CONNECTION TECHNOLOGY SYSTEMS

FOS-3148 Series

44 PORTS 100/1000BASE-X SFP WITH 4 COMBO PORTS (10/100/1000BASE-T, 100/1000BASE-X SFP) UPLINK MANAGEMENT SWITCH

Network Management

User's Manual

Version 0.92

Revision History

Version	F/W	Date	Description
0.90	0.99.15	20141201	Fisrt release
0.91	0.99.16	20141208	Minor modification according to F/W v0.99.16
0.92	0.99.16	20150224	Revise trust port

Trademarks

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

Copyright Statement

Copyright © Connection Technology Systems Inc..
This publication may not be reproduced as a whole or in part, in any way whatsoever unless prior consent has been obtained from Connection Technology Systems Inc..

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limitations are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult your local distributors or an experienced radio/TV technician for help.
- 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.

Copyright © 2014 All Rights Reserved.

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

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

Table of Content

1. INTRODUCTION 9
1.1 Management Options 9
1.2 Management Software 10
1.3 Management Preparations 11
2. Command Line Interface (CLI) 13
2.1 Using the Local Console 13
2.2 Remote Console Management - Telnet 14
2.3 Navigating CLI 14
2.3.1 General Commands 15
2.3.2 Quick Keys 15
2.3.3 Command Format 16
2.3.4 Login Username & Password 17
2.4 User Mode 18
2.4.1 Ping Command 18
2.4.2 Traceroute Command 18
2.5 Privileged Mode 19
2.5.1 Copy-cfg Command 19
2.5.2 Firmware Command 20
2.5.3 Ping Command 21
2.5.4 Reload Command 21
2.5.5 Traceroute Command 21
2.5.6 Write Command 21
2.5.7 Configure Command 22
2.5.8 Show Command 22
2.6 Configuration Mode 23
2.6.1 Entering Interface Numbers 24
2.6.2 No Command 24
2.6.3 Show Command 24
2.6.4 ACL Command 26
2.6.5 Channel-group Command 29
2.6.6 Dot1x Command 31
2.6.7 IP Command 34
2.6.8 IPv6 Command 40
2.6.9 LLDP Command 42
2.6.10 Loop Detection Command 44

2.6.11 MAC Command 45
2.6.12 Management Command 46
2.6.13 Mirror Command 47
2.6.14 NTP Command 48
2.6.15 QoS Command 49
2.6.16 Security Command 50
2.6.17 SNMP-Server Command 52
2.6.18 Spanning-tree Command 55
2.6.19 Switch Command 60
2.6.20 Switch-info Command 61
2.6.21 Syslog Command 62
2.6.22 User Command 63
2.6.23 VLAN Command 65
2.6.24 Interface Command 71
2.6.25 Show interface statistics Command 77
2.6.26 Show sfp Command 78
2.6.27 Show running-config & start-up-config Command 78
3. SNMP NETWORK MANAGEMENT 79
4. WEB MANAGEMENT 80
4.1 System Information 81
4.2 User Authentication 83
4.2.1 RADIUS Configuration 85
4.3 Network Management 85
4.3.1 Network Configuration 86
4.3.2 System Service Configuration 89
4.3.3 RS232/Telnet/Console Configuration 90
4.3.4 Time Server Configuration 91
4.3.5 Device Community 92
4.3.6 Trap Destination 93
4.3.7 Trap Configuration 94
4.3.8 Mal-attempt Log Configuration 94
4.4 Switch Management 95
4.4.1 Switch Configuration 97
4.4.2 Port Configuration 97
4.4.3 Link Aggregation 98
4.4.3.1 Distribution Rule 99
4.4.3.2 Port Trunking 100

4.4.3.3 LACP Port Configuration 102
4.4.4 Rapid Spanning Tree 104
4.4.4.1 RSTP Switch Settings 105
4.4.4.2 RSTP Aggregated Port Settings 106
4.4.4.3 RSTP Physical Port Settings 107
4.4.5 802.1X Configuration 110
4.4.5.1 802.1X System Settings 111
4.4.5.2 802.1X Port Admin State 111
4.4.5.3 802.1X Port Reauthenticate 112
4.4.6 MAC Address Management 113
4.4.6.1 MAC Table Learning 113
4.4.6.2 Static MAC Table Configuration 114
4.4.7 VLAN Configuration 115
4.4.7.1 Port-Based VLAN 116
4.4.7.2 802.1Q VLAN Concept 117
4.4.7.3 Introduction to Q-in-Q 120
4.4.7.4 802.1Q VLAN 121
4.4.7.4.1 VLAN Interface 121
4.4.7.4.2 Trunk VLAN table 122
4.4.7.4.3 Management VLAN 123
4.4.7.4.4 QinQ VLAN configuration 124
4.4.8 QoS Configuration 125
4.4.8.1 QoS Priority 125
4.4.8.2 QoS Rate Limit 128
4.4.9 IGMP/MLD Snooping 129
4.4.9.1 IGMP/MLD Configure 130
4.4.9.2 IGMP/MLD VLAN ID Configuration 131
4.4.9.3 IPMC Segment 132
4.4.9.4 IPMC Profile 133
4.4.9.5 IGMP/MLD Filtering 134
4.4.10 Static Multicast Configuration 135
4.4.11 Port Mirroring 136
4.4.12 Security Configuration 137
4.4.12.1 DHCP Option 82/DHCPv6 Option 37 Settings 138
4.4.12.2 IP Source Guard Settings 141
4.4.12.3 Filter Configuration 141
4.4.12.4 Static IP/IPv6 Table Configuration 143

4.4.12.5 Configure DHCP Snooping 144
4.4.12.6 Storm Control 144
4.4.13 Access Control List (ACL) Configuratiom 145
4.4.14 LLDP Configuration 147
4.4.15 Loop Detection Configuration 148
4.5 Switch Monitor 149
4.5.1 Switch Port State 150
4.5.2 Port Traffic Statistics 152
4.5.3 Port Packet Error Statistics 152
4.5.4 Port Packet Analysis Statistics 153
4.5.5 LACP Monitor 154
4.5.5.1 LACP Port Status 155
4.5.5.2 LACP Statistics 156
4.5.6 RSTP Monitor 157
4.5.6.1 RSTP Bridge Overview 157
4.5.6.2 RSTP Port Status 158
4.5.6.3 RSTP Statistics 158
4.5.7 802.1X Monitor 159
4.5.7.1 802.1X Port Status 160
4.5.7.2 802.1X Statistics 161
4.5.8 IGMP/MLD Monitor 161
4.5.8.1 IGMP Snooping Status 162
4.5.8.2 IGMP Group Table 162
4.5.8.3 MLD Snooping Status 163
4.5.8.4 MLD Group Table 164
4.5.9 SFP Information 164
4.5.9.1 SFP Port Info 164
4.5.9.2 SFP Port State 165
4.5.10 DCHP Snooping 166
4.5.11 MAC Address Table 167
4.5.12 LLDP Status 167
4.5.13 Loop Detection Status 168
4.5.14 IEEE 802.1q Tag VLAN Table 169
4.6 System Utility 169
4.6.1 Ping 170
4.6.2 Event Log 171
4.6.3 Upgrade 171

4.6.4 Load Factory Settings 173
4.6.5 Load Factory Settings Except Network Configuration 173
4.7 Save Configuration 173
4.8 Reset System 174
APPENDIX A: Free RADIUS readme 175
APPENDIX B: Set Up DHCP Auto-Provisioning 176
APPENDIX C: VLAN Application Note 185

1. INTRODUCTION

Thank you for using the 44 100/1000Mbps SFP ports plus 4 10/100/1000Mbps combo 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

4 x 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 the enable 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, Enable, and Configuration mode, 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.

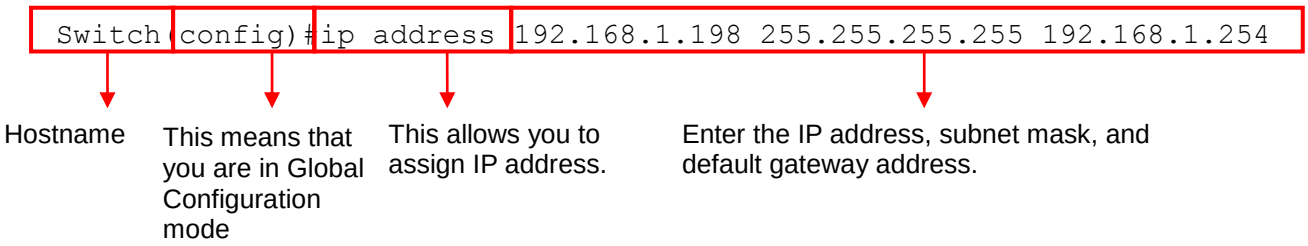
Unfinished command followed by ?	Enter an unfinished command or keyword and press “?” key to complete the command and get command syntax help.
	
	Example: List all available commands starting with the characters that you enter.
	
	`Switch#h?`
	`help  Show available commands`
	`history  Show history commands`

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 1.6.21 for edtailed explanations.
[port_list]	Enter a range of port numbers or server discontinuous port numbers. See section 1.6.21 for edtailed explanations.
[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.

Enable Mode Password

Enable mode is password-protected. When you try to enter Enable mode, a password prompt will appear to request the user to provide the legitimate passwords. Enable 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 Enable 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 trach 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 (Enable) mode is in User mode. When you successfully enter Enable 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 Enable mode and return to User Mode.
exit	Exit Enable mode and return to User Mode.
firmware	Allow users to update firmware via FTP or TFTP.
help	Display a list of available commands in Enable 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 want to restore.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
Switch# copy-cfg from tftp [A.B.C.D | 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 want to restore.
Example		
Switch# copy-cfg from ftp 192.168.1.198 HS_0600_file.conf misadmin1 abcxyz Switch# copy-cfg from tftp 192.168.1.198 HS_0600_file.conf		

2. 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]	[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	Specify backup config to be running, default or

[user_name] [password]	| startup]	startup
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
Switch# copy-cfg to tftp [A.B.C.D | A:B:C:D:E:F:G:H] [file_name] [running | default | startup]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the 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 contact information for this Managed Switch. Use “switch-info sys-contact [sys-contact]” command to edit this field.

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

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

Model Name: Display the product’s model name.

Host Name: Display the product’s host name.

Firmware Version1: Display the firmware version 1 (image-1) used in this device.

Firmware Version2: Display the firmware version 2 (image-2) used in this device.

M/B Version: Display the main board version.

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

Fiber Wavelength: Display the slide-in or fixed fiber’s TX and RX wavelength information.

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

Date Code: Display the Managed Switch Firmware date code.

Up Time: Display the up time since last restarting.

Local Time: Display local time.

Current Run In: Display the current running firmware image.

Reboot Run To: Display the firmware image which will run after next restarting.

Case Fan (1-6): Display the status of case fans.

Power (A-B): Display the status of powers.

Battery State: Display the status of battery (For BAT version only).

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.

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.
channel-group	Configure static link aggregation groups or enable LACP function.
dot1x	IEEE 802.1X global configuration commands
exit	Exit the configuration mode.
help	Display a list of available commands in 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, 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	Set up acceptable frame size and address learning, etc.
syslog	Set up required configurations for Syslog server.
user	Create a new user account.
vlan	Set up VLAN mode and VLAN configuration.
no	Disable a command or set 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 set 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 contact information for this Managed Switch. Use “switch-info sys-contact [sys-contact]” command to edit this field.

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

Model Name: Display the product’s model name.

Host Name: Display the product’s host name.

Firmware Version1: Display the firmware version 1 (image-1) used in this device.

Firmware Version2: Display the firmware version 2 (image-2) used in this device.

M/B Version: Display the main board version.

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

Fiber Wavelength: Display the slide-in or fixed fiber’s TX and RX wavelength information.

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

Date Code: Display the Managed Switch Firmware date code.

Up Time: Display the up time since last restarting.

Local Time: Display local time.

Current Run In: Display the current running firmware image.

Reboot Run To: Display the firmware image which will run after next restarting.

Case Fan (1-6): Display the status of case fans.

Power (A-B): Display the status of powers.

Battery State: Display the status of battery (For BAT version only).

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.

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 [permit | copy | redirect]	[permit | copy | redirect]	Permit, copy or redirect the action for this rule.
Switch(config-acl-RULE)# action-port [port]	[port]	Specify action port (1~48)
Switch(config-acl-RULE)# apply		Application effective
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
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 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 or “ANY”
Switch(config-acl-RULE)# rate-limit [16-1048560]	[16-1048560]	Specify rate limitation from 16 to 1048560 kbps
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

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 or “ANY”
Switch(config-acl-RULE)# vid [any | 1-4094]	[any | 1-4094]	Specify 802.1q VLAN ID or “ANY”
No command		
Switch(config-acl-RULE)# no action		Undo action command
Switch(config-acl-RULE)# no action-port		Undo action port specification
Switch(config-acl-RULE)# no destination-ipv4		Undo destination-ipv4 specification
Switch(config-acl-RULE)# no destination-ipv6		Undo destination-ipv6 specification
Switch(config-acl-RULE)# no destination-l4-port		Undo destination-l4-port specification
Switch(config-acl-RULE)# no destination-mac		Undo destination-mac specification
Switch(config-acl-RULE)# no ingress-port		Undo ingress-port specification
Switch(config-acl-RULE)# no ethertype		Undo ethertype specification
Switch(config-acl-RULE)# no protocol		Undo protocol specification
Switch(config-acl-RULE)# no rate-limit		Undo rate-limit specification
Switch(config-acl-RULE)# no source-ipv4		Undo source-ipv4 specification
Switch(config-acl-RULE)# no source-ipv6		Undo source-ipv6 specification
Switch(config-acl-RULE)# no source-l4-port		Undo source-l4-port specification
Switch(config-acl-RULE)# no source-mac		Undo source-mac specification
Switch(config-acl-RULE)# no tos		Undo TOS specification
Switch(config-acl-RULE)# no vid		Undo vid specification
Show command		**Description**
Switch(config-acl-RULE)# show		Display ACL rule configuration

2.6.5 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.
Channel-group command example		
Switch(config)# channel-group trunking corenetwork		Create a link aggregation group called "corenetwork".
Switch(config)# channel-group type destination-mac		Load-balancing depending on destination MAC address.
Switch(config)# channel-group type source-mac		Load-balancing depending on source MAC address.

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.
Channel-group & interface command example		
Switch(config)# interface 1-3		Enter port 1 to port 3's interface mode.
Switch(config-if-1-3)# channel-group lacp		Enable LACP on the selected interfaces.
Switch(config-if-1-3)# channel-group lacp key 10		Set a key value "10" to the selected interfaces.
Switch(config-if-1-3)# channel-group lacp role active		Set the selected interfaces to active LACP type.

2.6.6 Dot1x Command

Command	Parameter	Description
Switch(config)# dot1x		Enable dot1x function. When enabled, the Managed Switch acts as a proxy between the 802.1X-enabled client and the authentication server. In other words, the Managed Switch requests identifying information from the client, verifies that information with the authentication server, and relays the response to the client.
Switch(config)# dot1x reauth-period [0-3600]	[0-3600]	Specify a period of authentication time that a client authenticates with the authentication server. The allowable value is between 0 and 3600 seconds.
Switch(config)# dot1x reauthentication		Enable re-authentication function.
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.
Switch(config)# dot1x timeout [1-255]	[1-255]	Specify the time value in seconds. The Managed Switch will wait for a period of time for the response from the authentication server to an authentication request before it times out. The allowable value is between 1 and 255 seconds.

No command		
Switch(config)# no dot1x		Disable IEEE 802.1x function.
Switch(config)# no dot1x reauth-period		Reset the re-authentication period value back to the default setting (60 seconds).
Switch(config)# no dot1x reauthentication		Disable re-authentication function.
Switch(config)# no dot1x secret		Remove the original shared secret.
Switch(config)# no dot1x server		Remove the specified server IP address.
Switch(config)# no dot1x timeout		Reset the timeout value back to the default setting (10 seconds).
Show command		
Switch(config)# show dot1x		Show or verify 802.1x settings.
Switch(config)# show dot1x interface		Show or verify each interface's 802.1x settings including port status and authentication status.
Switch(config)# show dot1x interface [port_list]	[port_list]	Show or verify the selected interfaces' 802.1x settings including port status and authentication status.
Switch(config)# show dot1x statistics		Show or verify 802.1x statistics.
Switch(config)# show dot1x statistics [port_list]	[port_list]	Show or verify the selected interfaces' statistics.
Switch(config)# show dot1x status		Show or verify 802.1x status.
Switch(config)# show dot1x status [port_list]	[port_list]	Show or verify the selected interfaces' 802.1x status.
Dot1x command example		
Switch(config)# dot1x		Enable IEEE 802.1x function.
Switch(config)# dot1x reauth-period 3600		Set the reauthentication period to 3600 seconds.
Switch(config)# dot1x reauthentication		Enable re-authentication function.
Switch(config)# dot1x secret agagabcxyz		Set the shared secret to "agagabcxyz"
Switch(config)# dot1x server 192.168.1.10		Set the 802.1x server IP address to 192.168.1.10.
Switch(config)# dot1x timeout 120		Set the timeout value to 120 seconds.

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

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

Dot1x & interface command example	
Switch(config)# interface 1-3	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-1-3)# dot1x port-control auto	Set the selected ports to “auto” state.
Switch(config-if-1-3)# dot1x reauthenticate	Re-authenticate the selected interfaces immediately.

2.6.7 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:E:F:G:H]	[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 address.
Switch(config)# ip address dhcp		Enable DHCP mode.
No command		
Switch(config)#no ip address		Remove the Managed Switch’s IP address.
Switch(config)# no ip address dhcp		Disable DHCP mode.
Show command		
Switch(config)#show ip address		Show the current IP configurations or verify the configured IP settings.
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 to 192.168.1.254.
Switch(config)# ip address dhcp		Get an IP address automatically.

2. Enable DHCP relay function.

IP DHCP Snooping Command	Parameter	Description
Switch(config)# ip dhcp snooping		Enable DHCP snooping function.
Switch(config)# ip dhcp snooping dhcp-server [port_list]	[port_list]	Configure DHCP server ports.
Switch(config)# ip dhcp snooping dhcp-server-ip		Globally enable DHCP server trust IP.
Switch(config)# ip dhcp snooping dhcp-server-ip [1-4]	[1-4]	Enable DHCP server trust IP address (1 to 4).
Switch(config)# ip dhcp snooping dhcp-server-ip [1-4] ip-address [A.B.C.D]	[1-4]	Enable DHCP server trust IP address (1 to 4).
	[A.B.C.D]	Specify DHCP server trust IP address.
Switch(config)# ip dhcp snooping initiated [0-9999]	[0-9999]	Specify the time value (0~9999 Seconds) that packets might be received.
Switch(config)# ip dhcp	[180-	Specify packets’ expired time (180~259200

snooping leased [180-259200]	259200]	Seconds).
Switch(config)# ip dhcp snooping option		Enable DHCP Option 82 Relay Agent.
No command		
Switch(config)# no ip dhcp snooping		Disable DHCP Snooping function.
Switch(config)# no ip dhcp snooping dhcp-server		Remove DHCP server ports.
Switch(config)# no ip dhcp snooping dhcp-server-ip		Reset the DHCP server trust IP to the default setting.
Switch(config)# no ip dhcp snooping initiated		Reset the initiated value back to the default setting.
Switch(config)# no ip dhcp snooping leased		Reset the leased value back to the default setting.
Switch(config)# no ip dhcp snooping option		Disable DHCP Option 82 Relay Agent.
Show command		
Switch(config)# show ip address		Show the current IP configurations or verify the configured IP settings.
Switch(config)# show ip dhcp snooping		Show each interface's DHCP Snooping settings.
Switch(config)# show ip dhcp snooping interface		Show each port's DHCP Snooping Option 82 and trust port settings.
Switch(config)# show ip dhcp snooping interface [port_list]	[port_list]	Show the specified ports' DHCP Snooping Option 82 and trust port settings.
Switch(config)# show ip dhcp snooping status		Show DHCP Snooping status.
IP DHCP Snooping example		
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.

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 option		Enable the selected interfaces' DHCP Option 82 Relay Agent.
Switch(config-if-PORT-PORT)# ip dhcp snooping trust		Configure the selected interfaces to DHCP Option 82 trust ports.
Switch(config-if-PORT-PORT)# ip dhcp snooping server-trust		Configure the selected interfaces to DHCP server trust 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 ip dhcp snooping option		Set the selected interfaces to non-DHCP Option 82 Relay Agent.
Switch(config-if-PORT-PORT)# no ip dhcp snooping trust		Set the selected interfaces' to non-DHCP Option 82 trust ports.
Switch(config-if-PORT-PORT)# no ip dhcp snooping server-trust		Set the selected interfaces' to non-DHCP 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.
DHCP & Interface Example		
Switch(config)# interface 1-3		Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-1-3)# ip dhcp snooping option		Set the selected interfaces to DHCP Option 82 Relay Agent.
Switch(config-if-1-3)# ip dhcp snooping trust		Set the selected interfaces to DHCP Option 82 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 function.

Switch(config)# ip igmp snooping flooding		Set forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic will flood when enabled. However, the traffic will forward to router-ports only when disabled.
Switch(config)# ip igmp snooping immediate-leave		Enable immediate leave function.
Switch(config)# ip igmp snooping max-response-time [1-6000] (1/10secs)	[1-6000] (1/10secs)	Specify the maximum response time. This determines the maximum amount of time allowed before sending an IGMP/MLD response report.
Switch(config)# ip igmp snooping mcast-router [port_list]	[port_list]	Specify multicast router ports.
Switch(config)# ip igmp snooping query-interval [1-6000] secs	[1-6000]	Specify Query time interval. This is used to set the time interval between transmitting IGMP/MLD queries.
Switch(config)# ip igmp snooping vlan [1-4094]	[1-4094]	Specify a VLAN ID. This enables IGMP/MLD Snooping on a specified VLAN.
Switch(config)# ip igmp snooping vlan [1-4094] query	[1-4094]	Enable a querier on the specified VLAN.
No command		
Switch(config)# no ip igmp snooping		Disable IGMP/MLD Snooping function.
Switch(config)# no ip igmp snooping flooding		Disable flooding function. Traffic will forward to router-ports only when disabled.
Switch(config)# no ip igmp snooping immediate-leave		Disable immediate leave function.
Switch(config)# no ip igmp snooping max-response-time		Reset maximum response time back to the factory default.
Switch(config)# no ip igmp snooping mcast-router [port_list]	[port_list]	Remove the selected ports from the router port list.
Switch(config)# no ip igmp snooping query-interval		Reset Query interval value back to the factory default.
Switch(config)# no ip igmp snooping vlan [1-4094]	[1-4094]	Disable IGMP/MLD Snooping on the specified VLAN.
Switch(config)# no ip igmp snooping vlan [1-4094] query	[1-4094]	Disable a querier on the specified VLAN.
Show command		
Switch(config)#show ip igmp snooping		Show current IGMP/MLD snooping status including immediate leave function.
Switch(config)#show ip igmp snooping groups		Show IGMP/MLD group table.
Switch(config)#show ip igmp snooping status		Show IGMP/MLD Snooping status.

Configure IGMP Filtering policies.

IGMP Filtering command	Parameter	Description
Switch(config)# ip igmp filter		Enable IGMP Filtering function.
Switch(config)# ip igmp profile [profile_name]	[profile_name]	Specify a name for this profile.

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

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

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

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

filter		
Switch(config)# show ip igmp filter interface [port_list]	[port_list]	Show the specified ports' IGMP Filtering status.
Switch(config)# show ip igmp profile		Show IP multicast profile information.
Switch(config)# show ip igmp profile [profile_name]	[profile_name]	Show the specified profile's setting.
Switch(config)# show ip igmp segment		Show IP multicast segment information.
Switch(config)# show ip igmp segment [1-400]	[1-400]	Show the specified segment's setting.
Switch(config)# show ip igmp static-multicast-ip		Show static multicast IP table.
Switch(config-segment-ID)# show		Show the selected segment's setting.
Switch(config-profile-ID)# show		Show the selected profile's setting.
Switch(config)# show ip sourceguard interface		Show each interface's IP sourceguard type.
Switch(config)# show ip sourceguard static-ip		Show the IP source binding table for sourceguard function.
IGMP & Interface example		
Switch(config)# interface1-3		Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-1-3)# ip igmp filter		Enable IGMP Filter on port 1 to port 3.
Switch(config-if-1-3)# ip igmp filter profile Silverprofile		Assign the selected ports to the specified profile "Silverprofile".
Switch(config-if-1-3)# ip igmp max-groups 400		Set the maximum number of multicast streams to 400.
Switch(config-if-1-3)# ip igmp static-multicast-ip 224.10.0.5 vlan 50		Create a static multicast IP to VLAN entry.

2.6.8 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 auto mode.
Switch(config)# ipv6 address dhcp force		Configure DHCPv6 function in force mode.
Switch(config)# ipv6 address dhcp rapid-commit		Allows the two-way message exchange instead of 4-way for address assignment.
“ipv6 address dhcp” commands are functional only when autoconfiguration is enabled.		
Switch(config)# ipv6 address global [A:B:C:D:E:F:G:H/10~128] [A:B:C:D:E:F:G:H]	[A:B:C:D:E:F:G:H/10~128]	Specify switch IPv6 global address and prefix-length.
	[A:B:C:D:E:F:G:H]	Specify switch IPv6 default gateway.
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		Disable IPv6 stateless autoconfig.

address autoconfig		
Switch(config)# no ipv6 address dhcp		Disable DHCPv6 function.
Switch(config)# no ipv6 address dhcp rapid-commit		Disable rapid-commit feature.
Switch(config)# ipv6 address global		Clear IPv6 global address entry
Switch(config)# 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 information of the Managed Switch.
IPv6 command example		
Switch(config)# ipv6 address autoconfig		Enable Ipv6 autoconfiguration.
Switch(config)# ipv6 address dhcp auto		Enable DHCPv6 auto mode.

2.6.9 LLDP Command

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

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 initiated-delay [0-300]	[0-300]	Specify a period of time the Managed Switch will wait before the initial LLDP packet is sent. The allowable initiated-delay value is between 0 and 300 seconds.

