLAN Name VLAN 1 8 41 48 CPU ---------- ---- -------- -------- --- Default_VLAN 1 VVVVVVVV ….. VVVVVVVV - Access-0015 15 -------- ----VVVV V

2. Now, change the Management VLAN 15 into VLAN 20 and includes Port 45, 46 and 47 to Access mode (It's necessary to include Port 46 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 45-47 to Management port.	Switch(config)# vlan management-vlan 20 management-port 45-47 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 & 20.	Switch(config)# show vlan dot1q-vlan tag-vlan ========== Configure Trunk VLAN : ---------- CPU VLAN ID : 20 Management Priority : 0 VLAN Name VLAN 1 8 41 48 CPU ---------- ---- -------- -------- --- Default_VLAN 1 VVVVVVVV ….. VVVVVVVV - Access-0015 15 -------- -------V - Access-0020 20 -------- ----VVV- 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 45,46,47,48 and CPU, we can create new Management VLAN 20 as required.

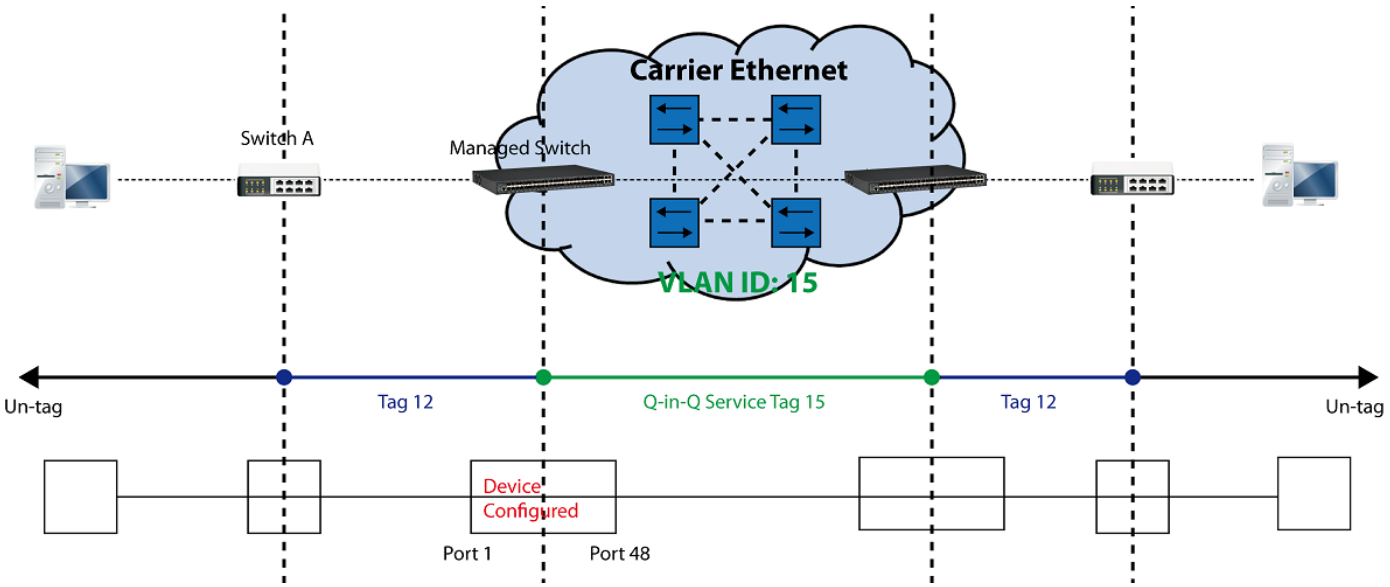
1. Change the Management VLAN 15 into VLAN 20 that includes Port 45, 46, 47 under Trunk mode.

Steps…	Commands…
1. Enter Global Configuration mode.	Switch> enable Password: Switch# configure Switch(config)#
2. Assign VLAN 20 to Management VLAN and Port 45-47 to Management port.	Switch(config)# vlan management-vlan 20 management-port 45-47 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.