Switch(config)# lldp interval [1-180]	[1-180]	Specify the time interval for updated LLDP packets to be sent. The allowable interval value is between 1 and 180 seconds.
Switch(config)# lldp packets [1-16]	[1-16]	Specify the amount of packets that are sent in each discovery. The allowable packet value is between 1 and 16 seconds.
Switch(config)# lldp tlv-select capability		Enable Capability attribute to be sent.
Switch(config)# lldp tlv-select management-address		Enable Management Address attribute to be sent.
Switch(config)# lldp tlv-select port-description		Enable Port Description attribute to be sent.
Switch(config)# lldp tlv-select system-description		Enable System Description attribute to be sent.
Switch(config)# lldp tlv-select system-name		Enable System Name attribute to be sent.
No command		
Switch(config)# no lldp hold-time		Reset the hold-time value back to the default setting.
Switch(config)# no lldp initiated-delay		Reset the initiated-delay value back to the default setting.
Switch(config)# no lldp interval		Reset the interval value back to the default setting.
Switch(config)# no lldp packets		Reset the packets-to-be-sent value back to the default setting.
Switch(config)# no lldp tlv-select capability		Disable Capability attribute to be sent.
Switch(config)# no lldp tlv-select management-address		Disable Management Address attribute to be sent.
Switch(config)# no lldp tlv-select port-description		Disable Port Description attribute to be sent.
Switch(config)# no lldp tlv-select system-description		Disable System Description attribute to be sent.
Switch(config)# no lldp tlv-select system-name		Disable System Name attribute to be sent.
Show command		
Switch(config)# show lldp		Show or verify LLDP settings.
Switch(config)# show lldp interface		Show or verify each interface's LLDP port state.
Switch(config)# show lldp interface [port_list]		Show or verify the selected interfaces' LLDP port state.
Switch(config)# show lldp status		Show current LLDP status.
LLDP command example		**Description**
Switch(config)# lldp hold-time 60		Set the hold-time value to 60 seconds.
Switch(config)# lldp initiated-delay 60		Set the initiated-delay value to 60 seconds
Switch(config)# lldp interval 10		Set the updated LLDP packets to be sent in very 10 seconds.
Switch(config)# lldp packets 2		Set the number of packets to be sent in each discovery to 2.
Switch(config)# lldp tlv-select capability		Enable Capability attribute to be sent.
Switch(config)# lldp tlv-select management-address		Enable Management Address attribute to be sent.

Switch(config)# lldp tlv-select port-description	Enable Port Description attribute to be sent.
Switch(config)# lldp tlv-select system-description	Enable System Description to be sent.
Switch(config)# lldp tlv-select system-name	Enable System Name to be sent.

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

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

2.6.10 Loop Detection Command

Command	Parameter	Description
Switch(config)# loop-detection		Enable Loop Detection function.
Switch(config)# loop-detection interval [1-180]	[0-180]	Set up Loop Detection time interval from 1 to 180 seconds.
Switch(config)# loop-detection unlock-interval [1-1440]	[1-1440]	Set up Loop Detection unlock time interval from 1 to 1440 minutes.
Switch(config)# loop-detection vlan-id [1-4094]	[1-4094]	Set up Loop Detection VLAN ID.
No command		
Switch(config)# no loop-detection		Disable Loop Detection function.
Switch(config)# no loop-detection interval		Reset Loop Detection time interval to default setting.
Switch(config)# no loop-detection unlock-interval		Reset Loop Detection unlock time interval to default setting.
Switch(config)# no loop-detection vlan-id		Reset Loop Detection unlock time interval to default setting.
Show command		
Switch(config)# show loop-detection		Show Loop Detection settings.
Switch(config)# show loop-detection status		Show Loop Detection status of all ports.
Switch(config)# show loop-detection status [port_list]	[port_list]	Show Loop Detection status of the ports.
Loop Detection command example		
Switch(config)# loop-detection interval 60		Set the Loop Detection time interval to 60 seconds.

Switch(config)# loop-detection unlock-interval 120	Set the Loop Detection unlock time interval to 120 minutes.
Switch(config)# loop-detection vlan-id 100	Set the Loop Detection VLAN ID to 100.

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

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

2.6.11 MAC Command

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

MAC Command	Parameter	Description
Switch(config)# mac address-table aging-time [0, 10-77925]	[0, 10-77925]	Enter the aging time for MAC addresses in seconds. 0= never aging out.
No command		
Switch(config)# no mac address-table aging-time		Set MAC address table aging time to the default value (300 seconds).
Show command		
Switch(config)# show mac address-table		Show MAC addresses learned by the Managed Switch
Switch(config)# show mac address-table clear		Clear MAC address table.
Switch(config)# show mac address-table interface [port_list]	[port_list]	Show MAC addresses learned by the specified interfaces.
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 table aging time or verify configured aging time.
MAC command example		
Switch(config)#mac address-table aging-time		Set MAC address aging time to 200

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]	Create a MAC address to VLAN entry. Specify a MAC address.
	[1-4094]	Specify the VLAN where the packets with the Destination MAC address can be forwarded.
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 address table.
	[1-4094]	Specify the VLAN to which the specified MAC belongs.
Switch(config-if-PORT-PORT)# no mac learning		Disable MAC learning function.
Show command		
Switch(config)# show mac address-table		Show MAC addresses learned by the Managed Switch
Switch(config)# show mac address-table clear		Clear MAC address table.
Switch(config)# show mac address-table interface [port_list]		Show MAC addresses learned by the specified interfaces.
Switch(config)# show mac address-table mac [mac-addr]		Show the specific MAC address information.
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 table aging time or verify currently configured aging time.

2.6.12 Management Command

Command	Parameter	Description
Switch(config)# management console timeout [0 | 5-300]	[0 | 5-300]	To disconnect the Managed Switch when console management is inactive for a certain period of time. Specify “0” to disable timeout function. The allowable value is from 5 to 300 seconds.
Switch(config)# management ssh		To management the Managed Switch via SSH.

Switch(config)# management telnet		To management 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		To manage the Managed Switch via Web management.
No command		
Switch(config)# no management console timeout		Reset console timeout to 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		Set Telnet port back to the default setting. The default port number is 23.
Switch(config)# no management web		Disable Web management.
Show command		
Switch(config)# show management		Show or verify current management settings including management platform that can be used and Telnet port number.
Management command example		
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.

2.6.13 Mirror Command

Command	Parameter	Description
Switch(config)# mirror destination [port]	[port]	Specify the preferred destination port (1~48) for mirroring.
Switch(config)# mirror source [port_list]	[port_list]	Specify a source port number or several source port numbers for port mirroring.
No command		
Switch(config)# no mirror destination		Disable port mirroring function or remove mirroring destination port.
Switch(config)# no mirror source		Remove mirroring source ports.
Show command		
Switch(config)# show mirror		Show or verify current port mirroring destination and source ports.
Mirror command example		
Switch(config)# mirror destination 26		The selected source ports' data will mirror to port 26.
Switch(config)# mirror source 1-10		Port 1 to 10's data will mirror to the destination (target) port.

2.6.14 NTP Command

Command	Parameter	Description
Switch(config)# ntp		Enable the Managed Switch to synchronize the clock with a time server.
Switch(config)# ntp daylight-saving		Enable the daylight saving function.
Switch(config)# ntp daylight-saving recurring		Enable daylight saving with recurring mode.
Switch(config)# ntp daylight-saving date		Enable daylight saving 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]	Offset setting for daylight saving function of 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]	Offset setting for daylight saving function of 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 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 time server IP/IPv6 address.
Switch(config)# ntp syn-interval [1-8]	[1-8]	Specify the interval time to synchronize from NTP time server. **1=1hour, 2=2hours, 3=3hours, 4=4hours** **5=ghours, 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 147 time zones. For example, “Switch(config)# ntp time-zone ?”
No command		
Switch(config)# no ntp		Disable the Managed Switch to synchronize the clock with a time server.
Switch(config)# no ntp daylight-saving		Disable the daylight saving function.
Switch(config)# no ntp offset		Set the offset value back to the default setting.
Switch(config)# no ntp server1		Delete the primary time server IP address.
Switch(config)# no ntp server2		Delete the primary time server IP address.
Switch(config)# no ntp syn-interval		Set the synchronization interval back to the default setting.
Switch(config)# no ntp time-zone		Set the time-zone setting back to the default.

Show command	
Switch(config)# show ntp	Show or verify current time server settings.
NTP command example	
Switch(config)# ntp	Enable the Managed Switch to synchronize the clock with a time server.
Switch(config)# ntp daylight-saving date	Enable the daylight saving function at ddate 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 time server IP address to 192.180.0.12.
Switch(config)# ntp server2 192.180.0.13	Set the secondary time server IP address to 192.180.0.13.
Switch(config)# ntp syn-interval 4	Set the synchronization interval to 4 hours.
Switch(config)# ntp time-zone 3	Set the time zone to GMT-8:00 Vancouver.

2.6.15 QoS Command

1. Set up Qos

QoS command	Parameter	Description
Switch(config)# qos [802.1p | dscp]	[802.1p | dscp]	Specify QoS mode
Switch(config)# qos dscp-map [0-63] [0-7]	[0-63]	Specify a DSCP value.
	[0-7]	Specify a queue value.
Switch(config)# qos management-priority [0-7]	[0-7]	Specify management default 802.1p bit
Switch(config)# qos queuing-mode [weight]	[weight]	Specify QoS queuing mode as weight mode
Switch(config)# qos queue-weighted [1:2:4:8:16:32:64:128]	[1:2:4:8:16:32:64:128]	Specify the queue weighted
Switch(config)# qos remarking dscp [by-dscp]	[by-dscp]	Specify DSCP bit remarking mode
Switch(config)# qos remarking dscp-map [1-8]	[1-8]	Specify 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 802.1p and priority mapping ID
Switch(config)# qos 802.1p-map	[0-7]	Specify a 802.1p value.
	[0-7]	Specify a queue value.
No command		
Switch(config)# no qos dscp-map [0-63]	[0-63]	Undo specify a DSCP value
Switch(config)# no qos management-priority		Undo specify management default 802.1p bit

Switch(config)# no queuing-mode		Specify QoS queuing mode as strict mode
Switch(config)# no qos queue-weighted		Undo specify the queue weighted
Switch(config)# no qos remarking dscp		Undo specify DSCP bit remarking mode
Switch(config)# no qos remarking dscp-map [1-8]	[1-8]	Undo specify DSCP and priority mapping ID
Switch(config)# no qos remarking 802.1p		Disable 802.1p bit remarking
Switch(config)# no qos remarking 802.1p-map [1-8]	[1-8]	Undo specify a 802.1p value
Switch(config)# no qos 802.1p-map		Undo 802.1p mapping
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 QoS interface per port(s)
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] kbps	[500-1000000] kbps	Specify ingress rate limit value.
Switch(config-if-PORT-PORT)# qos rate-limit egress [500-1000000] kbps	[500-1000000] kbps	Specify egress rate limit value.
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		Delete QoS ingress rate limit setting.
Switch(config-if-PORT-PORT)# no qos rate-limit egress		Delete QoS egress rate limit setting.
Switch(config-if-PORT-PORT)# no qos user-priority		Set the user priority value setting back to the factory default.

2.6.16 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/

multicast/ unknown unicast storms. Any broadcast/multicast/unknown unicast packets exceeding the specified value will then be dropped.

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

Security command	Parameter	Description
Switch(config)# security storm-protection broadcast [1-1024k]	[1-1024k]	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, 512k, 1024k 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 [1-1024k]	[1-1024k]	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, 512k, 1024k ***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 [1-1024k]	[1-1024k]	Specify the maximum unicast packets per second (pps). Any 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, 512k, 1024k ***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 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.
Show command		
Switch(config)# show security storm-protection		Show current storm control settings.
Security command example		
Switch(config)# security storm-protection broadcast 1024k		Set the maximum broadcast packets per second (pps) to 1024k. Any broadcast packets exceeding this specified threshold will then be dropped.
Switch(config)# security storm-protection multicast 1024k		Set the maximum unknown multicast packets per second (pps) to 1024k. Any unknown multicast packets exceeding this specified threshold will then be dropped.
Switch(config)# security storm-protection unicast 1024k		Set the maximum unicast packets per second (pps) to 1024k. Any unicast packets exceeding the specified threshold will then be dropped.

2.6.17 SNMP-Server Command

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

Snmp-server command	Parameter	Description
Switch(config)# snmp-server		Enable SNMP server function globally.
Switch(config)# snmp-server community [community]	[community]	Specify a SNMP community name of up to 20 alphanumeric characters.
Switch(config-community-NAME)# active		Enable this SNMP community account.
Switch(config-community-NAME)# description [Description]	[Description]	Enter the description for this SNMP community of up to 35 alphanumerical characters.
Switch(config-community-NAME)# level [admin | rw | ro]	[admin | rw | ro]	Specify the access privilege for this SNMP account. **admin:** Full access right, including maintaining user account, system information, loading factory settings, etc.. **rw:** Read & Write access privilege. Partial access right, unable to modify user account, system information and load factory settings. **ro:** Read Only access privilege.

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 this SNMP community account. In this example “mycomm” community is disabled.
Switch(config-community-NAME)# no description		Remove the SNMP community descriptions for “mycomm”.
Switch(config-community-NAME)# no level		Remove the configured access privilege. This will set this community’s level to “access denied”.
Show command		
Switch(config)# show snmp-server		Show or verify whether SNMP is enabled or disabled.
Switch(config)# show snmp-server community		Show or verify each SNMP server account’s information.
Switch(config)# show snmp-server community [community]		Show the specified SNMP server account’s settings.
Switch(config-community-NAME)# show		Show the selected community’s settings.
Exit command		
Switch(config-community-NAME)# exit		Return to Global Configuration mode.
Snmp-server example		
Switch(config)# snmp-server community mycomm		Create a new community “mycomm” and edit the details of this community account.
Switch(config-community-mycomm)# active		Activate the SNMP community “mycomm”.
Switch(config-community-mycomm)# description rddeptcomm		Add a description for “mycomm” community.
Switch(config-community-mycomm)# level admin		Set “mycomm” community level to admin (full access privilege).

2. Set up a SNMP trap destination.

Trap-destination command	Parameter	Description
Switch(config)# snmp-server trap-destination [1-10]	[1-10]	Create a trap destination account.
Switch(config-trap-ACCOUNT)# active		Enable this SNMP trap destination account.
Switch(config-trap-ACCOUNT)# community [community]	[community]	Enter the community name of network management system.
Switch(config-trap-ACCOUNT)# destination [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the trap destination IP/IPv6 address for this trap destination account.
No command		
Switch(config)# no snmp-	[1-10]	Delete the specified trap destination

server trap-dest [1-10]		account.
Switch(config-trap-ACCOUNT)# no active		Disable this SNMP trap destination account.
Switch(config-trap-ACCOUNT)# no community		Delete the configured community name.
Switch(config-trap-ACCOUNT)# no description		Delete the configured trap destination description.
Show command		
Switch(config)# show snmp-server trap-destination		Show SNMP trap destination account information.
Switch(config)# show snmp-server trap-destination [1-10]	[1-10]	Show the specified SNMP trap destination account information.
Switch(config-trap-ACCOUNT)# show		Show and verify the selected trap destination account's information.
Exit command		
Switch(config-trap-ACCOUNT)# exit		Return to Global Configuration mode.
Trap-destination example		
Switch(config)# snmp-server trap-destination 1		Create a trap destination account.
Switch(config-trap-1)# active		Activate this trap destination account.
Switch(config-trap-1)# community mycomm		Refer this trap destination account to the community "mycomm".
Switch(config-trap-1)# description redepttrapdest		Add a description for this trap destination account.
Switch(config-trap-1)# destination 192.168.1.254		Set trap destination IP address to 192.168.1.254.

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

Trap-type command	Parameter	Description
Switch(config)# snmp-server trap-type [all | auth-fail | battery-mode | case-fan | cold-start | port-link | power-down | warm-start]	[all | auth-fail | battery-mode | case-fan | cold-start | port-link | power-down | warm-start]	Specify a trap type that will be sent when a certain situation occurs. **all:** A trap will be sent when authentication fails, broadcast packets exceed the threshold value, the device cold /warm starts, port link is up or down and power is down. **auth-fail:** A trap will be sent when any unauthorized user attempts to login. **battery-mode:** A trap will be sent when the battery mode is changed. **case-fan:** A trap will be sent when the fan is not working or fails. **cold-start:** A trap will be sent when the device boots up.

		port-link: A trap will be sent when the link is up or down. **power-down:** A trap will be sent when the device's power is down. **warm-start:** A trap will be sent when the device restarts.
No command		
Switch(config)# no snmp-server trap-type [all | auth-fail | battery-mode | case-fan | cold-start | port-link | power-down | warm-start]	[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 community		Show community configuration.
Switch(config)# show snmp-server trap-destination		Show trap destination configuration.
Switch(config)# show snmp-server trap-type		Show the current enable/disable status of each type of trap.
Trap-type example		
Switch(config)# snmp-server trap-type all		All types of SNMP traps will be sent.

2.6.18 Spanning-tree Command

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

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

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

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

Spanning-tree command	Parameter	Description
Switch(config)# spanning-tree aggregated-port		Enable Spanning Tree Protocl function on aggregated ports.
Switch(config)# spanning-tree aggregated-port cost [0-200000000]	[0-200000000]	Specify aggregated ports' path cost.
Switch(config)# spanning-tree aggregated-port priority [0-15]	[0-15]	Specify aggregated ports' priority. **0=0, 1=16, 2=32, 3=48, 4=64, 5=80 6=96, 7=112, 8=128, 9=144, 10=160 11=176, 12=192, 13=208, 14=224, 15=240**
Switch(config)# spanning-tree aggregated-port edge		Enable aggregated ports to shift to forwarding state when the link is up. If you know a port is directly connected to an end device (that doesn't support RSTP) then set it as an edge port to ensure maximum performance. This will tell the switch to immediately start forwarding traffic on the port and not bother trying to establish a RSTP connection. Otherwise, turn it off.
Switch(config)# spanning-tree aggregated-port p2p [forced_true | forced_false | auto]	[forced_true | forced_false | auto]	Set the aggregated ports to non-point to point ports (forced_false) or allow the Managed Switch to detect point to point status automatically (auto). By default, aggregated ports are set to point to point ports (forced_true).
Switch(config)# spanning-tree delay-time [4-30]	[4-30]	Specify the Forward Delay value in seconds. The allowable value is between 4 and 30 seconds.
Switch(config)# spanning-tree hello-time [1-10]	[1-10]	Specify the Hello Time value in seconds. The allowable value is between 4 and 30 seconds.
Switch(config)# spanning-tree max-age [6-200]	[6-200]	Specify the Maximum Age value in seconds. The allowable value is between 6 and 200.
Switch(config)# spanning-tree priority [0-15]	[0-15]	Specify a priority value on a per switch basis. The allowable value is between 0 and 15. **0=0, 1=4096, 2=8192, 3=12288, 4=16384** **5=20480, 6=24576, 7=28672, 8=32768** **9=36864, 10=40960,** **11=45056,12=49152** **13=53248, 14=57344, 15=61440**
Switch(config)# spanning-tree version [compatible | normal]	[compatible | normal]	Set up RSTP version. **"compatible"** means that the Managed Switch is compatible with STP. **"normal"** means that the Managed Switch uses RSTP.

No command		
Switch(config)# no spanning-tree aggregated-port		Disable STP on aggregated ports.
Switch(config)# no spanning-tree aggregated-port cost		Reset aggregated ports' cost to the factory default.
Switch(config)# no spanning-tree aggregated-port priority		Reset aggregated ports' priority to the factory default.
Switch(config)# no spanning-tree aggregated-port edge		Disable aggregated ports' edge ports status.
Switch(config)# no spanning-tree aggregated-port p2p		Reset aggregated ports to point to point ports (forced_true).
Switch(config)# no spanning-tree delay-time		Reset the Forward Delay time back to the factory default.
Switch(config)# no spanning-tree hello-time		Reset the Hello Time back to the factory default.
Switch(config)# no spanning-tree max-age		Reset the Maximum Age back to the factory default.
Show command		
Switch(config)# show spanning-tree		Show or verify STP settings on the per switch basis.
Switch(config)# show spanning-tree aggregated-port		Show or verify STP settings on aggregated ports.
Switch(config)# show spanning-tree interface		Show each interface's STP information including port state, path cost, priority, edge port state, and p2p port state.
Switch(config)# show spanning-tree interface [port_list]	[port_list]	Show the selected interfaces' STP information including port state, path cost, priority, edge port state, and p2p port state.
Switch(config)# show spanning-tree statistics		Show each interface and each link aggregation group's statistics information including the total RSTP packets received, RSTP packets transmitted, STP packets received, STP packets transmitted, TCN (Topology Change Notification) packets received, TCN packets transmited, illegal packets received, and unknown packets received.
Switch(config)# show spanning-tree statistics [port_list | llag]	[port_list | llag]	Show the selected interfaces or link aggregation groups' statistics information including the total RSTP packets received, RSTP packets transmitted, STP packets received, STP packets transmitted, TCN (Topology Change Notification) packets received, TCN packets transmited, illegal packets received, and unknown packets received.
Switch(config)# show spanning-tree status		Show current RSTP port status.
Switch(config)# show spanning-tree status [port_list	[port_list | llag]	Show the selected interfaces or link aggregation groups' statistics information

| llag]		
Switch(config)# show spanning-tree overview		Show the current STP state.

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

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

Spanning tree & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# spanning-tree		Enable spanning-tree protocol on the selected interfaces.
Switch(config-if-PORT-PORT)# spanning-tree cost [1-200000000]	[1-200000000]	Specify cost value on the selected interfaces.
Switch(config-if-PORT-PORT)# spanning-tree priority [0-15]	[0-15]	Specify priority value on the selected interfaces. **0=0, 1=4096, 2=8192, 3=12288, 4=16384** **5=20480, 6=24576, 7=28672, 8=32768** **9=36864, 10=40960, 11=45056,12=49152** **13=53248, 14=57344, 15=61440**
Switch(config-if-PORT-PORT)# spanning-tree edge		Set the selected interfaces to edge ports.
Switch(config-if-PORT-PORT)# spanning-tree p2p [forced_fasle | auto]	[forced_fasle | auto]	Set the aggregated ports to non-point to point ports (forced_false) or allow the Managed Switch to detect point to point status automatically (auto). By default, aggregated ports are set to point to point ports (forced_true).
No command		

Switch(config-if-PORT-PORT)# no spanning-tree		Disable spanning-tree protocol on the selected interfaces.
Switch(config-if-PORT-PORT)# no spanning-tree cost		Set the cost value back to the factory default.
Switch(config-if-PORT-PORT)# no spanning-tree priority		Set the priority value back to the factory default.
Switch(config-if-PORT-PORT)# no spanning-tree edge		Set the selected interfaces to non-edge ports.
Switch(config-if-PORT-PORT)# no spanning-tree p2p		Set the selected interface to point to point ports.
Show command		
Switch(config)# show spanning-tree		Show or verify STP settings on the per switch basis.
Switch(config)# show spanning-tree aggregated-port		Show or verify STP settings on aggregated ports.
Switch(config)# show spanning-tree interface		Show each interface's STP information including port state, path cost, priority, edge port state, and p2p port state.
Switch(config)# show spanning-tree interface [port_list]	[port_list]	Show the selected interfaces' STP information including port state, path cost, priority, edge port state, and p2p port state.
Switch(config)# show spanning-tree statistics		Show each interface and each link aggregation group's statistics information including the total RSTP packets received, RSTP packets transmitted, STP packets received, STP packets transmitted, TCN (Topology Change Notification) packets received, TCN packets transmited, illegal packets received, and unknown packets received.
Switch(config)# show spanning-tree statistics [port_list | llag]	[port_list | llag]	Show the selected interfaces or link aggregation groups' statistics information including the total RSTP packets received, RSTP packets transmitted, STP packets received, STP packets transmitted, TCN (Topology Change Notification) packets received, TCN packets transmited, illegal packets received, and unknown packets received.
Switch(config)# show spanning-tree status		Show current RSTP port status.
Switch(config)# show spanning-tree status [port_list | llag]	[port_list | llag]	Show the selected interfaces or link aggregation groups' statistics information
Switch(config)# show spanning-tree overview		Show the current STP state.
Spanning-tree & interface command example		**Description**
Switch(config)# interface 1-3		Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For

	example:1,3 or 2-4
Switch(config-if-1-3)# spanning-tree cost 100	Set the selected interfaces' cost to 100.
Switch(config-if-1-3)# spanning-tree priority 0	Set the selected interfaces' priority to 0
Switch(config-if-1-3)# spanning-tree edge	Set the selected ports to edge ports.
Switch(config-if-1-3)# spanning-tree p2p forced_false	Set the selected ports to non-P2P ports.

2.6.19 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 transmission unit in bytes. The allowable MTU value is between 1518 and 9600 bytes.
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 to default 1518 bytes.
Show command		
Switch(config)# show switch bpdu		Show current BPDU information.
Switch(config)# show switch mtu		Show current maximum transmission unit setting.
Switch command example		
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.

2.6.20 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 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 contact information for this Managed switch, up to 55 alphanumeric characters.
Switch(config)# switch-info system-location [sys_location]	[sys_location]	Enter a brief description, up to 55 alphanumeric characters, of the Managed Switch location. 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		Delete the entered company name information.
Switch(config)# no switch-info dhcp-vendor-id		Delete the entered DHCP vendor ID information.
Switch(config)# no switch-info system-contact		Delete the entered system contact information.
Switch(config)# no switch-info system-location		Delete the entered system location information.
Switch(config)# no switch-info system-name		Delete the entered system name information.
Switch(config)# no switch-info host-name		Set the hostname to the factory default.
Show command		
Switch(config)# show switch-info		Show or verify switch information including company name, system contact, system

	location, system name, model name, firmware version and fiber type.
Switch-info example	
Switch(config)# switch-info company-name telecomxyz	Set the company name to “telecomxyz”.
Switch(config)# switch-info system-contact info@company.com	Set the system contact 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 to “edgeswitch10”.

2.6.21 Syslog Command

Syslog command	Parameter	Description
Switch(config)# syslog		Enable system 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 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 current system log settings.
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.