3. Show currently configured dot1q settings and check CPU has been a member port in Management VLAN 20.	Switch(config)# show vlan dot1q-vlan tag-vlan ========== Configure Trunk VLAN : ========== CPU VLAN ID : 20 Management Priority : 0 VLAN Name VLAN 1 8 41 48 CPU ---------- ---- -------- -------- ---

```
Default_VLAN        1  VVVVVVVV …..  VVVV----    -
                   13  --------      -------V    -
                   14  --------      ----V--V    -
                   15  --------      ----VVVV    -
                   16  --------      ----VVVV    -
                   17  --------      ----VVVV    -
                   18  --------      ----VVVV    -
                   19  --------      ----VVVV    -
                   20  --------      ----VVV-    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.	`SWH> enable`
	`Password:`
	`SWH# config`
	`SWH(config)#`

2. Enable Q-in-Q VLAN	`SWH(config)# vlan qinq-vlan` `OK !`
3. Assign Port 48 to ISP port	`SWH(config)# vlan qinq-vlan isp-port 48` `OK !`

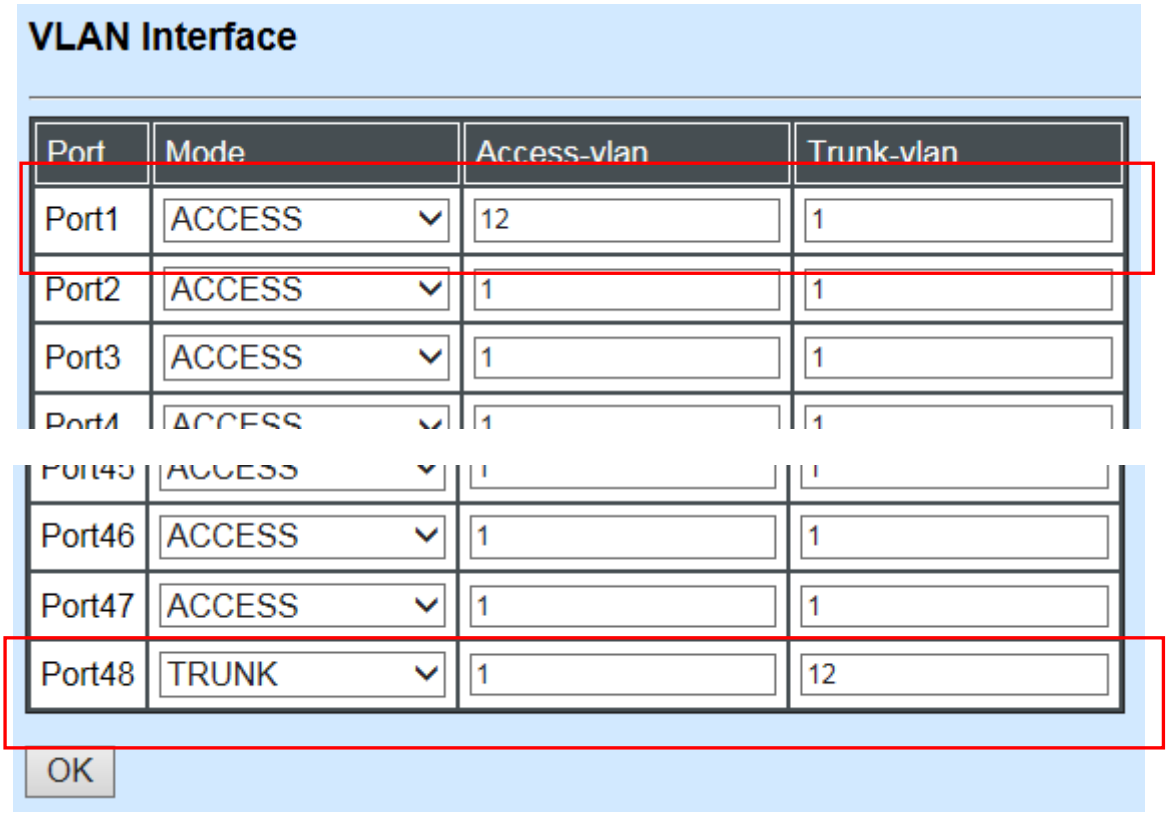
4. Create S-Tag 15 on Port 1.	`SWH(config)# interface 1`
	`SWH(config-if-1)# vlan qinq-vlan stag-vid 15`
	`OK !`
	`SWH(config-if-1)# exit`

5. Show currently configured dot1q VLAN membership.	`SWH(config)# show vlan qinq-vlan`
	`==========`
	`Q-in-Q VLAN Configuration :`
	`==========`
	`QinQ VLAN : enable`
	`Stag Ethertype : 0x9100`
	`Management Stag : 15`
	
	`Port Stag VID ISP Port`
	`---- -------- --------`
	`1 15 disable`
	`2 1 disable`
	`.`
	`.`
	`46 1 disable`
	`47 1 disable`
	`48 1 enable`
	
	`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.

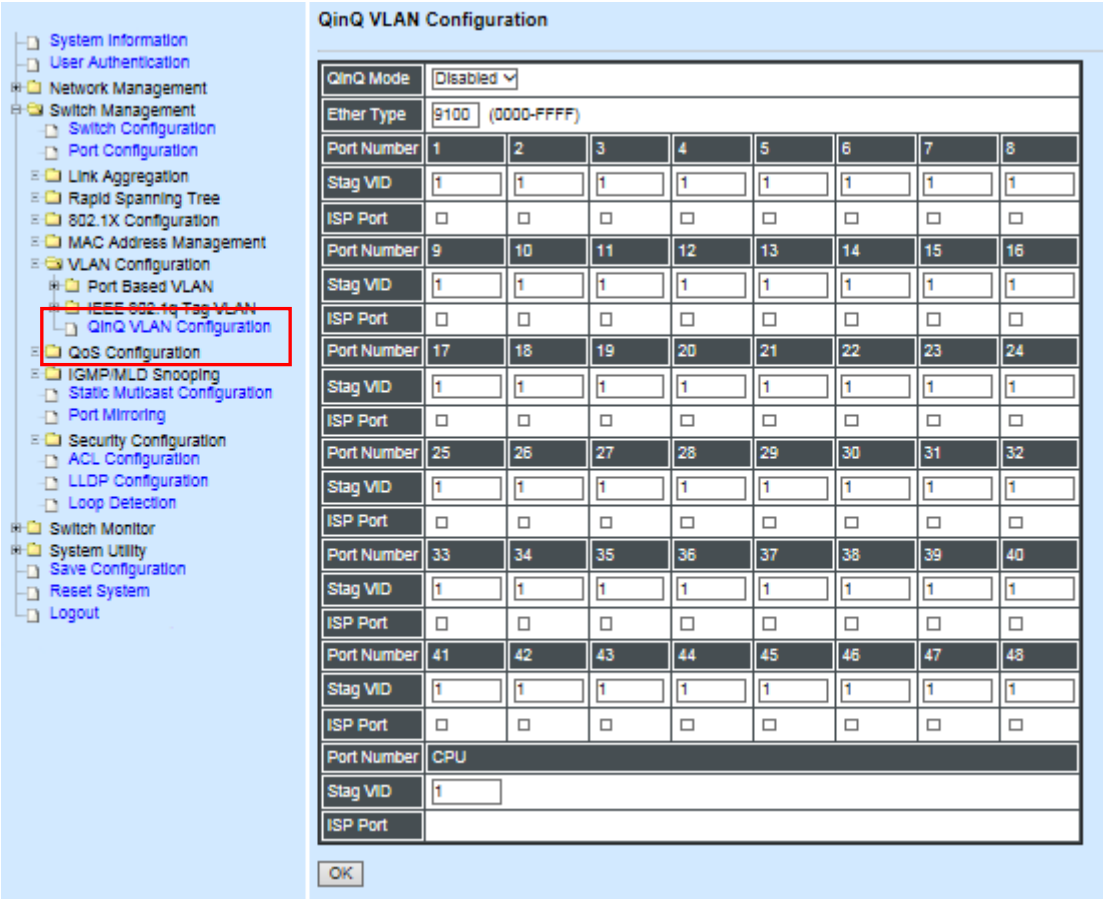
Web Management Configuration:

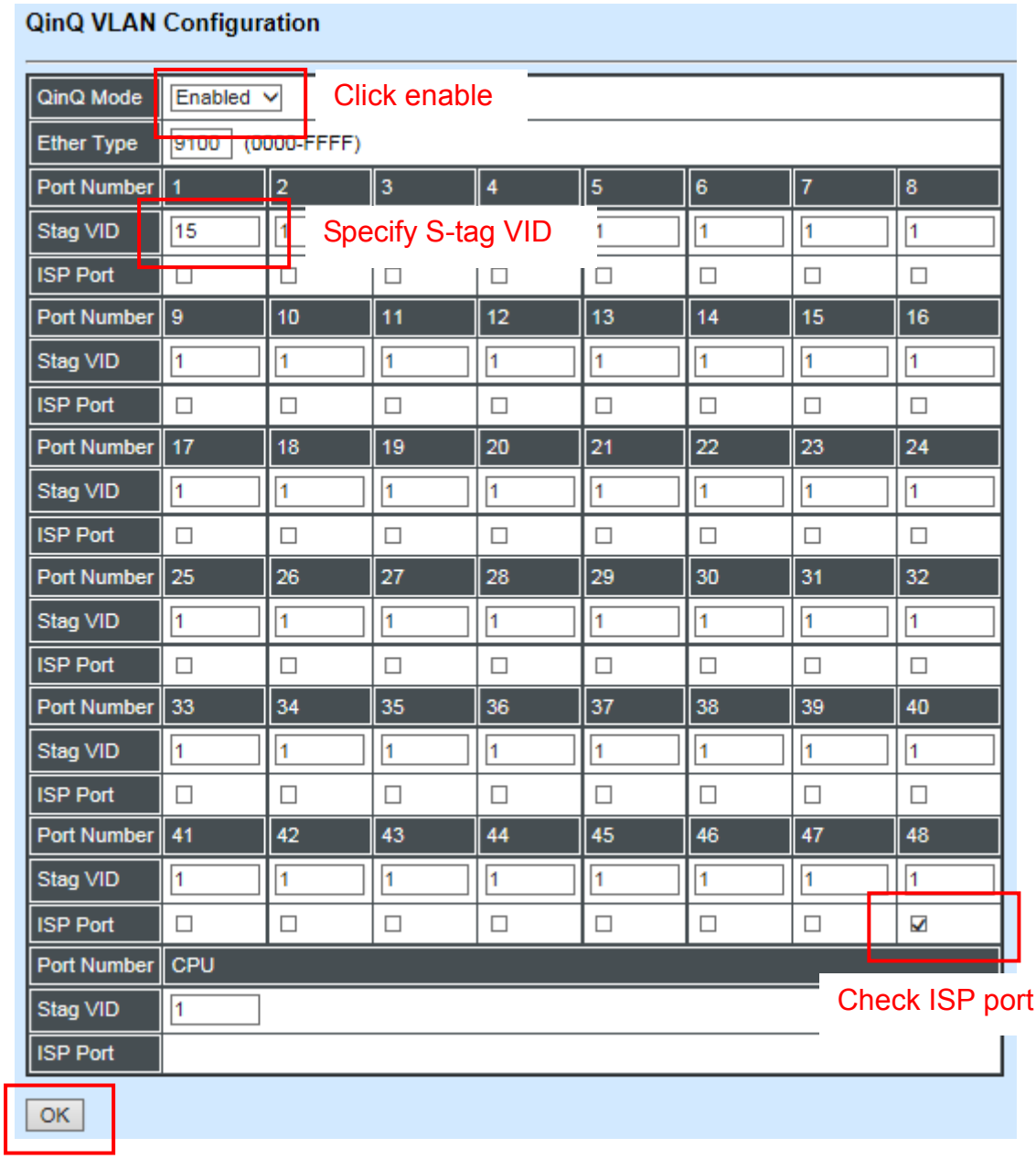
1. **Select "VLAN Interface" option in IEEE 802.1Q Tag VLAN menu.**
   Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>VLAN Interface



Check the VLAN status. Supposed that Port 1 carries access VLAN 12 while Port 48 trunk VLAN 12

2. **Create a new Service VLAN 15 that includes Port 1 and Port 48 as member ports.**
Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>QinQ VLAN Configuration





Click “OK” to apply the settings.

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 PVID configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.

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 48, two tags will be forwarded out because Port 48 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.