2.6.22 User Command

1. Create a new login account.

User command	Parameter	Description
Switch(config)# user name [user_name]	[user_name]	Enter the new account's username. The authorized user login name is up to 20 alphanumeric characters. Only 3 login accounts can be registered in this device.
Switch(config-user-NAME)# active		Activate this user account.
Switch(config-user-NAME)# description [description]	[description]	Enter the brief description for this user account.
Switch(config-user-NAME)# level [admin | rw | ro]	[admin | rw | ro]	Specify this user's access level. **admin (administrator):** Full access right, including maintaining user account & system information, loading factory settings, etc.. **rw (read & write):** 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 this user account.
No command		
Switch(config)#no user name [username]	[username]	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.
Switch(config-user-NAME)# no password		Remove the configured password value.
Switch(config-user-NAME)# no level		Reset access level privilege back to the factory default (access denied).
Show command		
Switch(config)# show user name		List all user accounts.
Switch(config)# show user name [user_name]	[user_name]	Show the specific account's information.
Switch(config-user-NAME)# show		Show or verify the newly-created user account's information.
User command example		
Switch(config)#user name miseric		Create a new login account "miseric".

Switch(config-user-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 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 31 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		Set the radius port setting back to the factory default.
Switch(config)# no user radius retry-time		Set the retry time setting back to the factory default.
Switch(config)# no user radius secret		Remove the configured secret value.
Switch(config)# no user radius server1		Delete the specified IP address.
Switch(config)# no user radius server2		Delete the specified IP address.
Show command		
Switch(config)#show user radius		Show current RADIUS settings.
User command example		
Switch(config)# user radius		Enable RADIUS authentication.
Switch(config)# user radius radius-port 1812		Set RADIUS server port number to 1812.
Switch(config)# user radius retry-time 2		Set the retry value to 2. The Managed Switch will try to reconnect twice if the RADIUS server is not reachable.
Switch(config)# user radius secret abcxyzabc		Set up a secret for validating communications between RADIUS clients.

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

2.6.23 VLAN Command

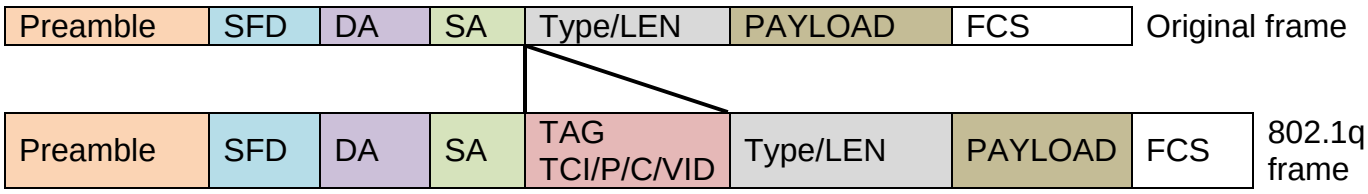
A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast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

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

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 VLAN ID 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.

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

1. Use "Interface" command to configure a group of ports' 802.1q VLAN settings.

VLAN & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
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 access mode (untagged).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk		Set the selected ports to trunk mode (tagged).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk native		Set the selected ports to trunk-native mode. (Tagged and untagged) **Note : When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.**
Switch(config-if-PORT-PORT)# vlan port-based [name]	[name]	Set the selected ports to a specified port-based VLAN. **Note :** **Need to create a port-based VLAN group under VLAN global configuration mode before joining it.**
No command		
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan access-vlan		Set the selected ports' PVID to the default setting.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan mode trunk		Disable native VLAN for untagged traffic.

native		
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected ports' from the specified trunk VLAN.
Switch(config-if-PORT-PORT)# no vlan port-based [name]	[name]	Delete the selected ports from the specified port-based VLAN.
VLAN & interface command example		
Switch(config)# interface 1-3		Enter port 1 to port 3's interface mode.
Switch(config-if-1-3)# vlan dot1q-vlan access-vlan 10		Set port 1 to port 3's Access-VLAN ID (PVID) to 10.
Switch(config-if-1-3)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
Switch(config-if-1-3)# vlan dot1q-vlan mode trunk native		Enable native VLAN for untagged traffic.
Switch(config-if-1-3)# vlan port-based mktpbvlan		Set the selected ports to the specified port-based VLAN "mktpbvlan".

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

Port-based VLAN can effectively segment one network into several broadcast domains. Broadcast, multicast and unknown packets will be limited 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.

VLAN dot1q command	Parameter	Description
Switch(config)# vlan dot1q-vlan [1-4094]	[1-4094]	Enter a VID number to modify an existing 802.1q VLAN. **Note :** **802.1q VLAN ID need to be created under interface global command. In here you can only modify it instead of creating a new VLAN ID.**
Switch(config-vlan-ID)# name [vlan_name]	[vlan_name]	Specify a descriptive name for this VLAN ID, max 15 characters.
Switch(config)# vlan isolation [port_list]	[port_list]	To assign uplink ports which will form a port-based VLAN group with all other downlink ports seperatedly so to isolated downlink ports from each other except from uplink ports.
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 name for this port-based VLAN.
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.
Show command		
Switch(config)# show vlan dot1q-vlan tag-vlan		Show IEEE 802.1q tag VLAN table
Switch(config)# show vlan dot1q-vlan trunk-vlan		Show configure trunk VLAN table
Switch(config-vlan-ID)# show		Show the membership status of this VLAN ID
Switch(config)# show vlan interface		Show all ports’ VLAN assignment and VLAN mode.
Switch(config)# show vlan interface [port_list]	[port_list]	Show the selected ports’ VLAN assignment and VLAN mode.
Switch(config)# show vlan port-based		Show port-based VLAN table.
Exit command		
Switch(config-vlan-ID)# exit		Return to Global configuration mode.
Port-based VLAN example		
Switch(config)# vlan port-based MKT_Office		Create a port-based VLAN “MKT_Office”.
Switch(config)# vlan management-vlan 1 management-port 1-3 mode access		Set VLAN 1 to management VLAN (untagged) and port 1~3 to management ports.

802.1q VLAN Configuration Example

Name	Ports	Mode	PVID	VID
Sales	1-22	Trunk	Default	10,20
RD	23-44	Trunk-native	50	30,40
SQA	45-46	Access	60	N/A
PME	47-48	Access	70	N/A

1. Create 802.1q VLAN IDs

Switch(config)# interface 1-22	Enter port 1 to port 22's interface mode.
Switch(config-if-1-22)# vlan dot1q-vlan trunk-vlan 10, 20	Set port 1 to port 22's Trunk-VLAN ID (VID) to 10 and 20.
Switch(config-if-1-22)# vlan dot1q-vlan mode trunk	Set the selected ports to Trunk Mode (tagged).
Switch(config-if-1-22)#exit	Exit current ports interface mode
Switch(config)# interface 23-44	Enter port 23 to port 44's interface mode.
Switch(config-if-23-44)# vlan dot1q-vlan access-vlan 50	Set port 23 to port 44's Access-VLAN ID (PVID) to 50.
Switch(config-if-23-44)# vlan dot1q-vlan trunk-vlan 30,40	Set port 23 to port 44's Trunk-VLAN ID (VID) to 30 and 40.
Switch(config-if-23-44)# vlan dot1q-vlan mode trunk native	Set the selected ports to Trunk-native Mode (tagged and untagged).
Switch(config-if-1-4)#exit	Exit current ports interface mode
Switch(config)# interface 45-46	Enter port 45 to port 46's interface mode.
Switch(config-if-45-46)# vlan dot1q-vlan access-vlan 60	Set port 45 to port 46's Access-VLAN ID (PVID) to 60.
Switch(config-if-45-46)# vlan dot1q-vlan mode access	Set the selected ports to Access Mode (untagged).
Switch(config-if-45-46)#exit	Exit current ports interface mode
Switch(config)# interface 47-48	Enter port 47 to port 48's interface mode.
Switch(config-if-47-48)# vlan dot1q-vlan access-vlan 70	Set port 47 to port 48's Access-VLAN ID (PVID) to 70.
Switch(config-if-47-48)# vlan dot1q-vlan mode access	Set the selected ports to Access Mode (untagged).
Switch(config-if-47-48)#exit	Exit current ports interface mode

2. Modify 802.1q VLAN IDs' names.

Switch(config)# vlan dot1q-vlan 10, 20	Enter VLAN 10,20

Switch(config-vlan-10,20)# name Sales	Enater name for VLAN 10 and 20
Switch(config-vlan-10,20)# exit	Exit VLAN 10 and 20
Switch(config)# vlan dot1q-vlan 30,40,50	Enter VLAN 30,40 and 50
Switch(config-vlan-30,40,50)# name RD	Enater name for VLAN 30,40 and 50
Switch(config-vlan-30,40,50)# exit	Exit VLAN 30,40 and 50
Switch(config)# vlan dot1q-vlan 60	Enter VLAN 60
Switch(config-vlan-60)# name SQA	Enater name for VLAN 60
Switch(config-vlan-60)# exit	Exit VLAN 60
Switch(config)# vlan dot1q-vlan 70	Enter VLAN 70
Switch(config-vlan-70)# name PME	Enater name for VLAN 70
Switch(config-vlan-70)# exit	Exit VLAN 70

2.6.24 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 2-15 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		Set auto-negotiation setting to the default setting.

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, not more than 8 ports can be aggregated.**
Switch(config-if-PORT-PORT)# channel-group lacp key [0-255]	[0-255]	Configure LACP key, 0-255.

Switch(config-if-PORT-PORT)# channel-group lacp role		Specify LACP role as passive.
Switch(config-if-PORT-PORT)# channel-group lacp role active		Specify LACP role as active.
Switch(config-if-PORT-PORT)# channel-group trunking [group_name]	[group_name]	Specify ports to the trunking group. **Note1 : At lease 2 ports, 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 2.6.5 "channel-group")**
No command		
Switch(config-if-PORT-PORT)# no channel-group lacp		Diable LACP
Switch(config-if-PORT-PORT)# channel-group trunking		Disable port-trunking

4. Set up port description.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# description [description]	[description]	Type in the description for the port(s), max 35 characters.
No command		
Switch(config-if-PORT-PORT)# no description		Clear port description.

5. Set up port duplex mode.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# duplex [full]	[full]	Configure port duplex to **full.**
No command		
Switch(config-if-PORT-PORT)# no duplex		Configure port duplex to **half.** **Note1 : Only 45-48 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 port(s).
No command		

Switch(config-if-PORT-PORT)# no flowcontrol		Disable flow control on port(s).

7. **Set up port DHCP and IGMP parameters.**

Setup DHCP snooping/relay sub-commands

Command	Parameter	Description
Switch(config-if-PORT-PORT)# ip dhcp snooping option		Enable DHCP option 82 on port(s).
Switch(config-if-PORT-PORT)# ip dhcp snooping trust		Configure port(s) as DHCP option 82 trust port(s)
Switch(config-if-PORT-PORT)# ip dhcp snooping server-trust		Configure port(s) as DHCP server trust port(s) **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 DHCP option 82 on port(s).
Switch(config-if-PORT-PORT)# no ip dhcp snooping trust		Unconfigure port(s) as DHCP option 82 trust port(s)
Switch(config-if-PORT-PORT)# no ip dhcp snooping server-trust		Unconfigure port(s) as DHCP server trust port(s)

Setup IGMP snooping/MLD sub-commands

Command	Parameter	Description
Switch(config-if-PORT-PORT)# ip igmp filter		Enable IGMP filter
Switch(config-if-PORT-PORT)# ip igmp filter profile [profile_name]	[profile_name]	Specify an IGMP filter profile **Note : Need to create an IGMP filter profile first at Switch Management-->IGMP Snooping-->IPMC profile.**
Switch(config-if-PORT-PORT)# ip igmp max-groups [1-512]	[1-512]	Specify the max IGMP group number.
Switch(config-if-PORT-PORT)# ip igmp static-multicast-ip [E.F.G.H] vlan [1-4094]	[E.F.G.H]	Specify static multicast address.
	[1-4094]	Specify VLAN ID.
No command		
Switch(config-if-PORT-PORT)# no ip igmp filter		Disable IGMP filter
Switch(config-if-PORT-PORT)# no ip igmp filter profile [profile_name]	[profile_name]	Un-specify an IGMP filter profile
Switch(config-if-PORT-PORT)# no ip igmp max-groups		Un-specify the max IGMP groups number.

Switch(config-if-PORT-PORT)# no ip igmp static-multicast-ip [E.F.G.H] vlan [1-4094]		Un-specify static multicast address and VLAN ID.

Setup IP source guard

Command	Parameter	Description
Switch(config-if-PORT-PORT)# ip sourceguard [dhcp|fixed-ip]	[dhcp|fixed-ip]	Configure IP sourceguard setting as either DHCP or fixed-IP.
Switch(config-if-PORT-PORT)# ip sourceguard static-ip [A.B.C.D] mask [255.x.x.x] vlan [1-4094]	[A.B.C.D]	Specify static IP address.
	[255.x.x.x]	Configure subnet mask.
	[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 to default (unlimited).

8. Enable loop-detection per port.

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

9. 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 static MAC address
	[1-4094]	Specify VLAN ID
Switch(config-if-PORT-PORT)# mac learning		Enable MAC address learning
No command		
Switch(config-if-PORT-PORT)# no mac address-table static-mac [xx:xx:xx:xx:xx:xx] vlan [1-4094]	[xx:xx:xx:xx:xx:xx:]	Delete static MAC address entry
	[1-4094]	
Switch(config-if-PORT-PORT)# no mac learning		Disable MAC address learning

10. Configure media type.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# media-type [sfp]	[sfp]	Configure the media type of the port(s) as SFP.
No command		
Switch(config-if-PORT-PORT)# no media-type		Configure the media type of the port(s) as copper. **Note : Only port 45-48 can be configured as copper.**

11. Configure QoS rate limit.

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

12. Shutdown interface.

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

13. Configure RSTP parameters per port.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# spanning-tree		Enable spanning-tree protocol
Switch(config-if-PORT-PORT)# spanning-tree cost [0-200000000]	[0-200000000]	Specify port path cost
Switch(config-if-PORT-PORT)# spanning-tree priority [0-15]	[0-15]	Specify bridge priority **0=0, 1=4096, 2=8192, 3=12288, 4=16384 5=20480, 6=24576, 7=28672, 8=32768 9=36864, 10=40960, 11=45056,12=49152 13=53248, 14=57344,**

		15=61440
Switch(config-if-PORT-PORT)# spanning-tree edge		Specify the port as edge port so to enable it to move directly to forwarding state upon link-up.
Switch(config-if-PORT-PORT)# spanning-tree p2p [forced_true|forced_false|auto]	[forced_true|forced_false|auto]	Specify the port as point to point port and its mode.
No command		
Switch(config-if-PORT-PORT)# no spanning-tree		Disable spanning-tree protocol.
Switch(config-if-PORT-PORT)# no spanning-tree cost		Undo specify port path cost.
Switch(config-if-PORT-PORT)# spanning-tree priority		Undo specify bridge priority.
Switch(config-if-PORT-PORT)# no spanning-tree edge		Undo specify the port as edge port.
Switch(config-if-PORT-PORT)# no spanning-tree p2p		Undo specify the port as point to point port.

14. 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 can not be configured as 10Mbps.**
No command		
Switch(config-if-PORT-PORT)# no speed		Undo port speed setting.

15. Set up VLAN parameters per port.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Configure port PVID.
Switch(config-if-PORT-PORT)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Configure port VID.
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode access		Configure port as dot-1q access port.
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk		Configure port as dot-1q trunk port.

Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk native		Configure port as dot-1q trunk native port.
Switch(config-if-PORT-PORT)# vlan port-based [name]	[name]	Join port to specific port-based VLAN group. **Note : Need to create a port-based VLAN group first at Switch Management-->VLAN Configuration-->Port Based VLAN-->Configure VLAN.**
No command		
Switch(config-if-PORT-PORT)# vlan dot1q-vlan access-vlan		Undo configure port PVID.
Switch(config-if-PORT-PORT)# vlan dot1q-vlan trunk-vlan		Undo configure port VID.
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode		Undo VLAN mode configuration.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan mode trunk native		Undo VLAN trunk native mode configuration.
Switch(config-if-PORT-PORT)# no vlan port-based [name]	[name]	Undo join port to specific port-based VLAN group.

2.6.25 Show interface statistics Command

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

Command	Parameters	Description
Switch(config)# show interface		Show 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.
Switch(config)# show interface statistics clear [port_list]	[port_list]	Clear statistics 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.

2.6.26 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 temperature, voltage, TX Bias, TX power, and RX power.
Switch(config)# show sfp state	Show the slide-in SFP modules' current temperature, safety Bias power, TX power, RX power and voltage.

2.6.27 Show running-config & start-up-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.

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. Use the RS-232 RJ-45 console port or use a RJ45 LAN cable and any of the 10/100/1000Base-T RJ-45 ports of the Managed Switch (as the temporary RJ-45 Management console port) to login to the Managed Switch and set up the IP address for the first time. (The default IP of the Managed Switch can be reached at **"http://192.168.0.1"**. You can change the Managed Switch's IP to the needed one later in its **Network Management** menu.)

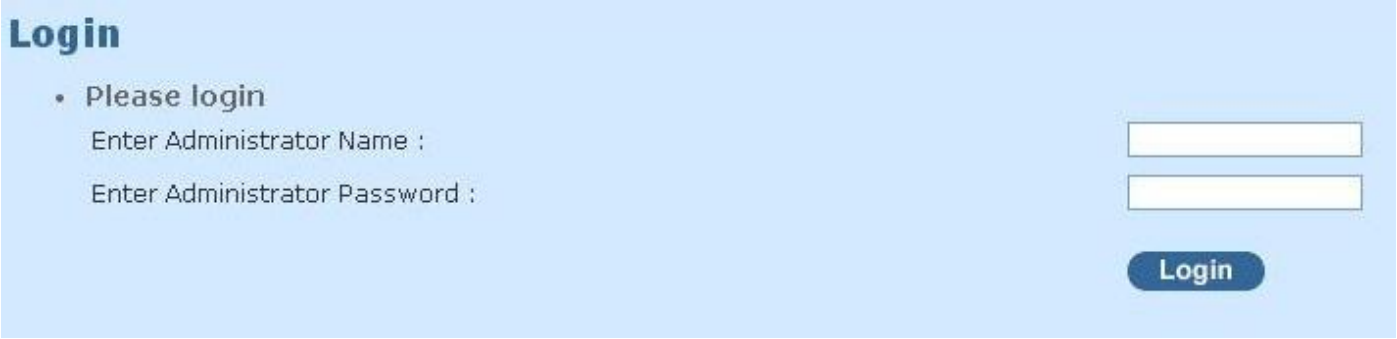
Follow these steps to manage the Managed Switch through a Web browser:

Use the RS-232 RJ-45 console port or one of the 10/100/1000Base-TX RJ-45 ports (as the temporary RJ-45 Management console port) to set up the assigned IP parameters of the Managed Switch, including IP address, Subnet Mask, and Default Gateway of the Managed Switch (if required)

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

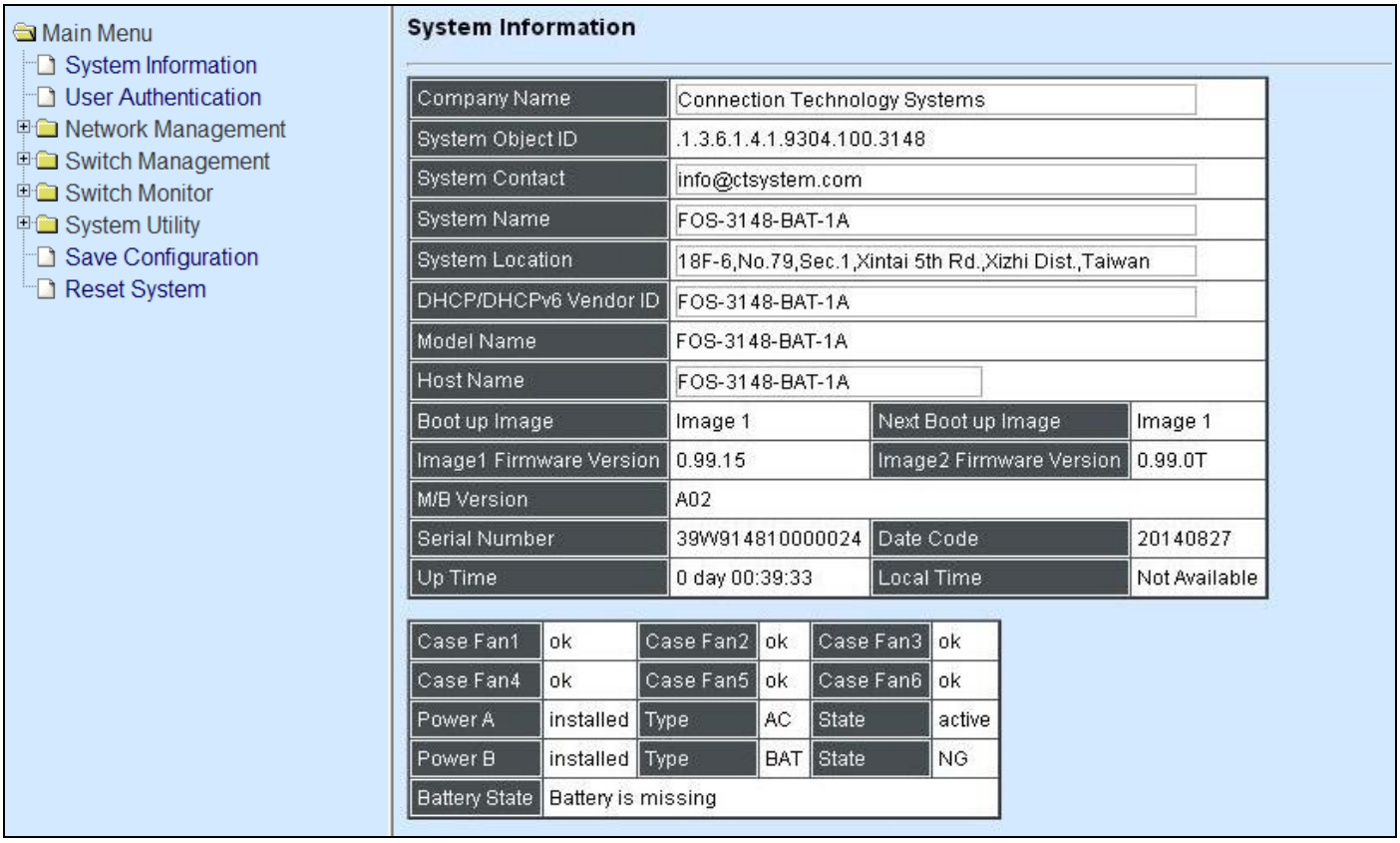
Login to the Managed Switch to reach the Main Menu.

Once you gain the access, a Login window appears like this:



Enter the default username (admin) and password (by default, no password is required) to login to the main screen page.

After a successful login, the Main Menu screen shows up. The rest of the menu functions in the Web Management are similar to those described at the Console Management and are also described below.



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

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

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

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

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

6. **System Utility:** Ping, Firmware Upgrade, Load Factory Settings, etc..

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

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

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

4.1 System Information

Select **System Information** from the **Main Menu** and then the following screen shows up.

System Information

Company Name	Connection Technology Systems		
System Object ID	.1.3.6.1.4.1.9304.100.3148		
System Contact	info@ctsystem.com		
System Name	FOS-3148-BAT-1A		
System Location	18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan		
DHCP/DHCPv6 Vendor ID	FOS-3148-BAT-1A		
Model Name	FOS-3148-BAT-1A		
Host Name	FOS-3148-BAT-1A		
Boot up Image	Image 1	Next Boot up Image	Image 1
Image1 Firmware Version	0.99.15	Image2 Firmware Version	0.99.0T
M/B Version	A02		
Serial Number	39W914810000024	Date Code	20140827
Up Time	0 day 00:39:33	Local Time	Not Available

Case Fan1	ok	Case Fan2	ok	Case Fan3	ok
Case Fan4	ok	Case Fan5	ok	Case Fan6	ok
Power A	installed	Type	AC	State	active
Power B	installed	Type	BAT	State	NG
Battery State	Battery is missing				

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 contact information for this Managed Switch. Use “switch-info sys-contact [sys-contact]” command to edit this field.

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

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

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

Model Name: Display the product’s model name.

Host Name: Display the product’s host name.

Image1 Firmware Version: Display the firmware version 1 (image-1) used in this device.

Image2 Firmware Version2: 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 Managed Switch Firmware date code.

Up Time: Display the up time since last restarting.

Local Time: Display local time.

Case Fan (1-6): Display the status of case fans.

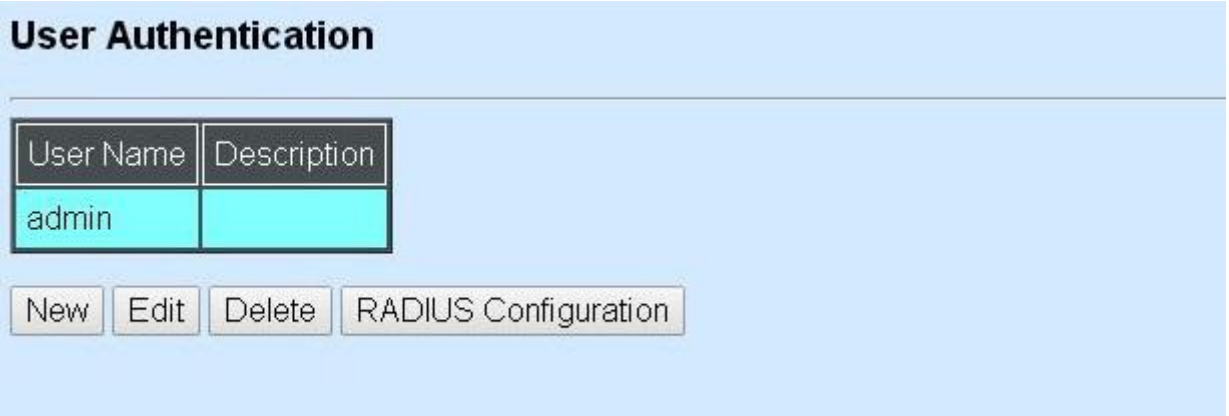
Power (A-B): Display the status of powers.

Battery State: Display the status of battery (For BAT version only).

4.2 User Authentication

To prevent any unauthorized operations, only registered users are allowed to operate the Managed Switch. Users who want to operate the Managed Switch need to register into the user list first.

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



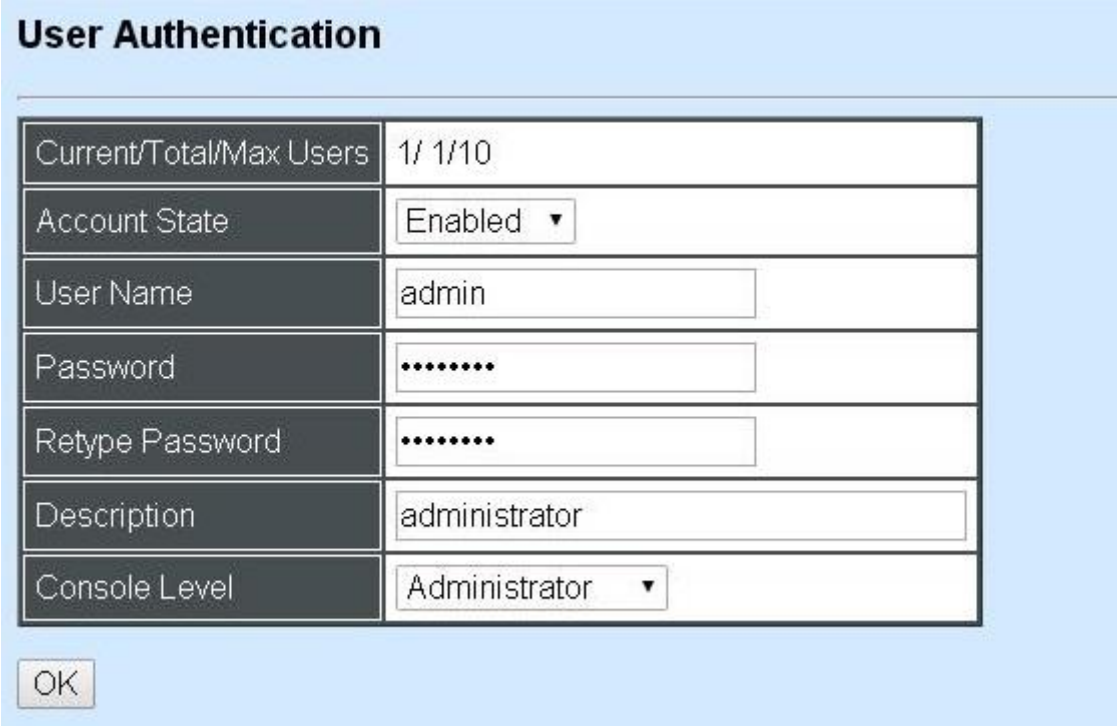
Up to 10 Users can be registered.

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

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

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

Click **RADIUS Configuration** for authentication setting via RADIUS.



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

Current: This shows the number of current registered users.

Total: This shows the total number of 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.

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

Retype Password: Enter the password again for double-checking.

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

Console Level: Select the desired privilege for the console operation from the pull-down menu. Four operation privileges are available in the Managed Switch:

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

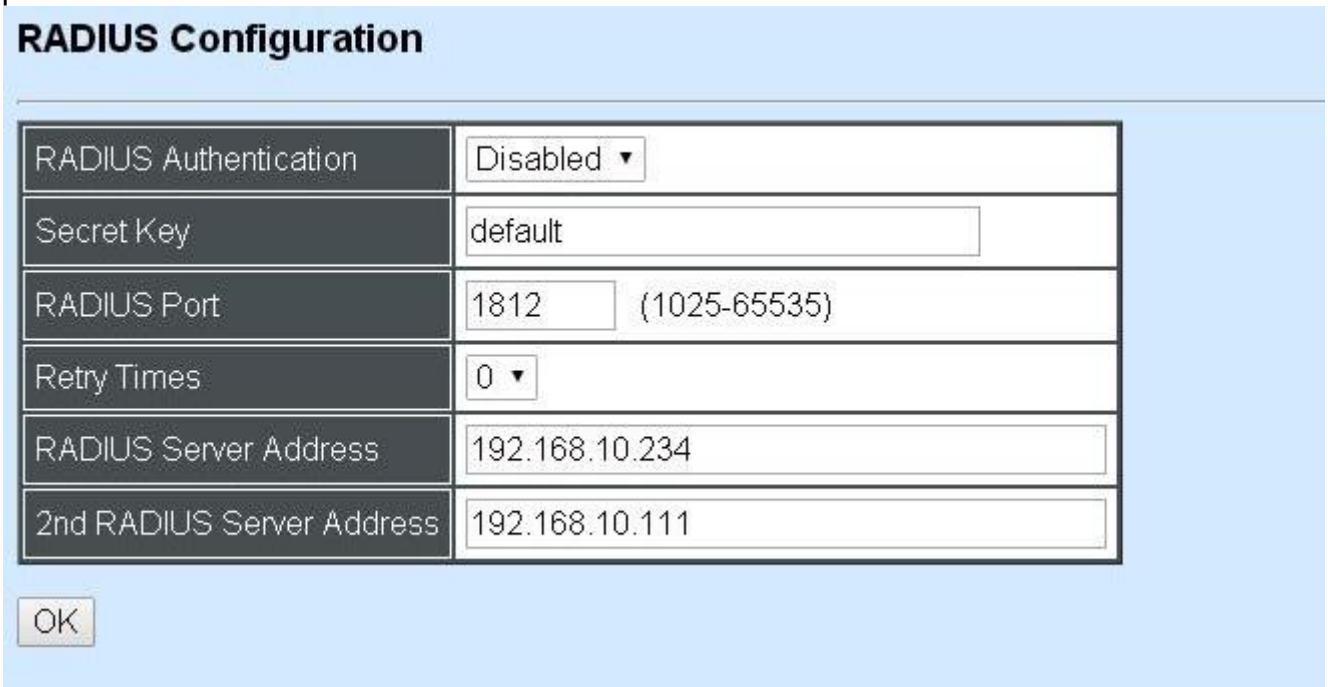
Read & Write: Partial access right, unable to modify user account, system information and items under System Utility menu.

Read Only: Read-Only access priviledge.

NOTE: *To prevent incautious operations, users cannot delete their own account, modify their own user name and change their own account state.*

4.2.1 RADIUS Configuration

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



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

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

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

RADIUS Port: The RADIUS service port on RADIUS server.

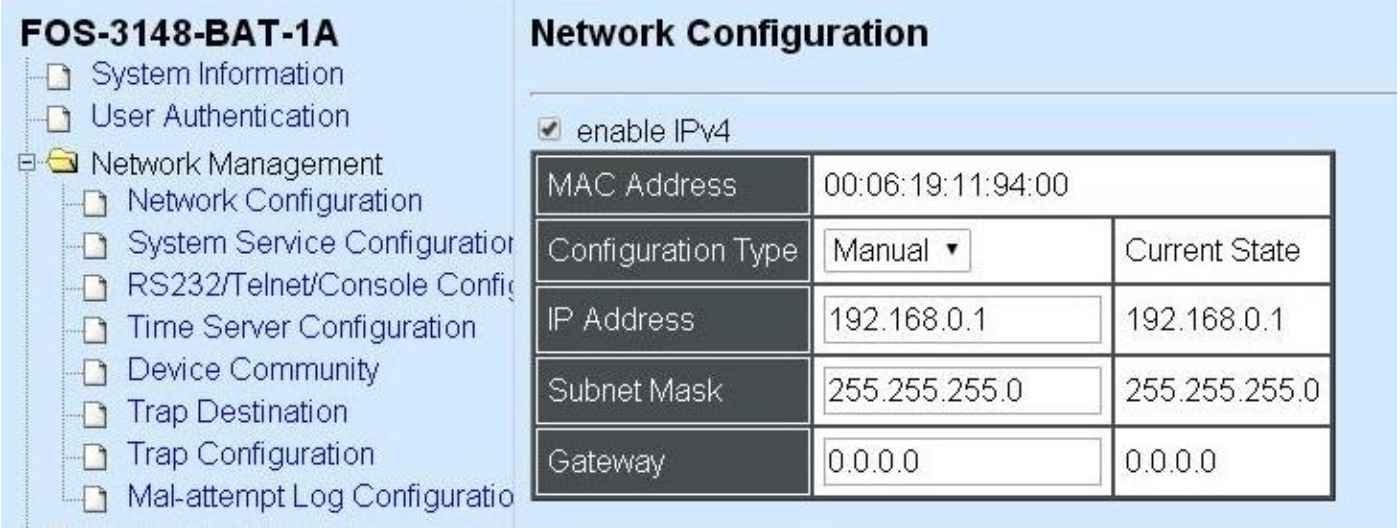
Retry Time: Times of trying to reconnect if the RADISU server is not reachable.

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

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

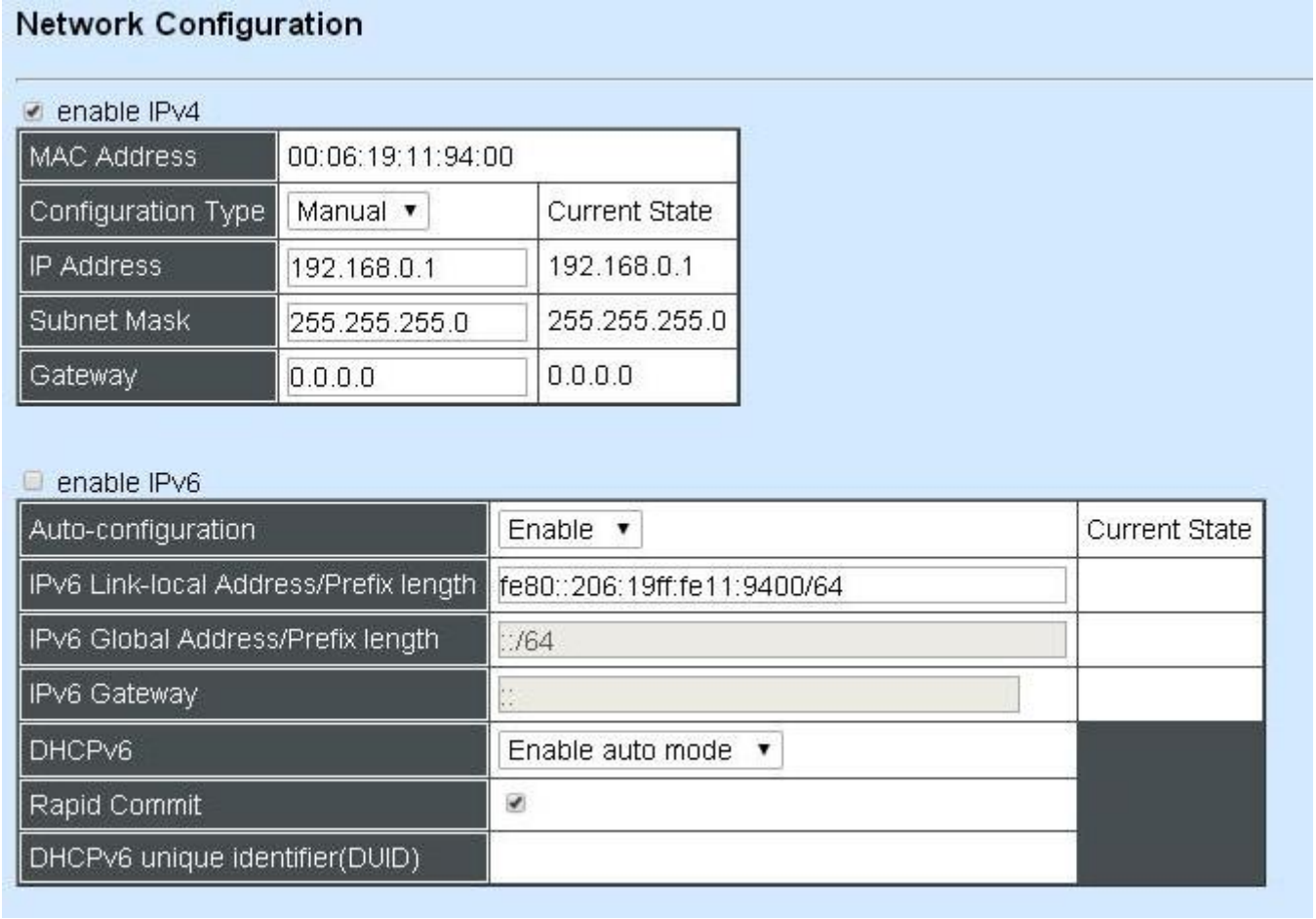
6. **Trap Destination:** View the registered SNMP trap destination list. Add a new trap destination or remove an existing trap destination.

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

8. **Mal-attempt Log 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: Check to enable IPv4 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: Check to enable IPv6 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.

IP Source Binding:

Source Binding state	Disabled ▼	
Index	State	IP/IPv6 Address
1	Disabled ▼	0.0.0.0
2	Disabled ▼	0.0.0.0
3	Disabled ▼	0.0.0.0
4	Disabled ▼	0.0.0.0
5	Disabled ▼	0.0.0.0
6	Disabled ▼	0.0.0.0
7	Disabled ▼	0.0.0.0
8	Disabled ▼	0.0.0.0
9	Disabled ▼	0.0.0.0
10	Disabled ▼	0.0.0.0
11	Disabled ▼	0.0.0.0
12	Disabled ▼	0.0.0.0

OK

Source Binding state: Enable or disable IP source binding.

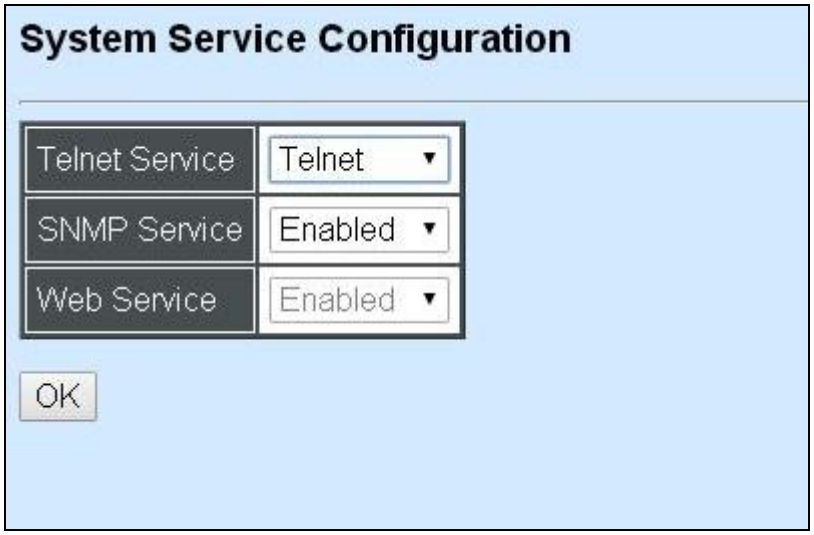
State: Disable or enable

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.



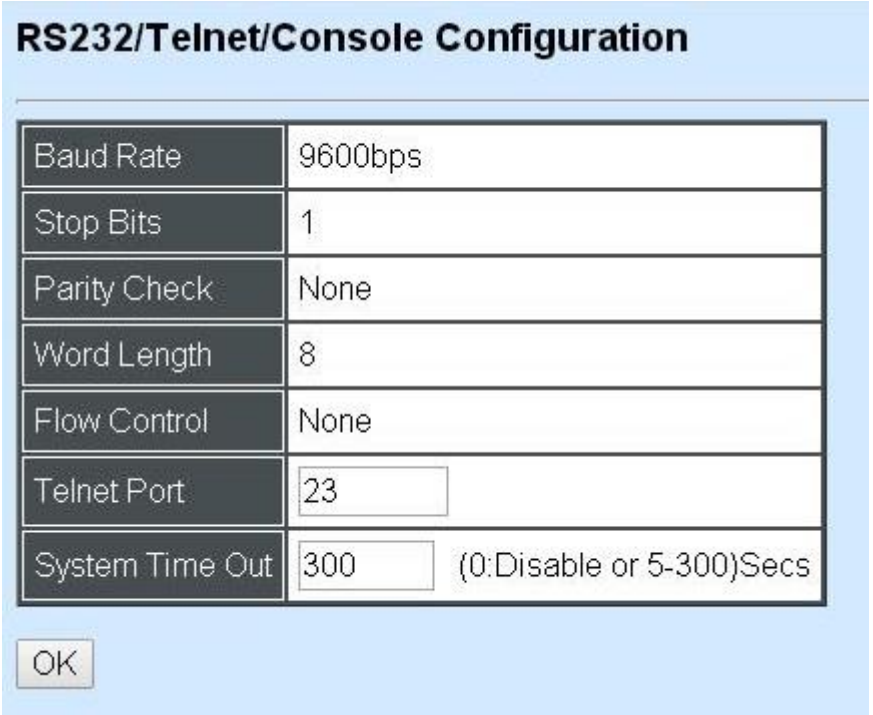
Telnet Service: To enable or disable the Telnet Management service.

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

Web Service: To enable or Disable the Web 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. Specifying “0” means an inactive connection will never be disconnected.

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 time synchronization.

Time Server IP/IPv6 Address: NTP time server address.

2nd Time Server IP/IPv6 Address: When the default time server is down, the Managed Switch will automatically connect to the 2nd time server.

Synchronization Interval: The time interval to synchronize from NTP time server.

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

Daylight Saving Time: 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.

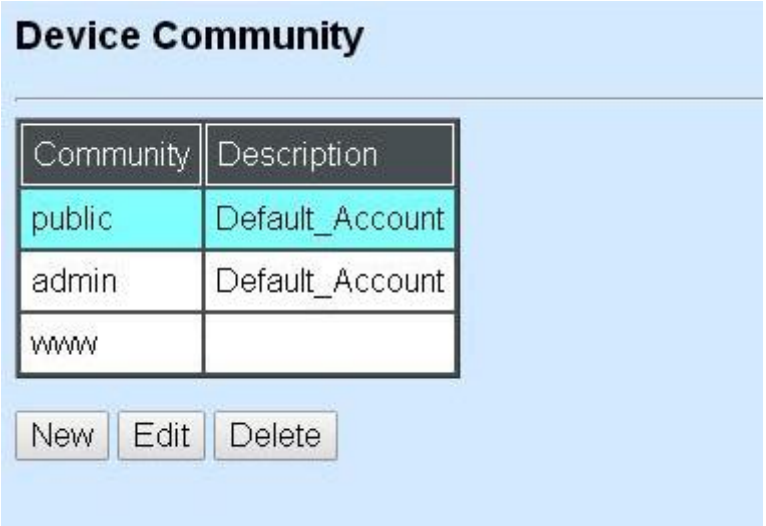
Daylight Saving Time Date Start: Click the pull-down menu to select the start date of daylight saving time.

Daylight Saving Time Date End: Click the pull-down menu to select the 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.



Up to 10 Device Communities can be set up.

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

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

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

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

Current: This shows the number of currently registered communities.

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

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

Account State: 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. 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 Trap Destination

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

Trap Destination

Index	State	Destination	Community
1	Enabled	0.0.0.0	
2	Disabled	0.0.0.0	
3	Disabled	0.0.0.0	
4	Disabled	0.0.0.0	
5	Disabled	0.0.0.0	
6	Disabled	0.0.0.0	
7	Disabled	0.0.0.0	
8	Disabled	0.0.0.0	
9	Disabled	0.0.0.0	
10	Disabled	0.0.0.0	

OK

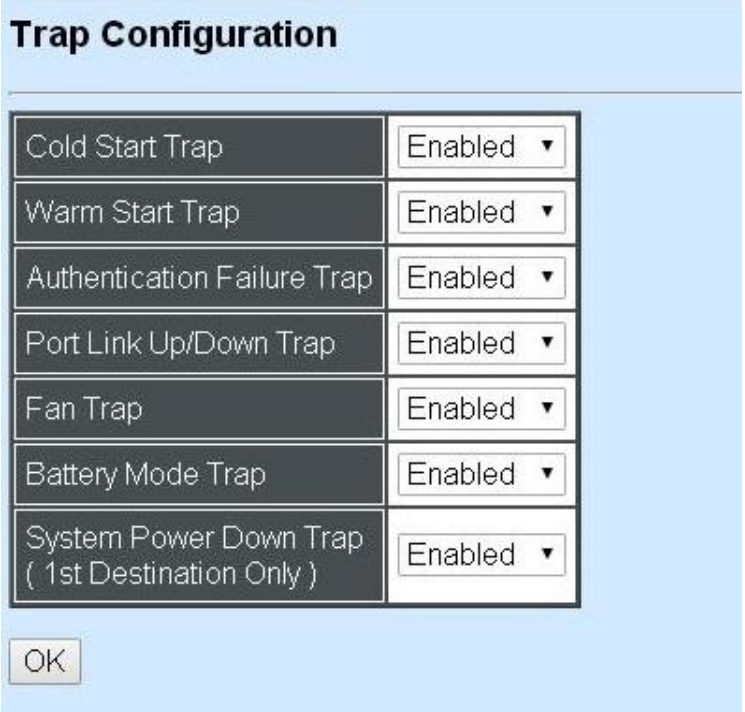
State: Enable or disable the function of sending trap to the specified destination.

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

Community: Enter the community name of the network management system.

4.3.7 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.

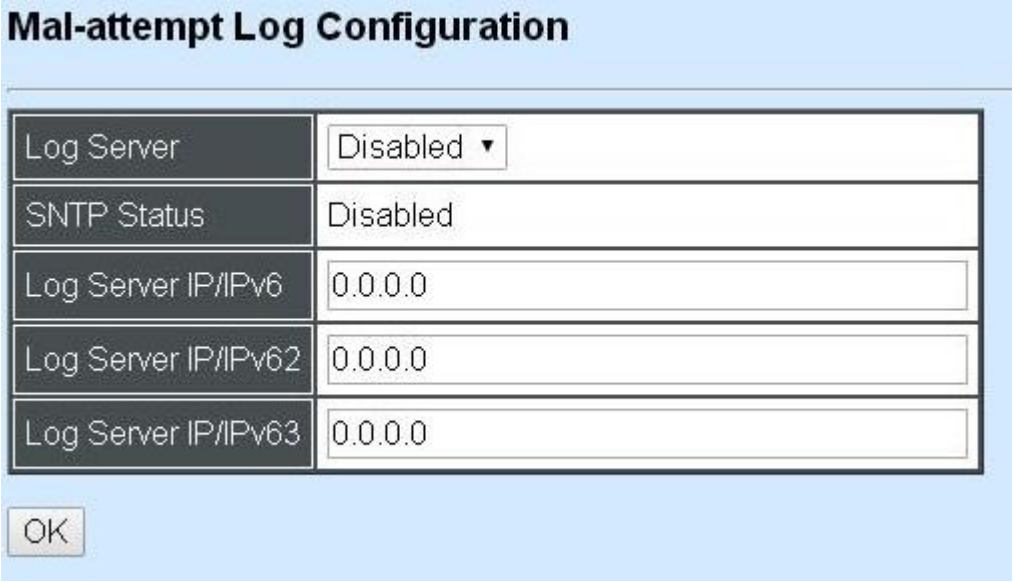
Fan Trap: Enable or disable the Managed Switch to send a trap when the fan is not working or fails.

Battery Mode Trap: Enable or disable the Managed Switch to send a trap when the battery is not working or fails.

System Power Down Trap (1st Destination Only): Send a trap notice while the Managed Switch is power down.

4.3.8 Mal-attempt Log Configuration

Click the option **Trap 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.

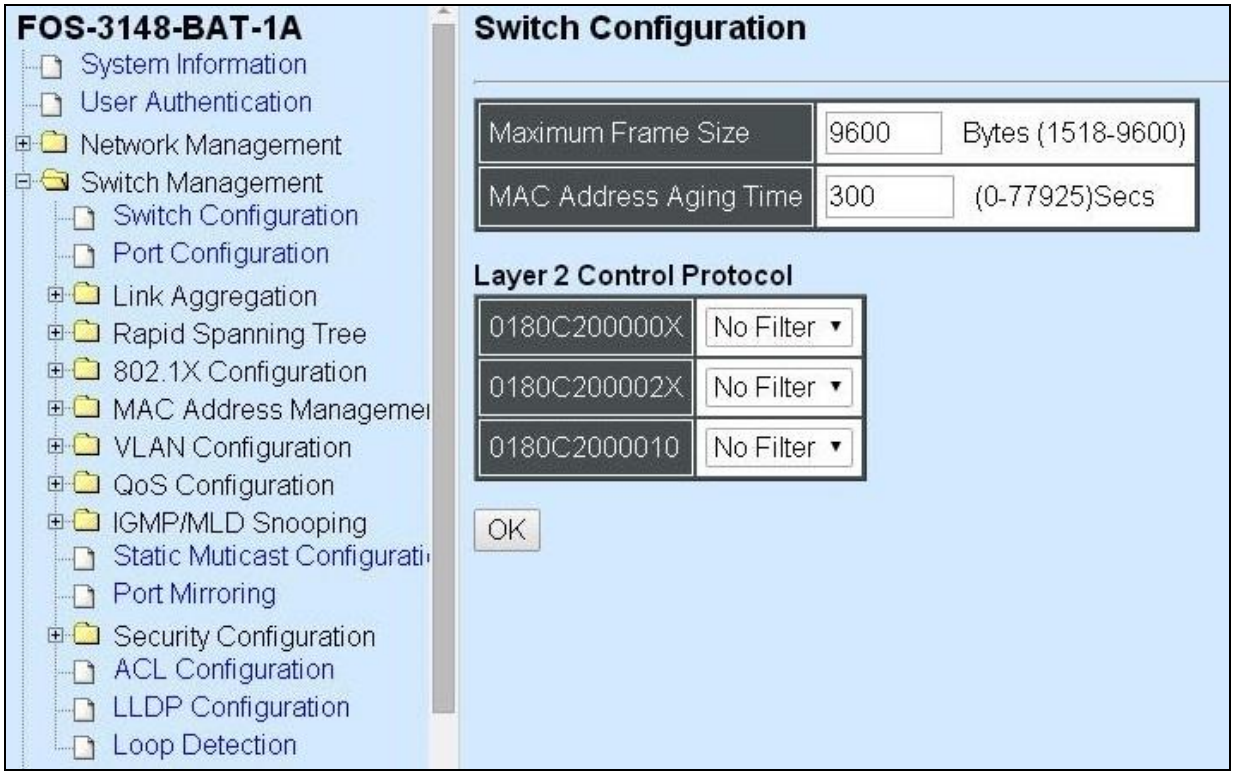
Log Server IP/IPv6: Specify the default Log server IP/IPv6 address.

Log Server IP/IPv62: Specify the second 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 IPv63: 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.

4.4 Switch Management

In order to manage the Managed switch and set up required switching functions, click the folder icon **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 Configuration:** Set up the 802.1X 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.

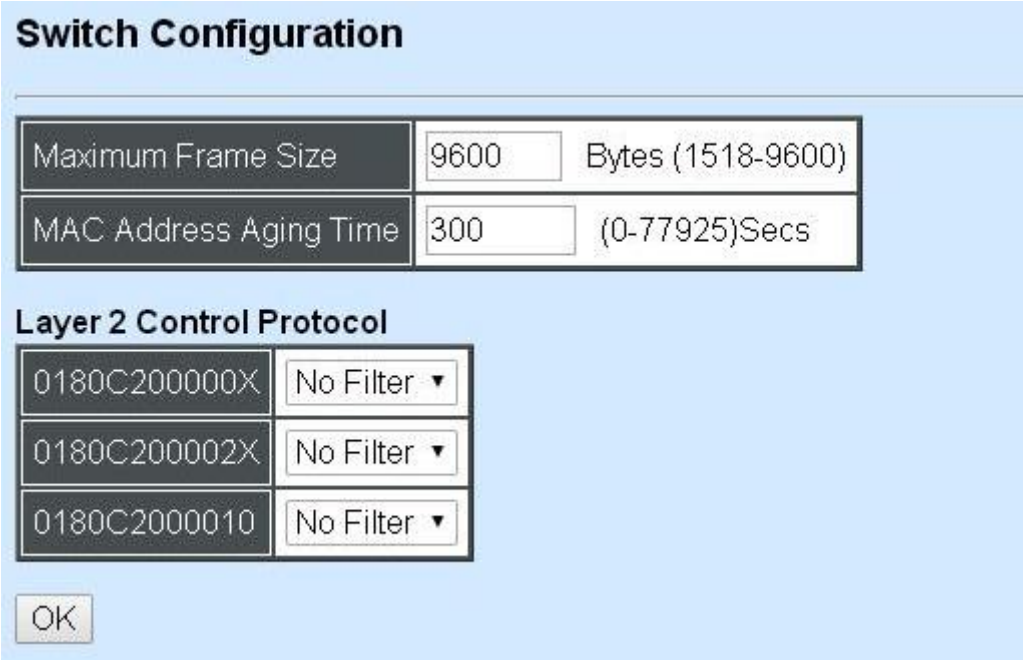
13. **Access Control List Management:** Set up access control entries and lists.

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.

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 77925 seconds. “0” means that MAC addresses will never age out.

Layer 2 Control Protocol

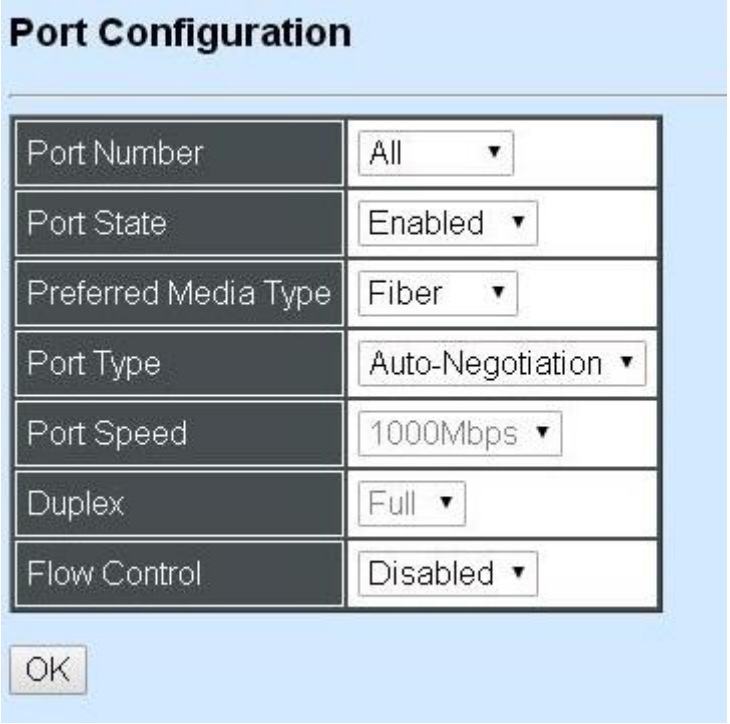
0180C200000X: Select either “Not Filter” or “Filter”. When “Filter” is selected, packets from the address ranging from 0180C2000000 to 0180C200000F will be dropped. Multicast MAC addresses from 0180C2000000 to 0180C200000F are reserved for use by 802.1/802.3 protocols. The purpose for each multicast address is described briefly below:

0180C200002X: Select either “Not Filter” or “Filter”. When “Filter” 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 “Not Filter” or “Filter”. 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 port type, you can further specify the transmission speed (10Mbps/100Mbps/1000Mbps) of the port(s).

Duplex: When you select Manual 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.

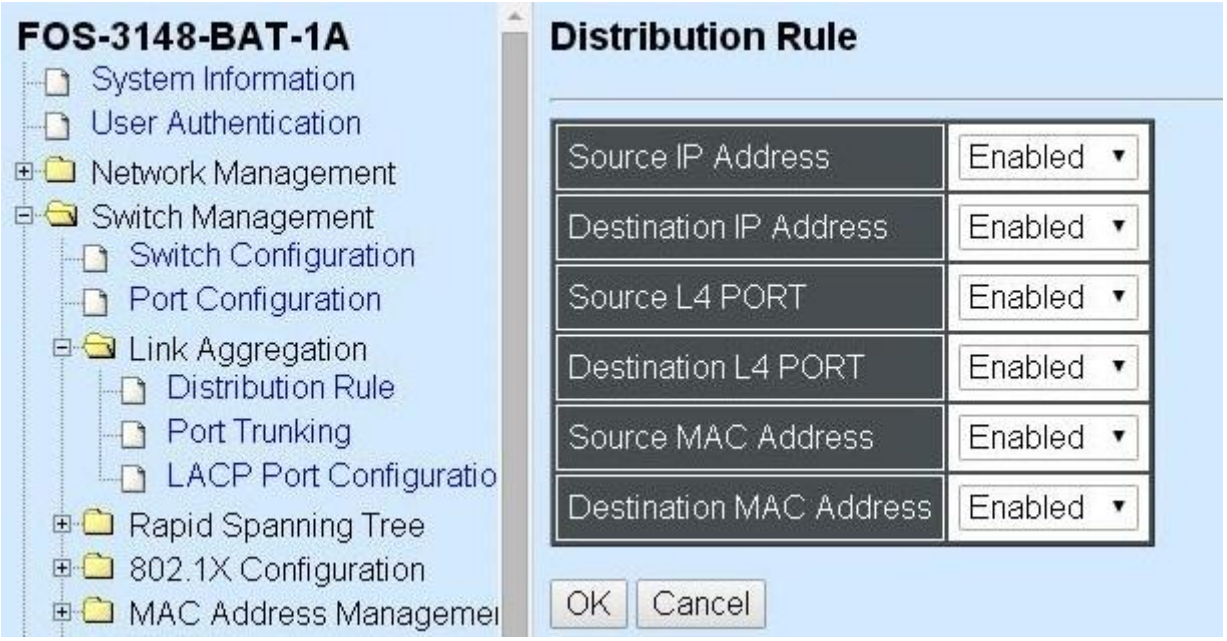
4.4.3 Link Aggregation

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.



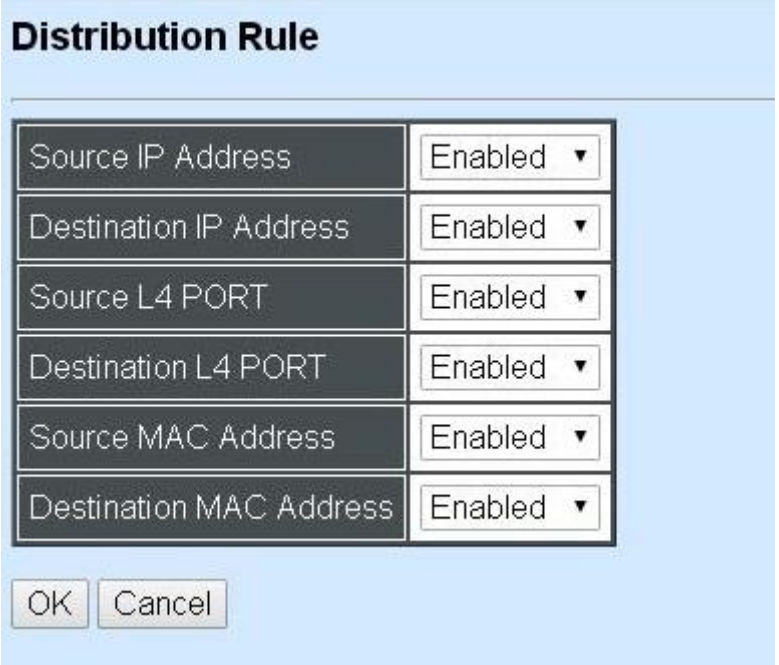
1. **Distribution Rule:** Configure the distribution rule of Port Trunking group(s).

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 fields for you to set up packets according to operations.

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

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

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

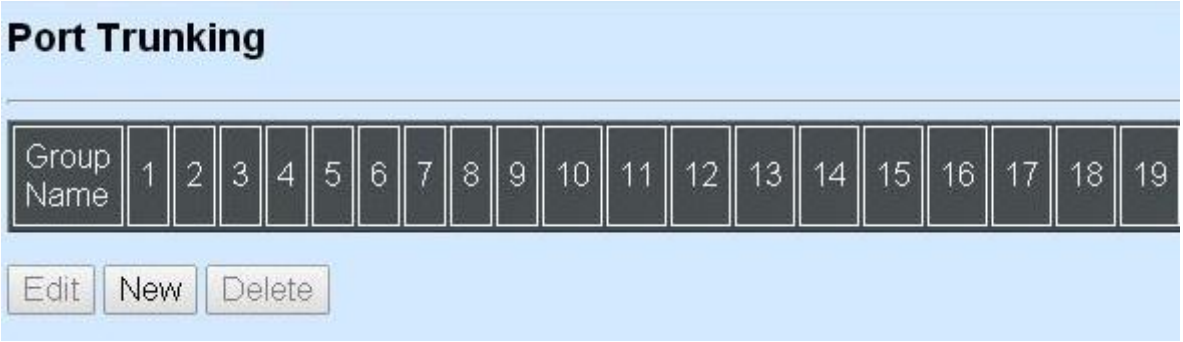
Destination L4 Port: Enable or disable packets according to Destination L4 Port.

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

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

4.4.3.2 Port Trunking

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

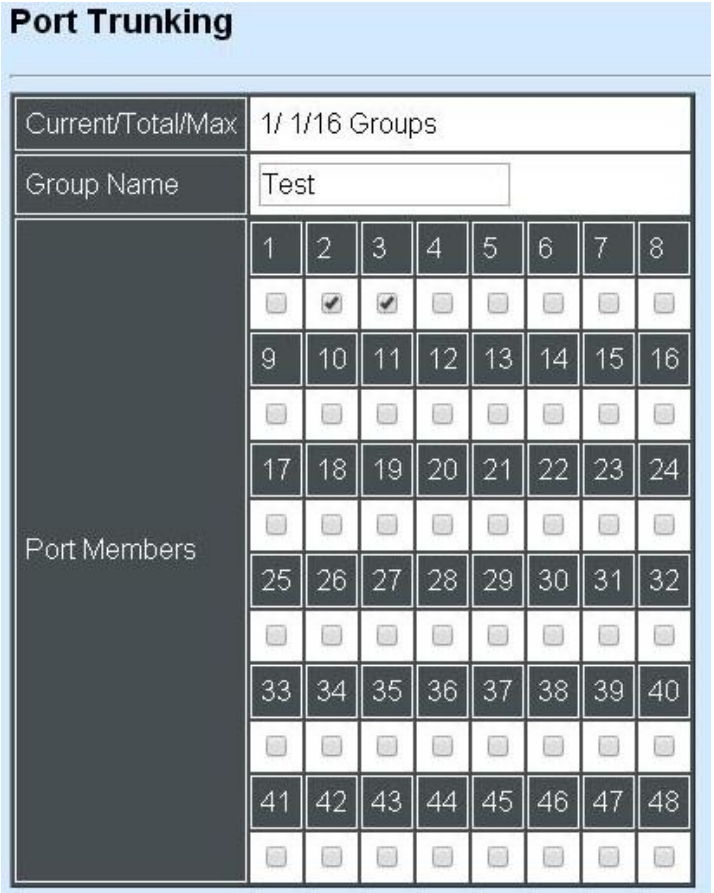


The Managed Switch allows users to create 16 trunking groups. Each group consists of 2 to 16 links (ports).

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

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

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



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

Current: This shows the number of currently registered groups.

Total: This shows the number of total registered groups.

Max: This shows the number of maximum number available for registration. The default maximum number is 16.

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 assign ports to a trunking group.

- Must have 2 to 16 ports in each trunking group.

- Each port can only be grouped in one group.

- If the port is already set On in LACP Port Configuration, it can't be grouped anymore.

Click **OK** and return back 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 can not 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.

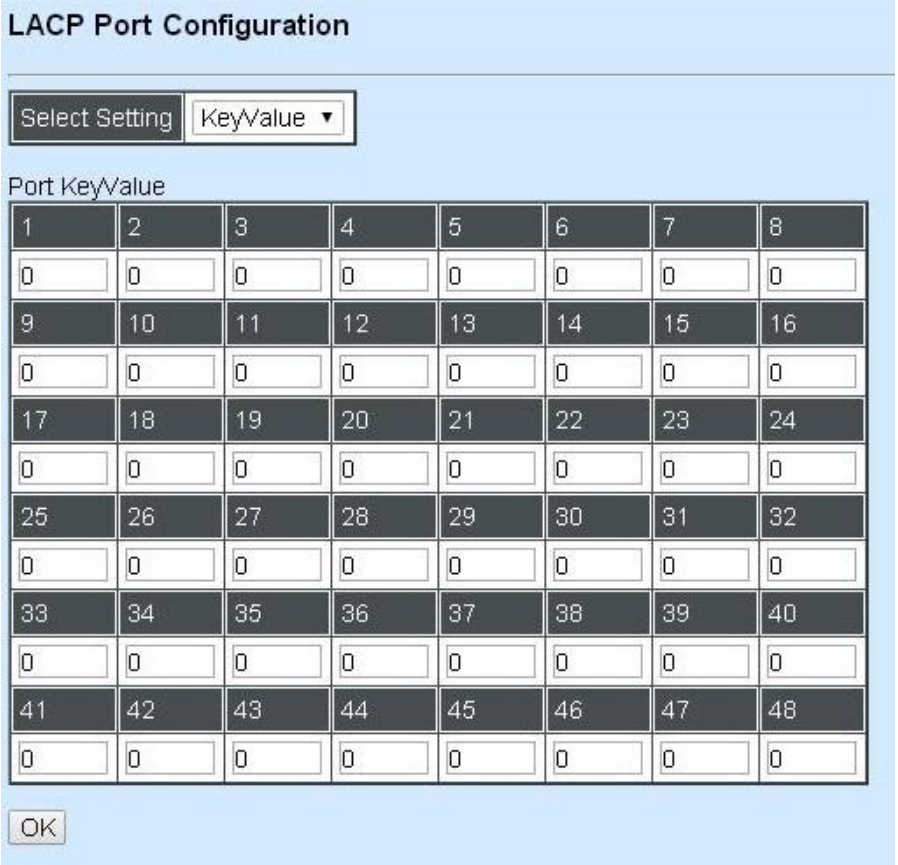
Configure Port Protocol:

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

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

Configure Key Value:

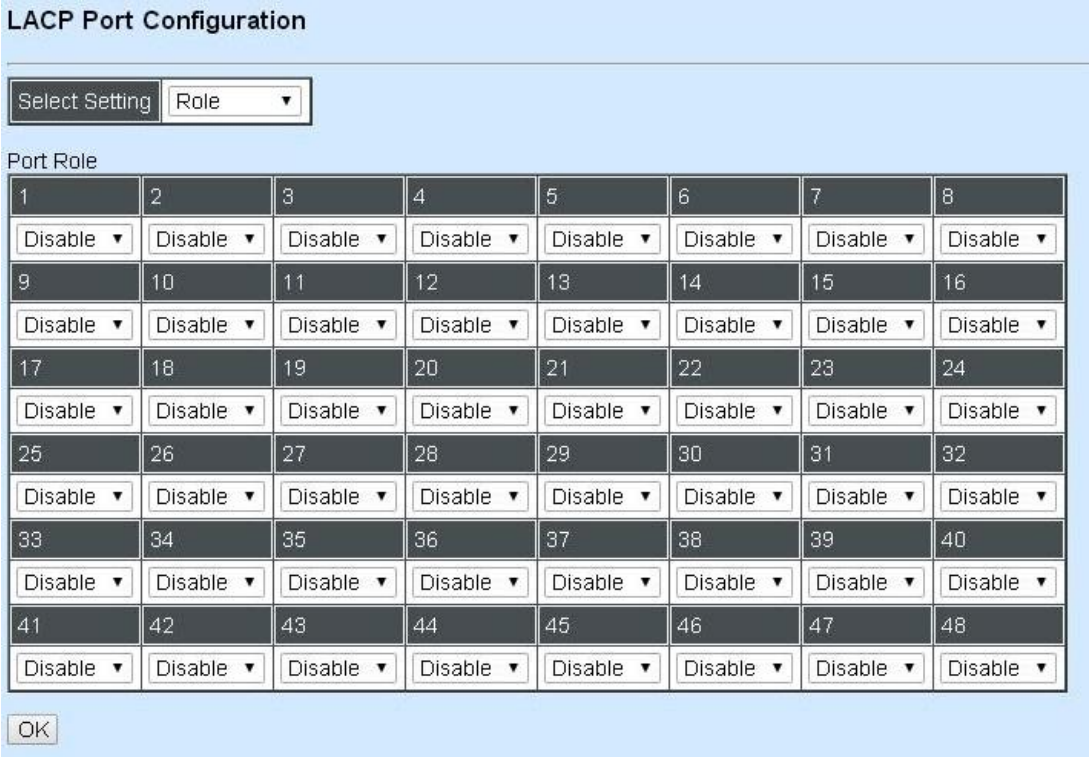
Select “Key Value” from the pull-down menu of Select Setting.



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.



"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.

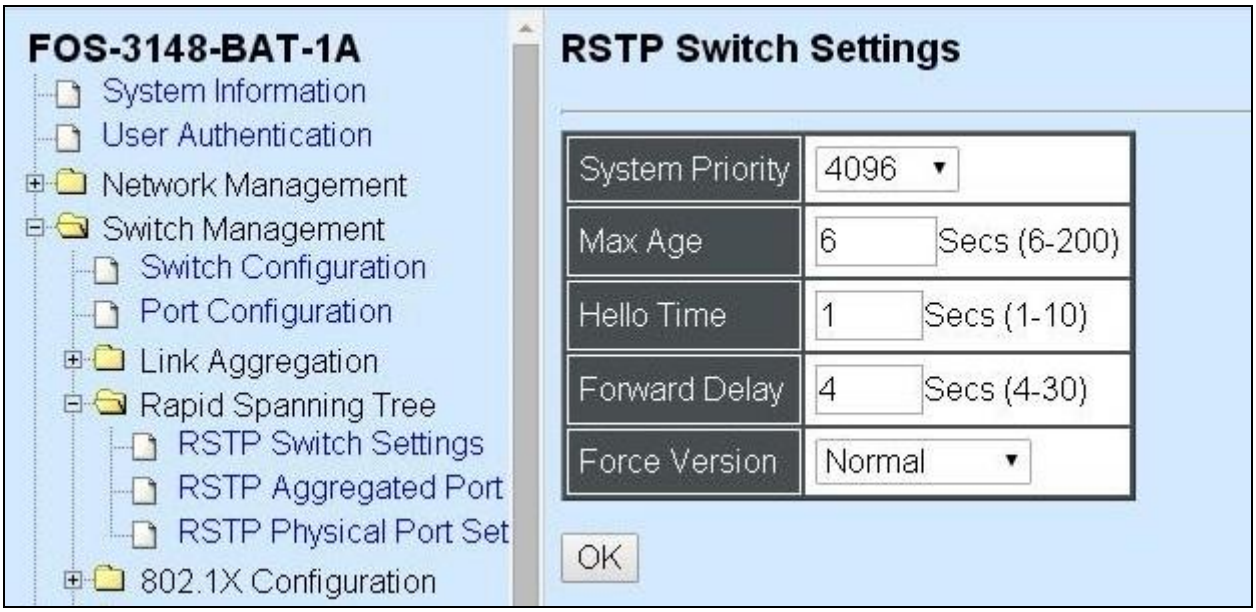
Multiple active paths between network nodes cause a bridge loop. Bridge loops create several problems. First, the MAC address table used by the switch or bridge can fail, since the same MAC addresses (and hence the same network hosts) are seen on multiple ports. Second, a broadcast storm occurs. This 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.



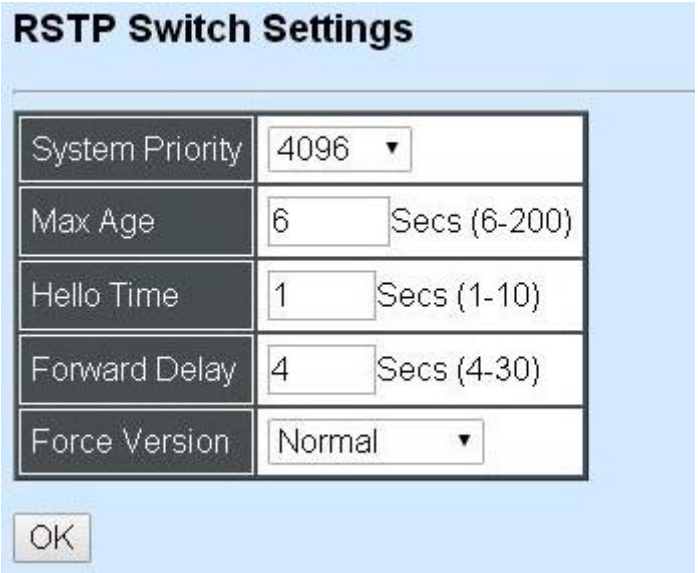
1. **RSTP Switch Settings:** Set up system priority, max Age, hello time, etc.

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

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

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. This timeout is set to 20 seconds.

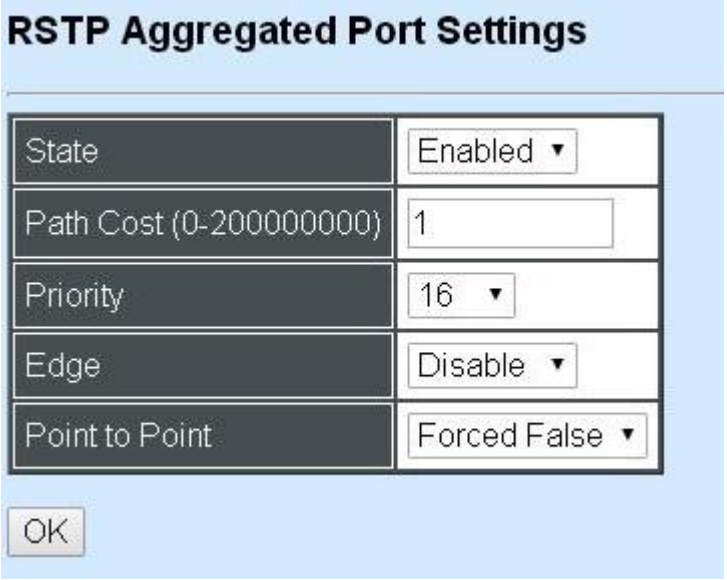
Hello Time: Periodically, a hello packet is sent out by the Root Bridge and the Designated Bridges that are used to communicate information about the topology throughout the entire Bridged Local Area Network.

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

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

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.

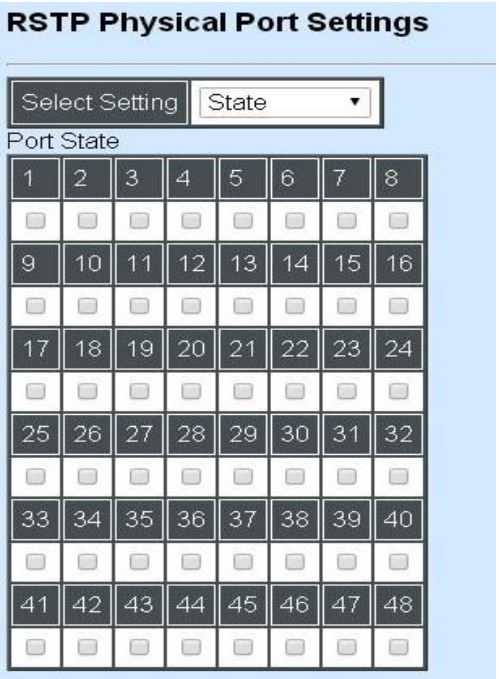
Auto: allows the port to have P2P status whenever possible and operates as if the P2P status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the P2P status changes to operate as if the P2P value were false. The default setting for this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

Configure Port Path Cost:

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

RSTP Physical Port Settings

Select Setting | Path Cost

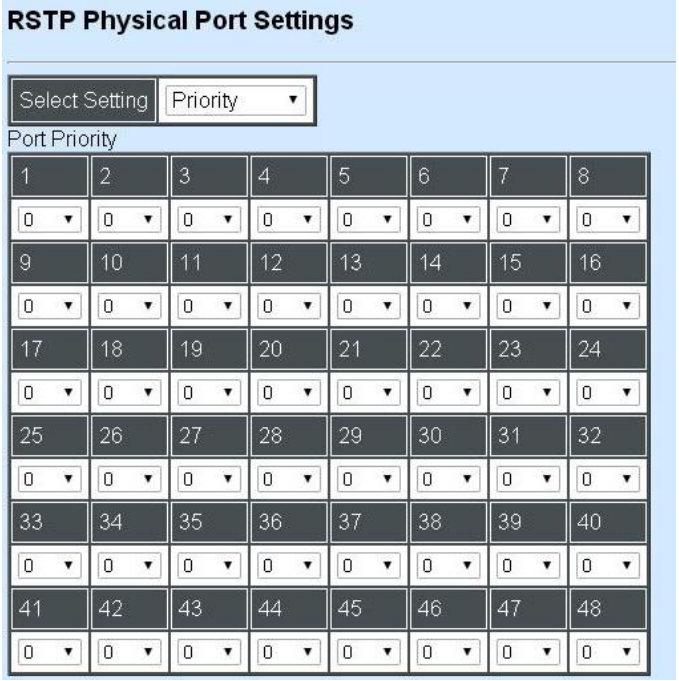
Port Path Cost(0-200000000)

1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0
9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0
17	18	19	20	21	22	23	24
0	0	0	0	0	0	0	0
25	26	27	28	29	30	31	32
0	0	0	0	0	0	0	0
33	34	35	36	37	38	39	40
0	0	0	0	0	0	0	0

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

Configure Port Priority:

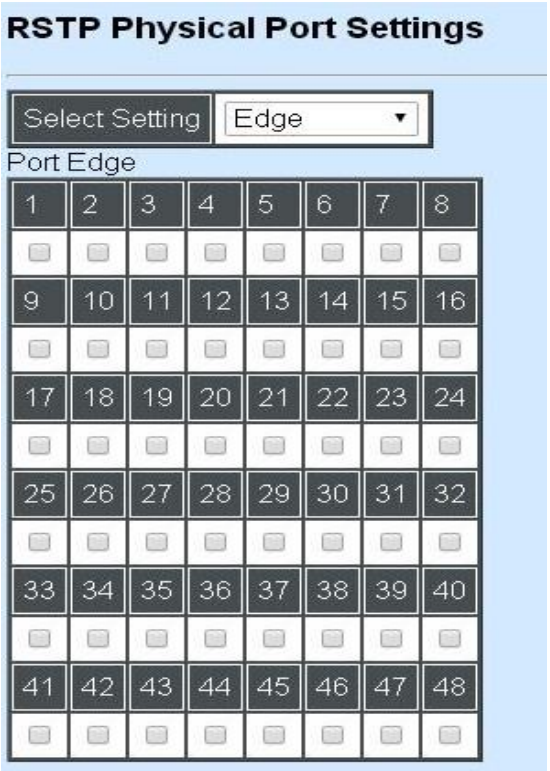
Select “Priority” from the pull-down menu of Select Setting.



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

Configure Port Edge:

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



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

Configure Port Point2point:

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

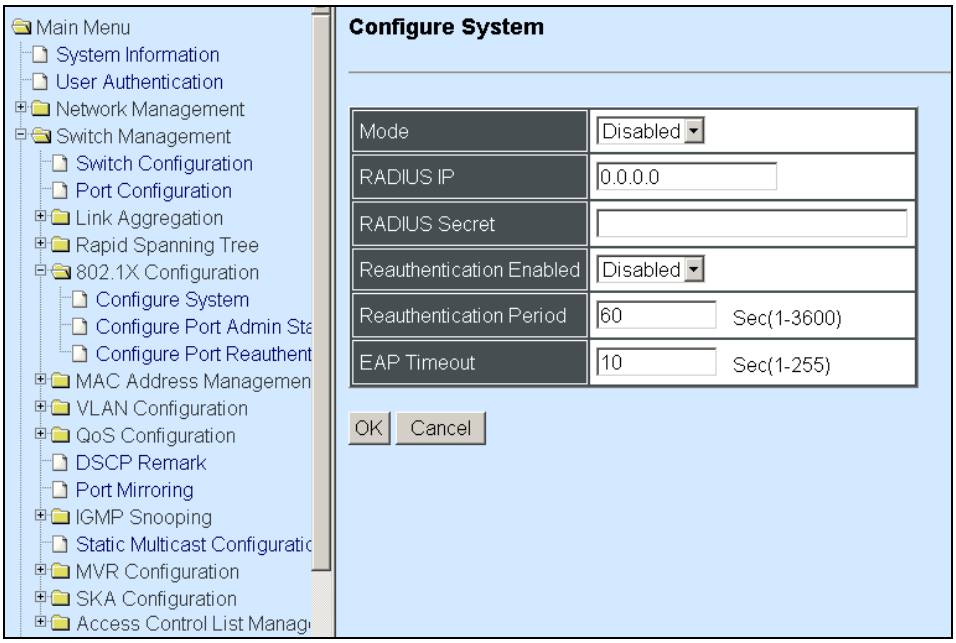
Set up the Point to Point setting. The default setting is “Forced True”.

4.4.5 802.1X Configuration

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

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

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



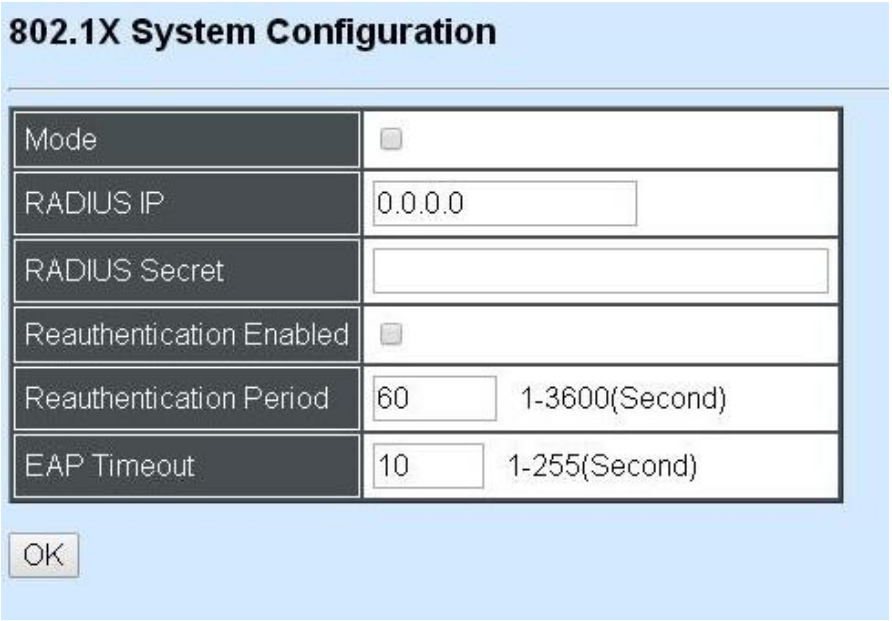
1. **802.1X System Settings:** Set up 802.1X RADIUS IP, RADIUS Secret, Reauthentication, Timeout.

2. **802.1X Port Admin State:** Set up aggregation, Path Cost, Priority, Edge, etc.

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

4.4.5.1 802.1X System Settings

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



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

RADIUS IP: Specify RADIUS Authentication server address.

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

Reauthentication Enabled: Enable or disable Reauthentication.

Reauthentication Period: Specify a period of authentication time that a client authenticates with the authentication server.

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

4.4.5.2 802.1X Port Admin State

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

802.1X Port Admin State

1	2	3	4	5	6	7
Authorized	Authorized	Authorized	Authorized	Authorized	Authorized	Authorized
9	10	11	12	13	14	15
Authorized	Authorized	Authorized	Authorized	Authorized	Authorized	Authorized
17	18	19	20	21	22	23
Authorized	Authorized	Authorized	Authorized	Authorized	Authorized	Authorized
25	26	27	28	29	30	31
Authorized	Authorized	Authorized	Authorized	Authorized	Authorized	Authorized
33	34	35	36	37	38	39
Authorized	Authorized	Authorized	Authorized	Authorized	Authorized	Authorized
41	42	43	44	45	46	47
Authorized	Authorized	Authorized	Authorized	Authorized	Authorized	Authorized

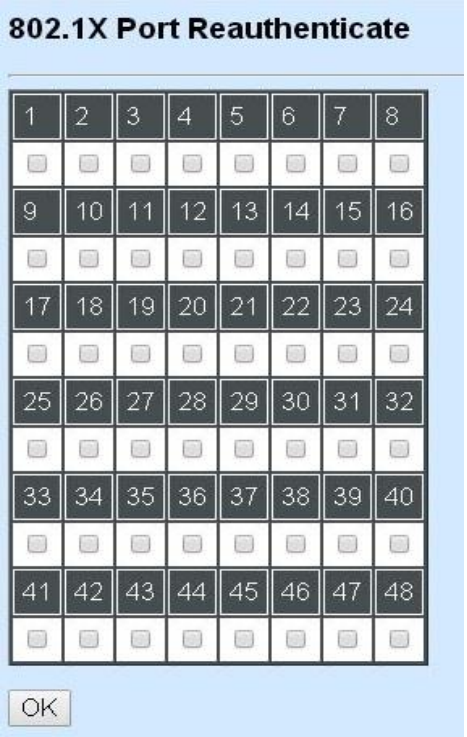
Authorized: This forces the Managed Switch to grant access to all clients, either 802.1X-aware or 802.1x-unaware. No authentication exchange is required. By default, all ports are set to “Authorized”.

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.

4.4.5.3 802.1X Port Reauthenticate

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



This allows users to enable or disable port Reauthenticate. 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 Table** 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

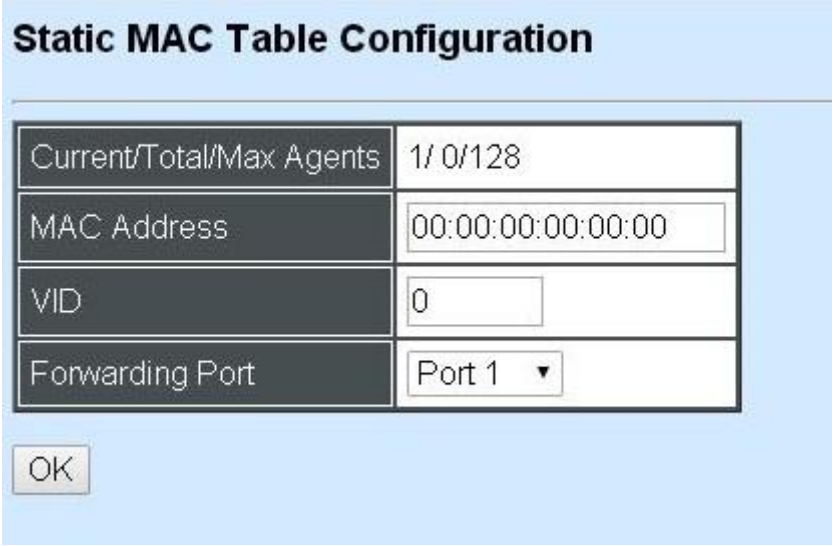
Click the option **Static MAC Table Configuration** from the **MAC Address Table** menu and then the following screen page appears.

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 **Edit** to view and edit the selected MAC address entity.

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



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.

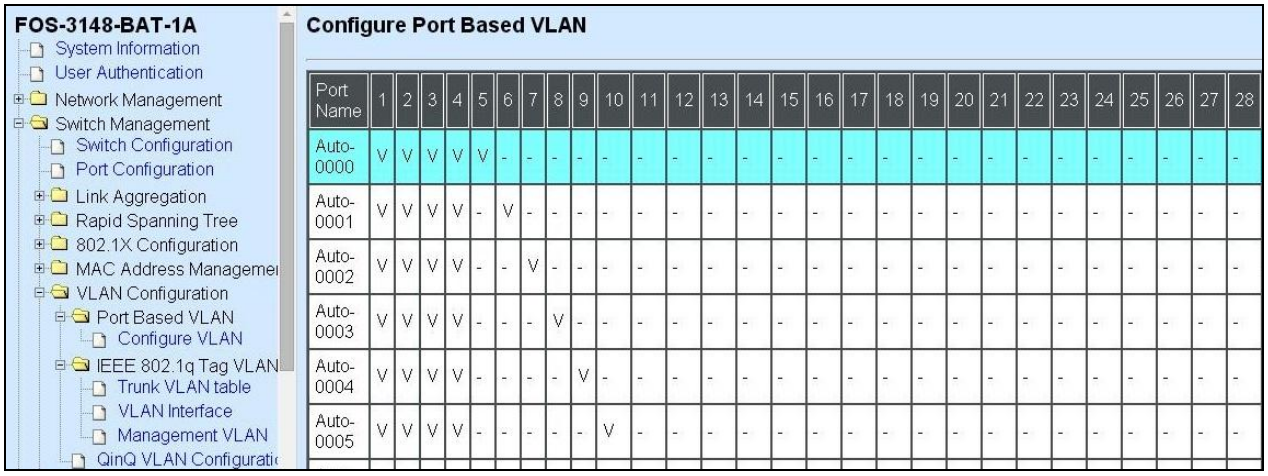
VID: Specify the VLAN where the packets with the Destination MAC address can be forwarded.

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.

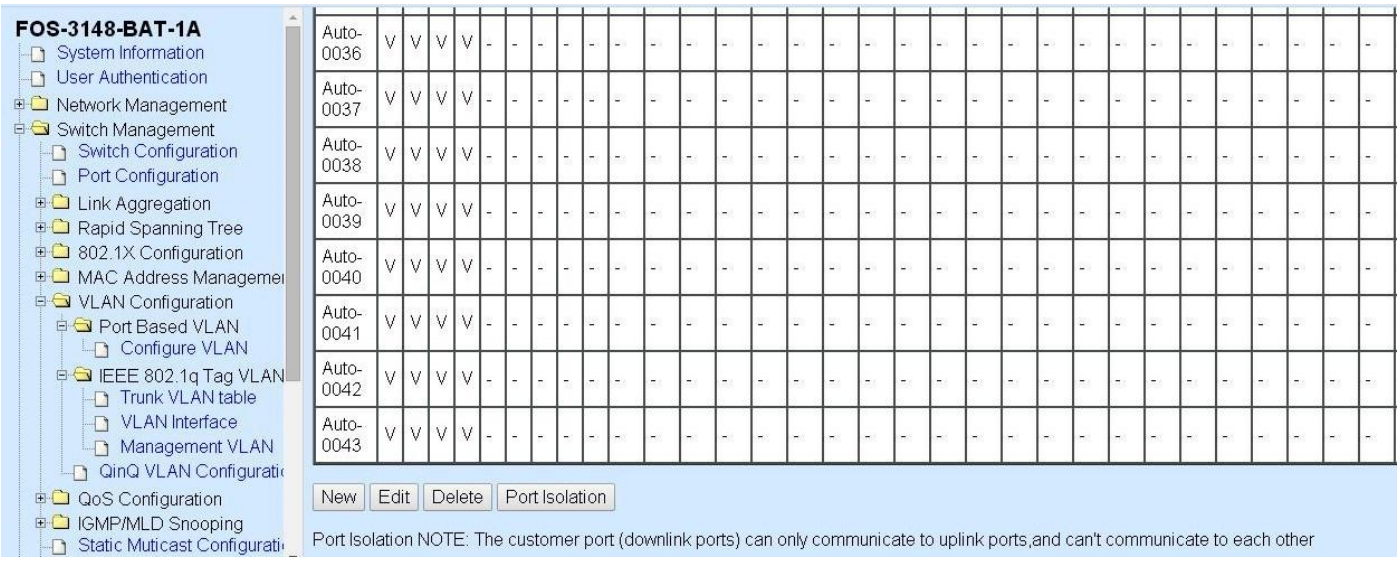


Port Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Auto-0000	V	V	V	V	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0001	V	V	V	V	-	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0002	V	V	V	V	-	-	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0003	V	V	V	V	-	-	-	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0004	V	V	V	V	-	-	-	-	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0005	V	V	V	V	-	-	-	-	-	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

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 and then select **Configure VLAN**.



Auto-0036	V	V	V	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0037	V	V	V	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0038	V	V	V	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0039	V	V	V	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0040	V	V	V	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0041	V	V	V	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0042	V	V	V	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0043	V	V	V	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

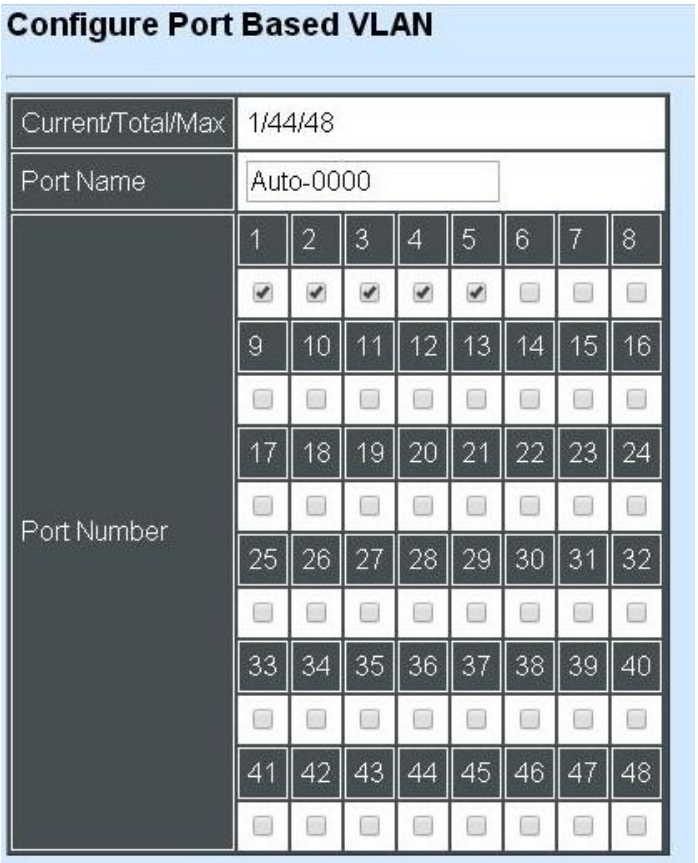
Since source addresses of the packets are listed in MAC address table of specific VLAN (except broadcast/multicast packets), in every VLAN the traffic between two ports will be two-way without restrictions.

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

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

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

Click **Port Isolation** to configure uplink port menbers.



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.

Port Number: By checking the ports, it denotes that the port selected belongs to the specified Port-Based VLAN.

4.4.7.2 802.1Q VLAN Concept

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.

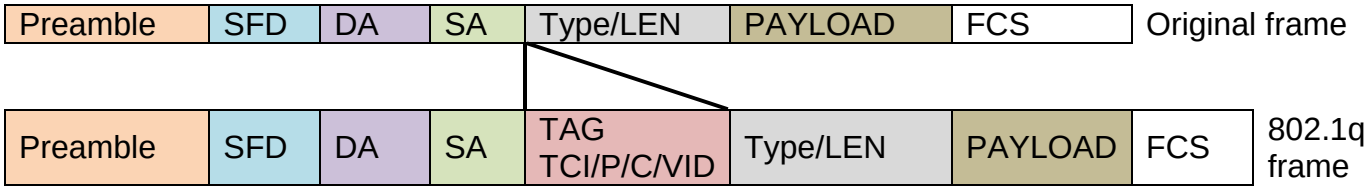
VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where 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.

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 VLAN ID 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.

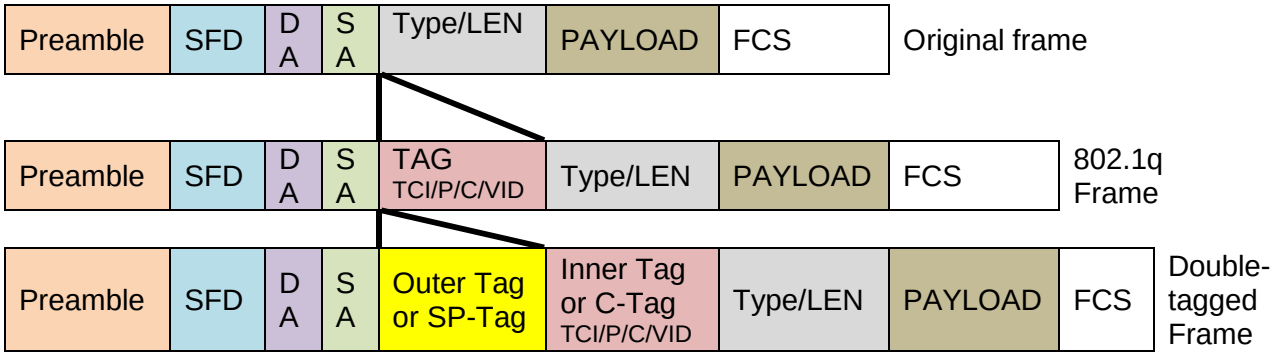
- **Trunk Native Mode :**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed 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.

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

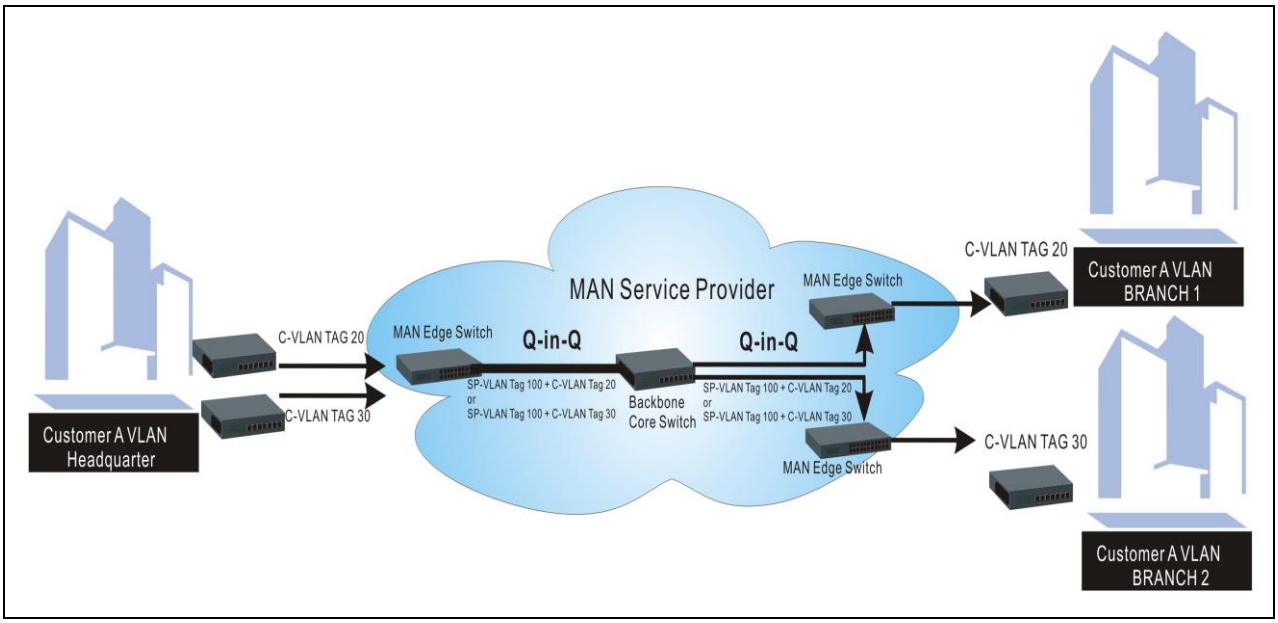
4.4.7.3 Introduction to Q-in-Q

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 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

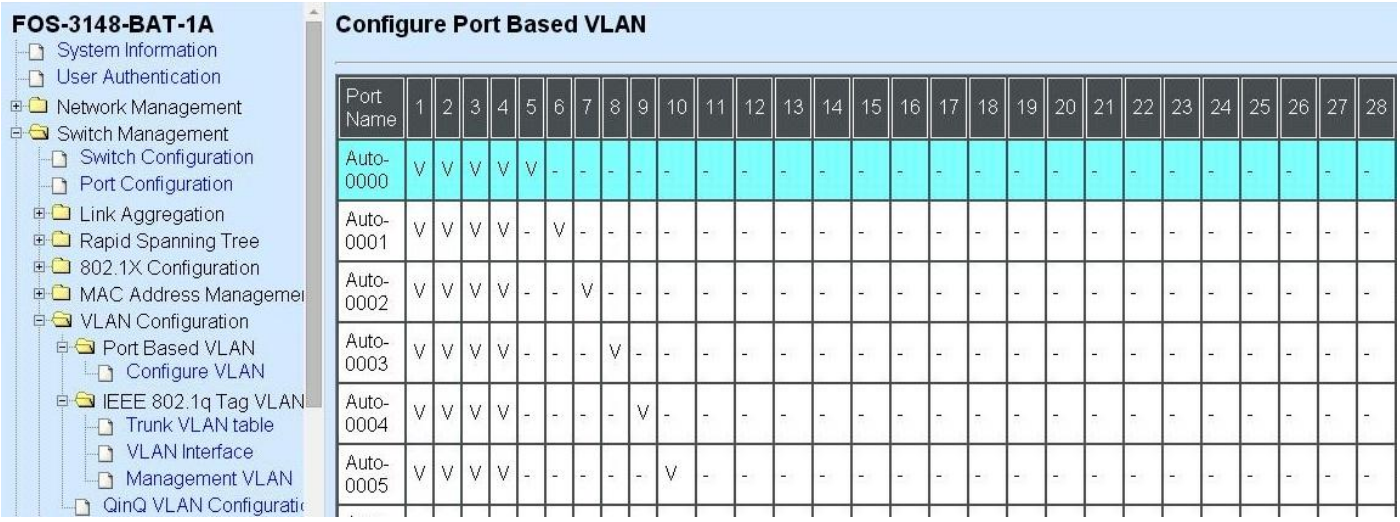
As shown below in “Q-in-Q Example” illustration, Headquarter A wants to communicate with Branch 1 that is 1000 miles away. One common thing about these two locations is that they have the same VLAN ID of 20, called C-VLAN (Customer VLAN). Since customer traffic will be routed to service provider’s backbone,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

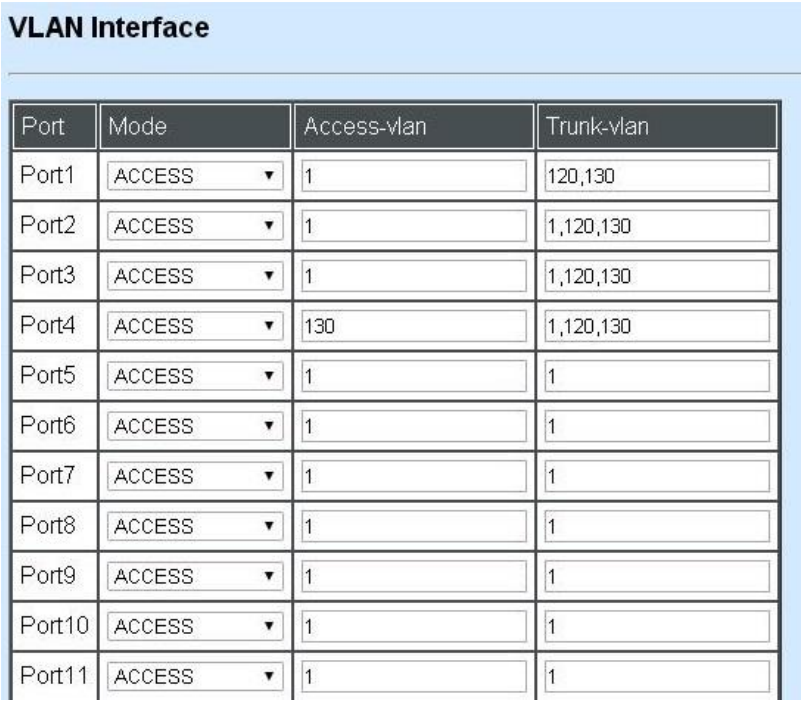


Port Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Auto-0000	V	V	V	V	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0001	V	V	V	V	-	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0002	V	V	V	V	-	-	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0003	V	V	V	V	-	-	-	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0004	V	V	V	V	-	-	-	-	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Auto-0005	V	V	V	V	-	-	-	-	-	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

1. **Trunk VLAN table:** To edit 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 VLAN Interface

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



Port	Mode	Access-vlan	Trunk-vlan
Port1	ACCESS	1	120,130
Port2	ACCESS	1	1,120,130
Port3	ACCESS	1	1,120,130
Port4	ACCESS	130	1,120,130
Port5	ACCESS	1	1
Port6	ACCESS	1	1
Port7	ACCESS	1	1
Port8	ACCESS	1	1
Port9	ACCESS	1	1
Port10	ACCESS	1	1
Port11	ACCESS	1	1

Mode: Select the appropriate mode for each port.

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

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

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

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.	

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

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

4.4.7.4.2 Trunk VLAN table

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

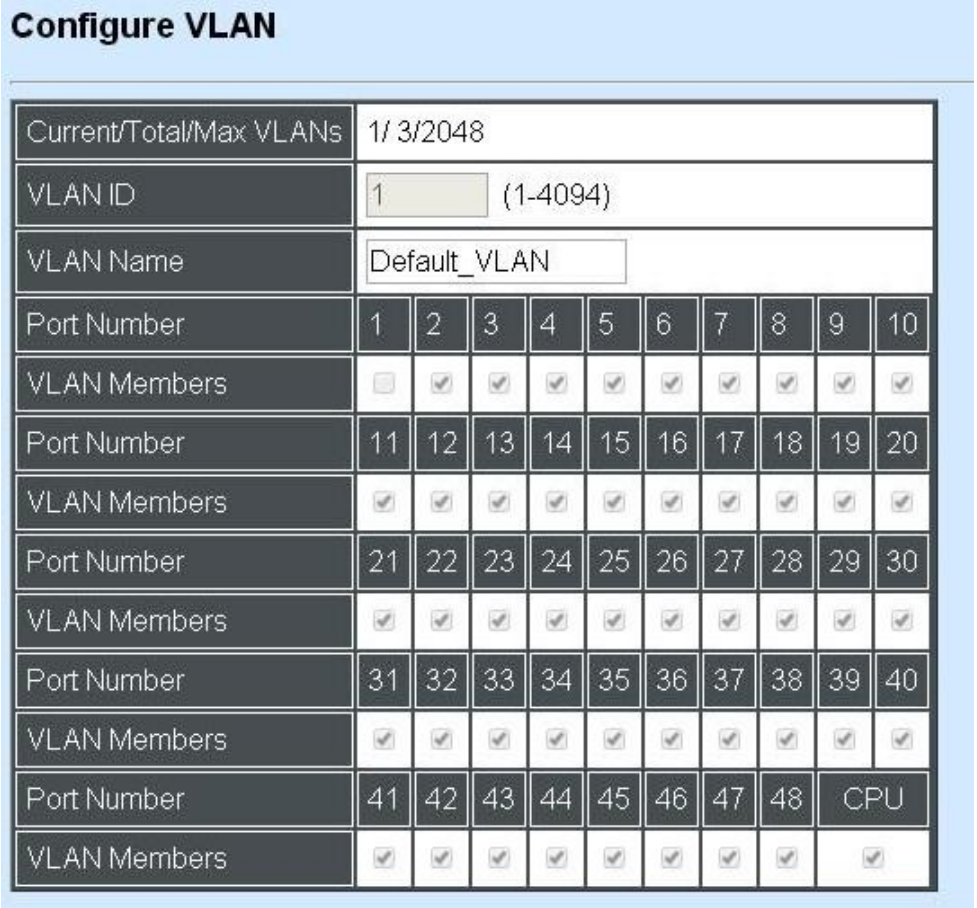
Trunk VLAN table

VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
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
	120	V	V	V	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	130	V	V	V	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Edit

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

Click **Edit** to view and edit current IEEE 802.1Q Tag VLAN setting.



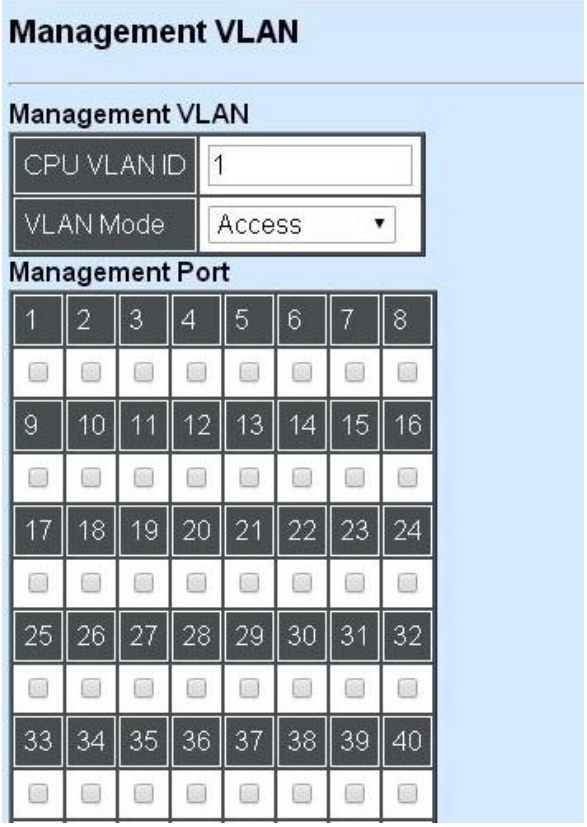
VLAN ID: View only field shows the VLAN ID of this VLAN group.

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.

4.4.7.4.3 Management VLAN

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



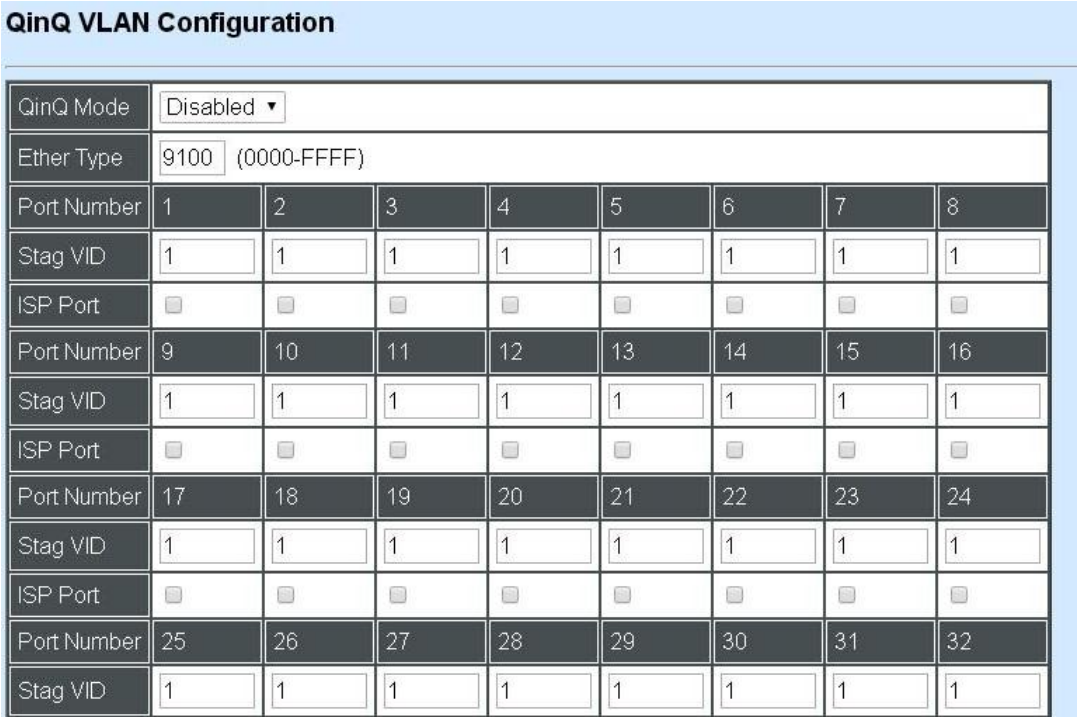
CPU VLAN ID: Specify an existing VLAN ID.

Mode: Select the VLAN mode for this Management VLAN.

Management Port: Tick the checkbox on the ports that you would like them to become Management ports.

4.4.7.4.4 QinQ VLAN configuration

The following screen page appears if you choose **QinQ VLAN configuration**.



QinQ Mode: Enable or Disable QinQ mode

Ether Type: Specify the Ether-type of the QinQ VLAN tag

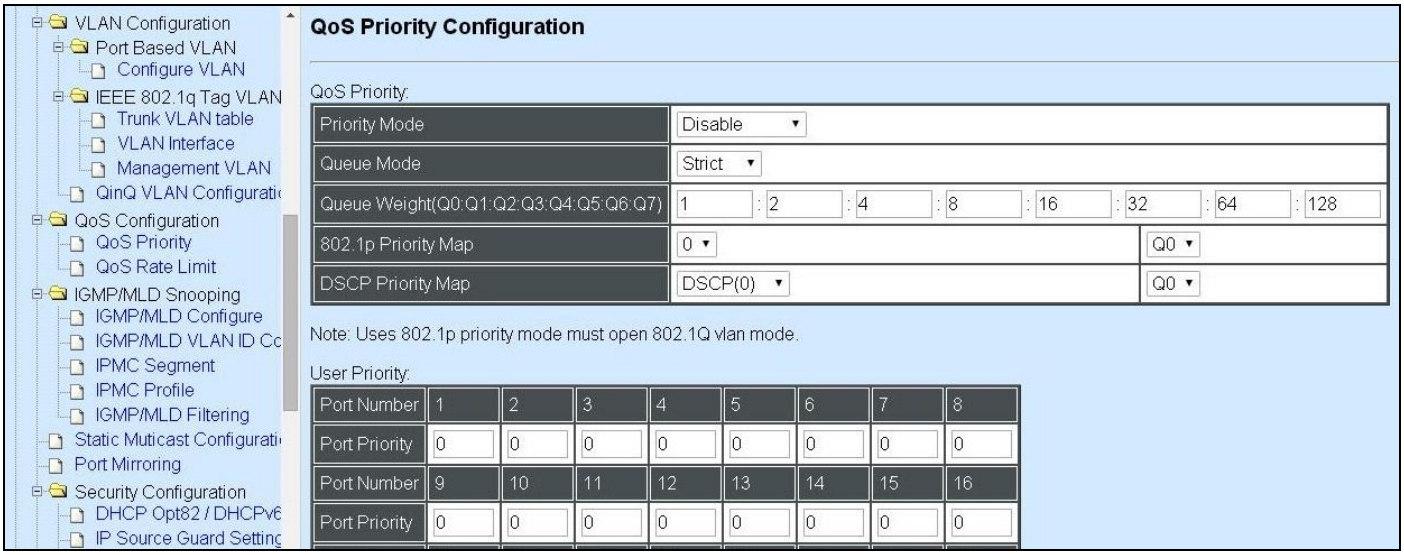
Stag VID: Specify the selected ports' Stag (service tag).

ISP Port: Check the port if it is the outbound port to the ISP.

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.

Qos Priority:

QoS Priority:

Priority Mode	Disable	
Queue Mode	Strict	
Queue Weight(Q0:Q1:Q2:Q3:Q4:Q5:Q6:Q7)	1 : 2 : 4 : 8 : 16 : 32 : 64 : 128	
802.1p Priority Map	0	Q0
DSCP Priority Map	DSCP(0)	Q0

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

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: Enable or Disable QinQ mode

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 eight different levels.

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

User Priority:

User Priority:

Port Number	1	2	3	4	5	6	7	8
Port Priority	0	0	0	0	0	0	0	0
Port Number	9	10	11	12	13	14	15	16
Port Priority	0	0	0	0	0	0	0	0
Port Number	17	18	19	20	21	22	23	24
Port Priority	0	0	0	0	0	0	0	0
Port Number	25	26	27	28	29	30	31	32
Port Priority	0	0	0	0	0	0	0	0
Port Number	33	34	35	36	37	38	39	40
Port Priority	0	0	0	0	0	0	0	0
Port Number	41	42	43	44	45	46	47	48
Port Priority	0	0	0	0	0	0	0	0
Port Number	CPU							
Port Priority	0							

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:

Remarking:

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

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

OK

Configure 802.1p Remark:

Check **802.1p Remarking** to enable.

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

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

Configure DSCP Remark:

Check **DSCP Remarking** to enable.

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

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

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:

Policer Rate (500-1000000 KBits/Sec 0:Disable)

1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0
9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0
17	18	19	20	21	22	23	24
0	0	0	0	0	0	0	0
25	26	27	28	29	30	31	32
0	0	0	0	0	0	0	0
33	34	35	36	37	38	39	40
0	0	0	0	0	0	0	0
41	42	43	44	45	46	47	48
0	0	0	0	0	0	0	0

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:

Shaper Rate (500-1000000 KBits/Sec 0:Disable)

1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0
9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0
17	18	19	20	21	22	23	24
0	0	0	0	0	0	0	0
25	26	27	28	29	30	31	32
0	0	0	0	0	0	0	0
33	34	35	36	37	38	39	40
0	0	0	0	0	0	0	0
41	42	43	44	45	46	47	48
0	0	0	0	0	0	0	0

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.

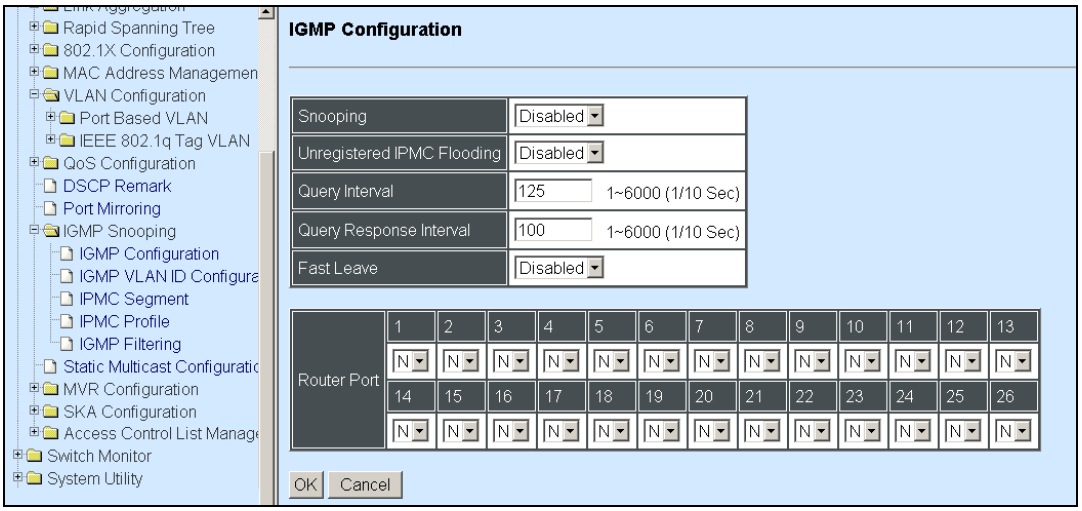
IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers by processing the layer 3 packets that IGMP packets sent in a multicast network.

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 the following screen page appears.



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

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

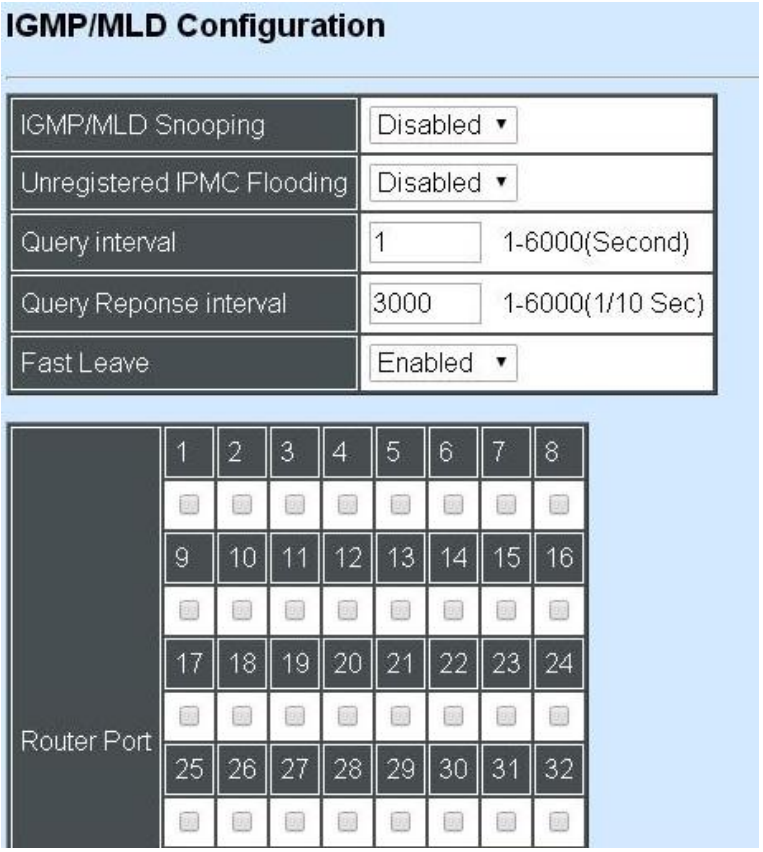
3. **IPMC Segment:** To create, edit or delete IPMC segment.

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

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

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.

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 1, One Unit =1 second)

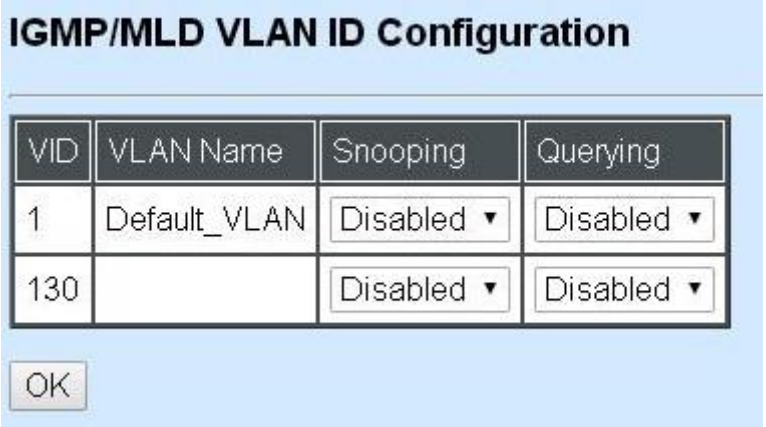
Query Response Interval: This determines the maximum amount of time allowed before sending an IGMP response report. (Default value 3000, One Unit=0.1 second)

Immediate Leave: The Immediate 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 ability information 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 want 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.

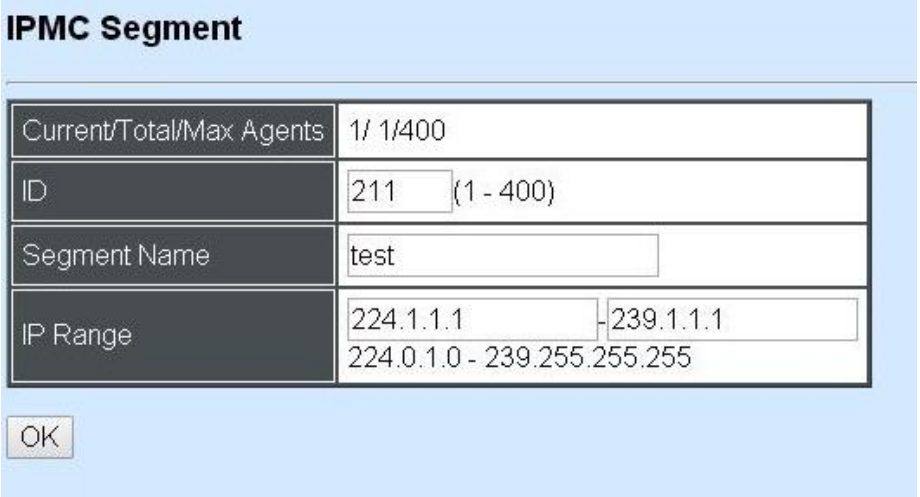
Segment Name: View-only field that shows the current registered Name.

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 edit and view the IPMC Segment settings.

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



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

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

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

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

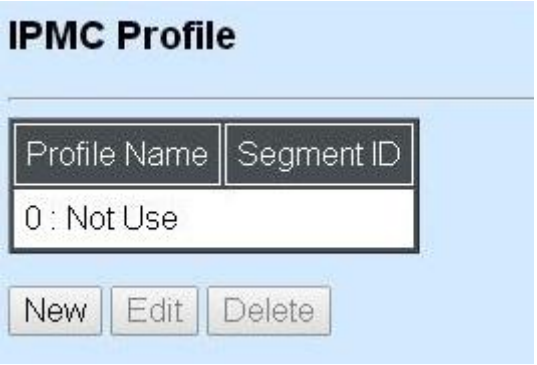
Segment ID: Specify a number from 1~400 for a new ID.

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

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

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.

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

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

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

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

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

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

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

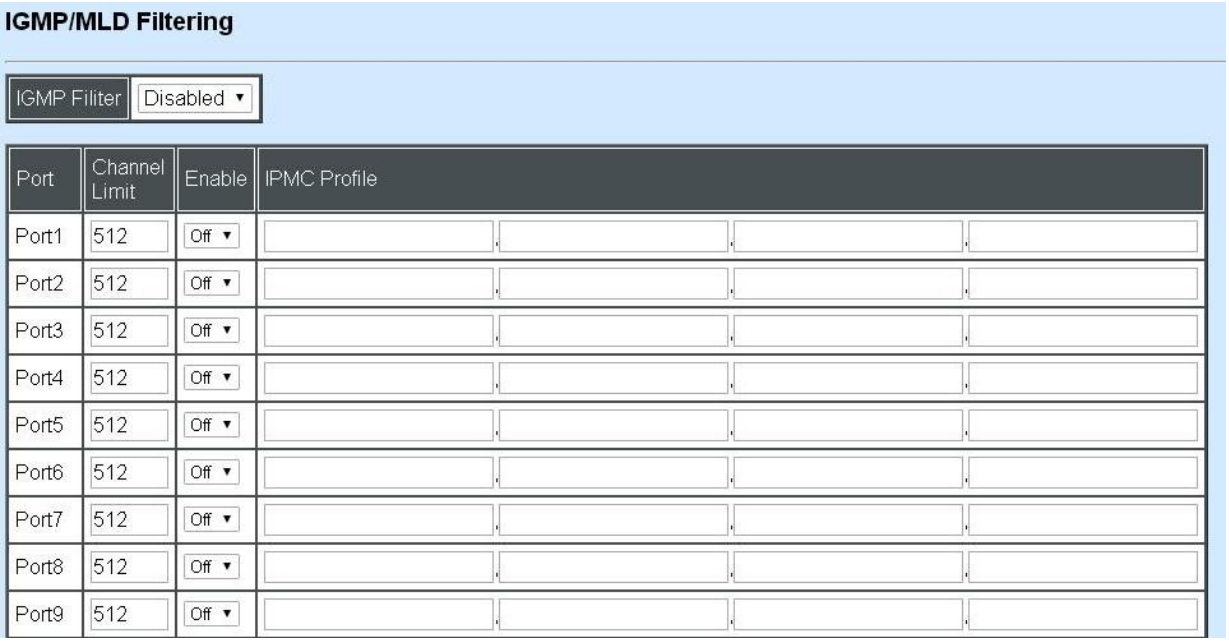
Max: This shows the maximum number available for IPMC Profile. The maximum number is 60.

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

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

4.4.9.5 IGMP/MLD Filtering

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



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

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

Channel Limit: Specify the maximum transport multicast stream.

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

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

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.

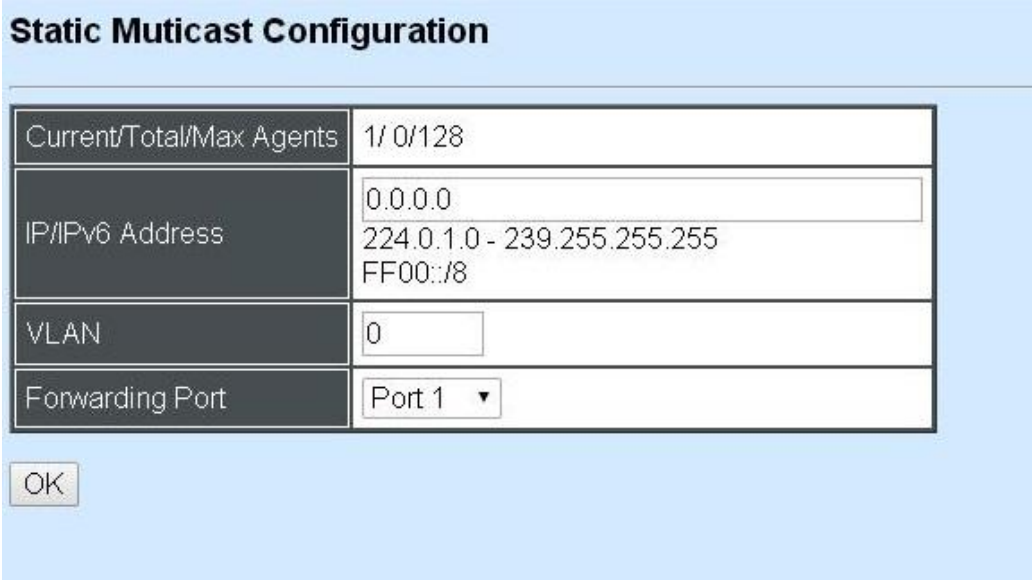
VID: View-only field that shows the specified VLAN ID for current multicast stream.

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 edit and view 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 total number of registered static multicast configuration.

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

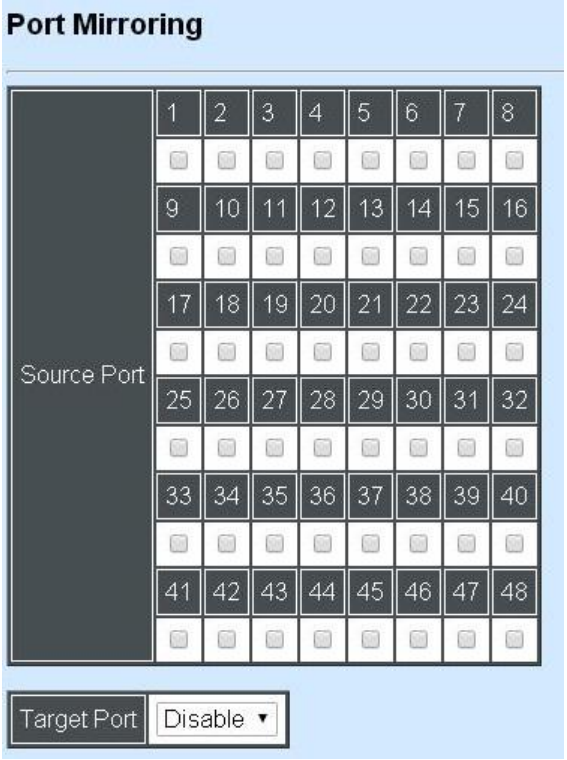
IP/IPv6 Address: Specify the multicast stream source IP/IPv6 address.

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 Target Port to mirror Source Port and enable traffic monitoring, select the option **Port Mirroring** from the **Switch Management** menu and then the following screen page appears.



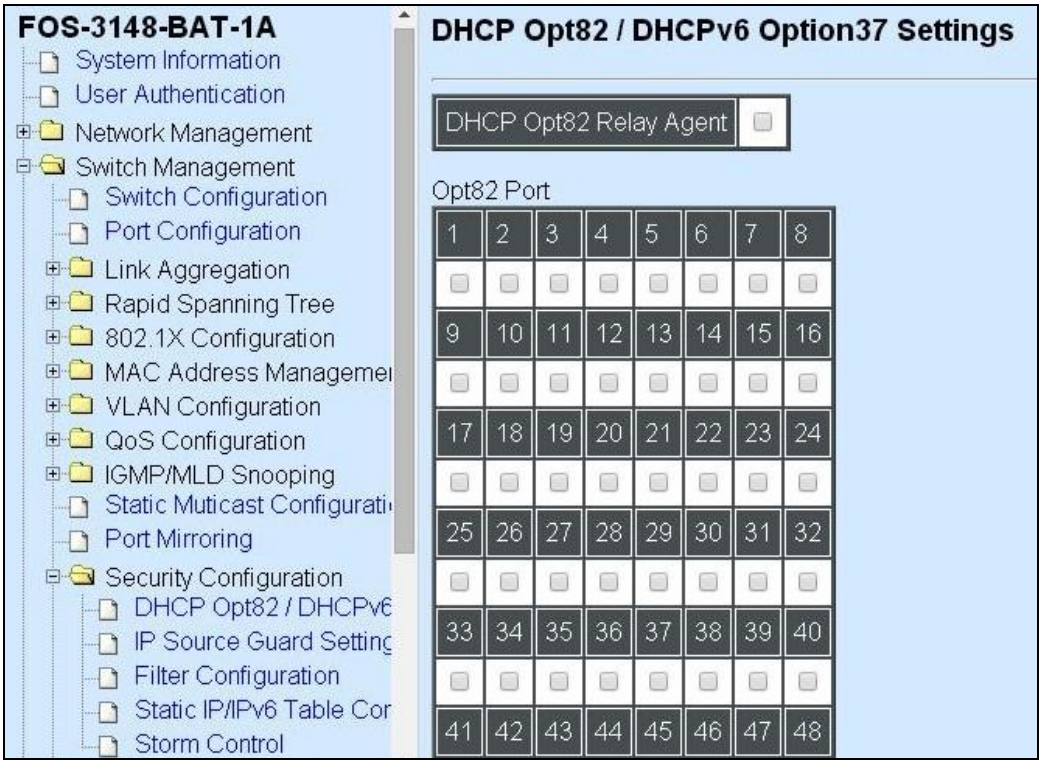
Source Port: Select the preferred source port for mirroring.

Target Port: Choose from port 1 to port 48 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 the following screen page appears.



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

3. **Filter Configuration:** Customer port filtering setting.

4. **Static IP Table Configuration:** To create static IP table for DHCP snooping setting.

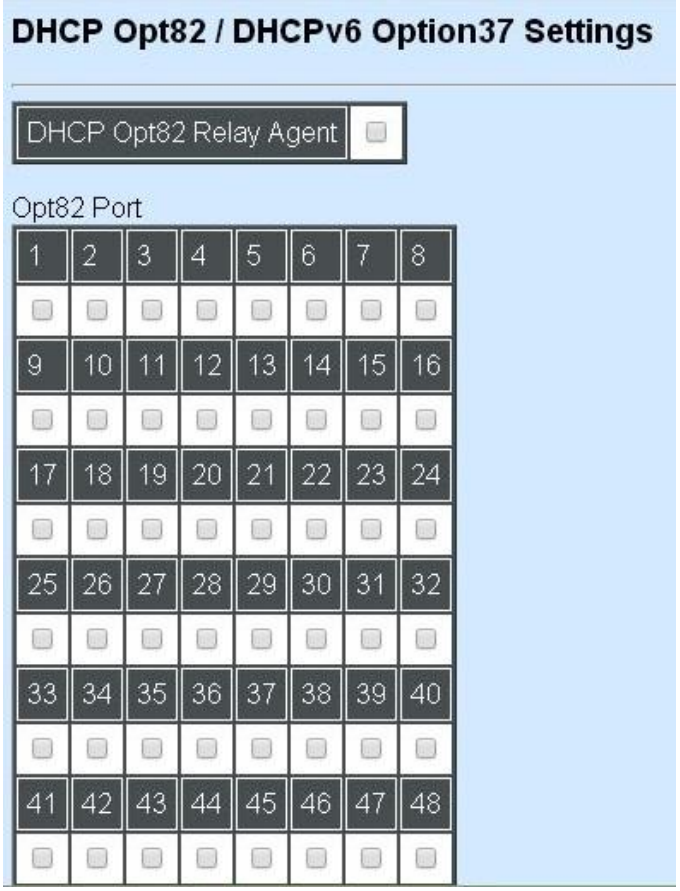
5. **Storm Control:** To prevent the Managed Switch from unicast, broadcast, and multicast storm.

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.



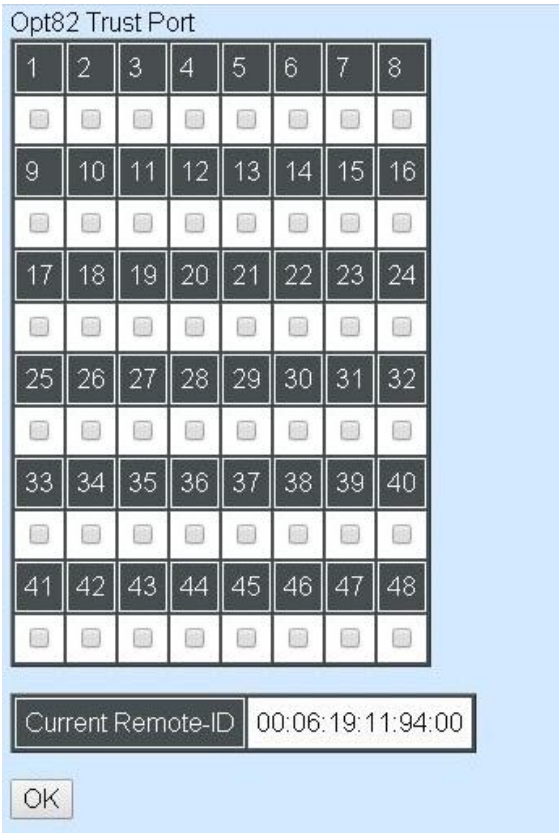
Relay Agent: To enable or disable DHCP Option 82 Relay Agent Global setting. When enabled, Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers recognizing the Relay Agent Information option may use the Information 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.

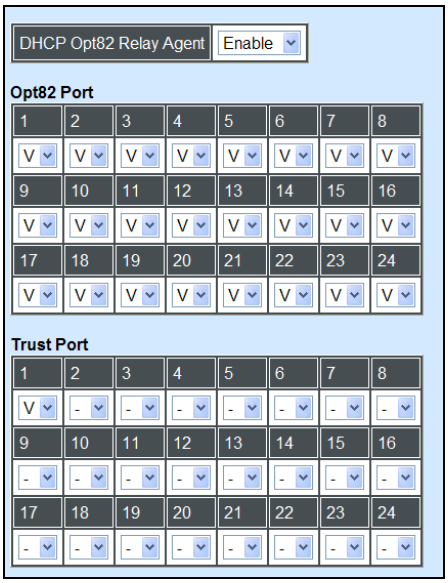
Disable (uncheck): Forward.

Configure Trust Port Setting:



Trust Port: Check 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.

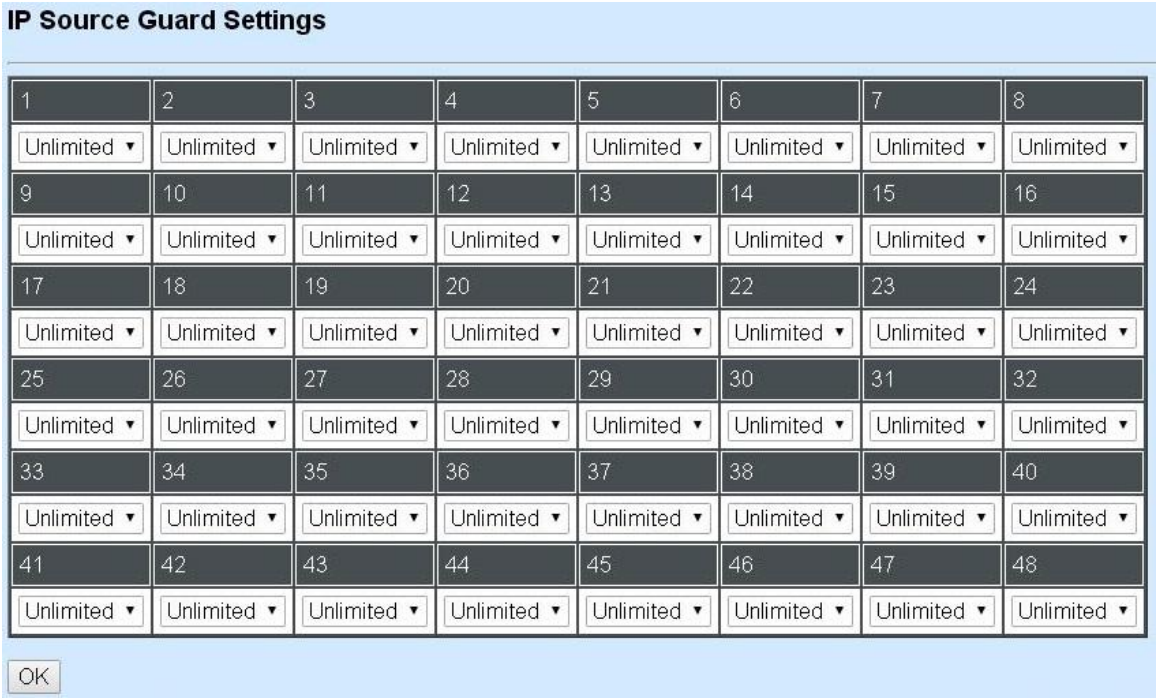
A. If a DHCP request is with Opt82 Agent information and then the Managed Switch will forward it.
B. If a DHCP request is without Opt82 Agent information and then the Managed Switch will add Opt82 Agent information and forward it.

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 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 authorized access information for each port. There are three options available.

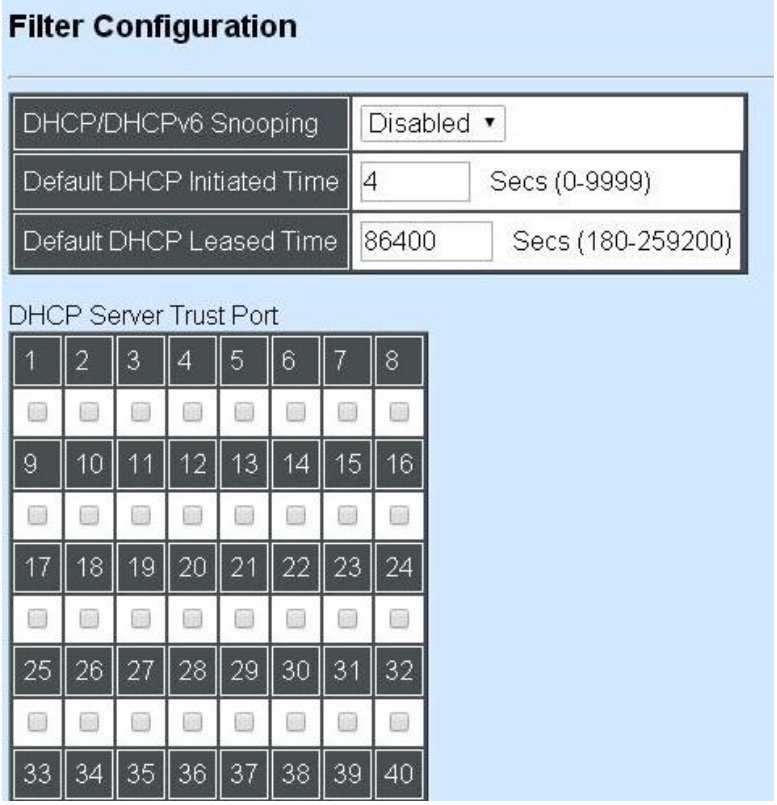
Unlimited: Non-Limited (Static IP or DHCP-assigned IP).

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.).

4.4.12.3 Filter Configuration

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

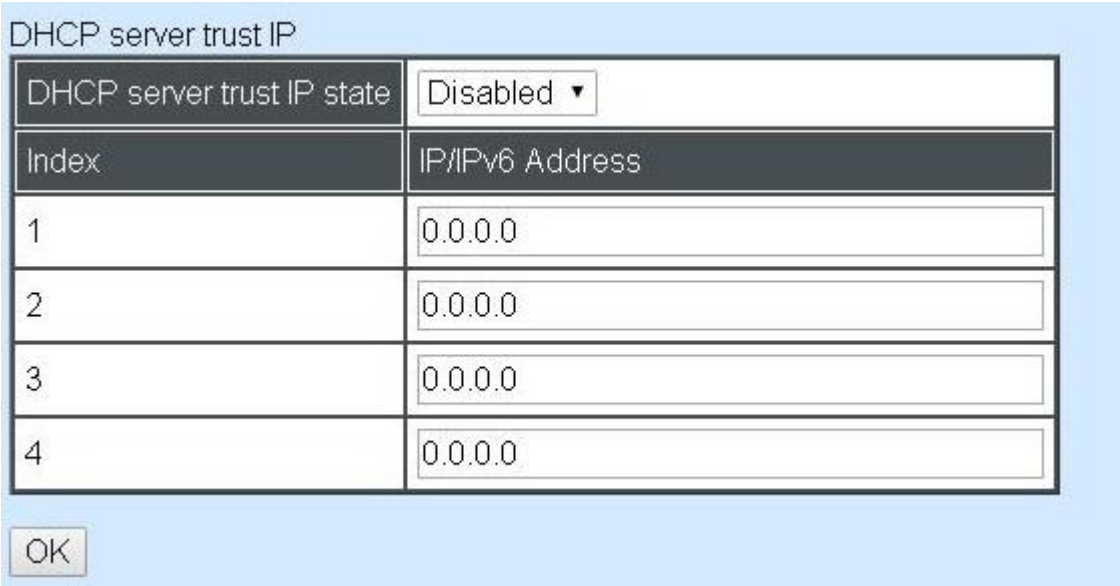


DHCP/DHCPv6 Snooping: Enable or disable DHCP/DHCPv6 Snooping function.

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 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.

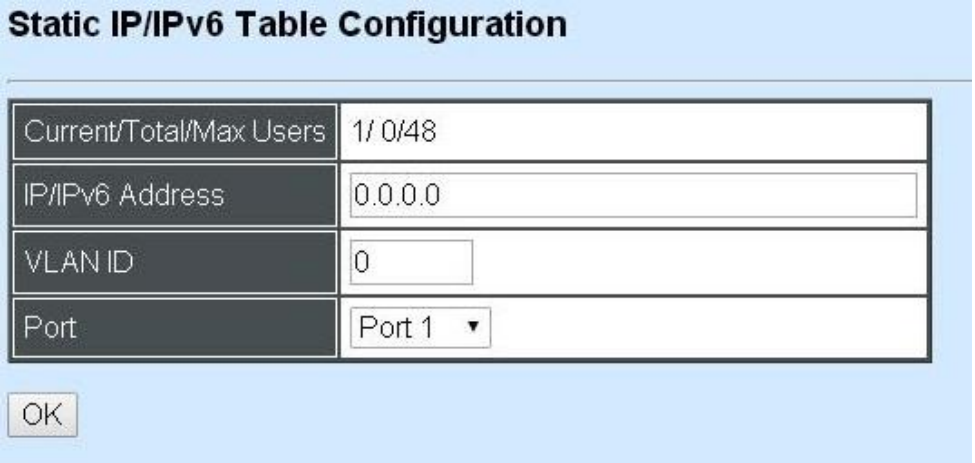
VLAN ID: View-only field that shows the VLAN ID.

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 edit and view Static 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 addresses.

Total: This shows the total number of 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.

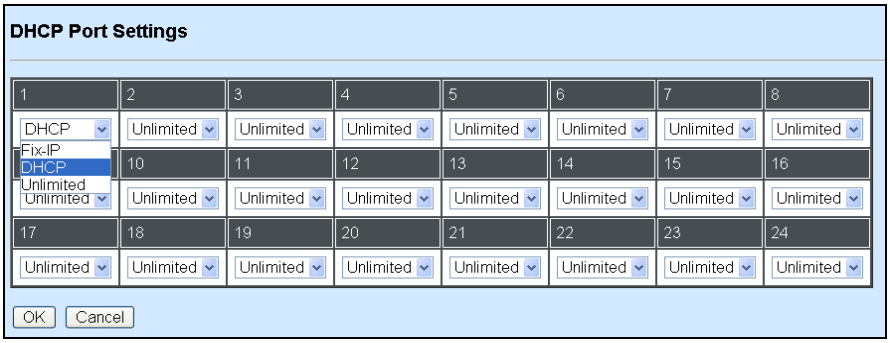
VLAN ID: Specify the VLAN ID. (0 means without VLAN ID)

Port: Specify the communication port number. (Port 1~48)

4.4.12.5 Configure DHCP Snooping

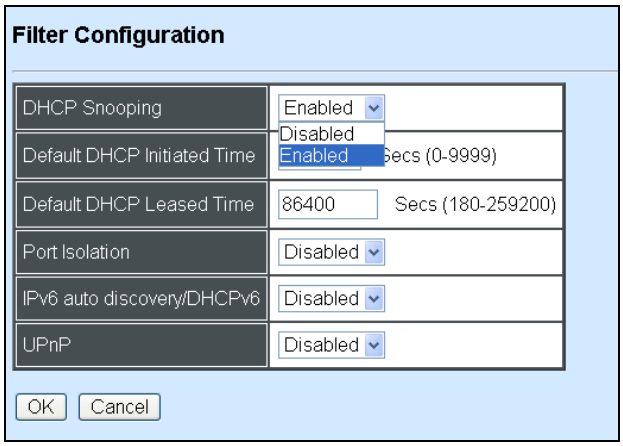
When you want to use DHCP Snooping function, follow the steps described below to enable a client to receive an IP from DHCP server.

Step 1. Select each port's IP type



Select "Unlimited" or "DHCP"

Step 2. Enable DHCP Snooping



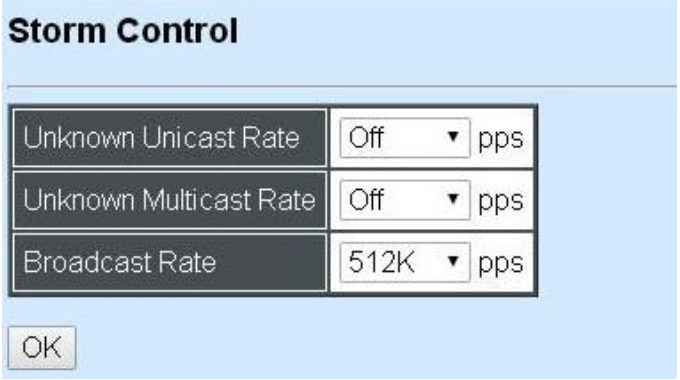
Step 3. Connect your clients to the Managed Switch

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.

4.4.12.6 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, which eventually degrades network performance and even worse cause a complete halt. The network can be protected from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packet exceeding the specified threshold will then be dropped (see Anti-broadcast Configuration).

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

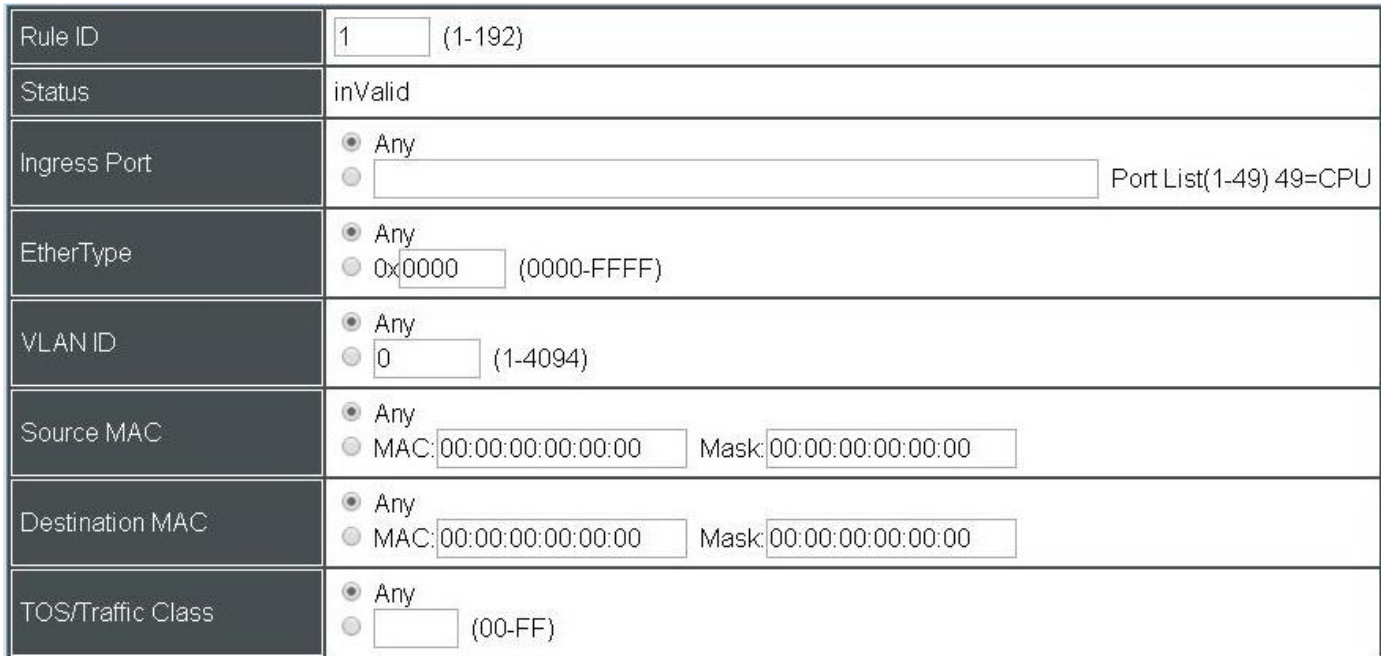
Unknown Unicast Rate: Enable or disable unknown Unicast traffic control and set up unknown Unicast Rate packet per second (pps).

Multicast Rate: Enable or disable Multicast traffic control and set up Multicast Rate packet per second (pps).
Broadcast Rate: Enable or disable Broadcast traffic control and set up broadcast Rate packet per second (pps).

4.4.13 Access Control List (ACL) Configuratiom

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.



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 Filter: Select “Any” or specify an Ethernet type value.

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

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

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

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

Protocol/Next Header	Any 0x (00-FF)
IPv4 Source IP	Any Network IP: 0.0.0.0 Mask: 0.0.0.0
IPv4 Destination IP	Any Network IP: 0.0.0.0 Mask: 0.0.0.0
IPv6 Source IP	Any Network IP: :: Mask: 0 (10-128)
IPv6 Destination IP	Any Network IP: :: Mask: 0 (10-128)
TCP/UDP Source Port	Any Port: 0 (1-65535) Mask:0x 0000 (0000-FFFF)
TCP/UDP Destination Port	Any Port: 0 (1-65535) Mask:0x 0000 (0000-FFFF)
Action	Deny
Port Number	1 (1-48)
Rate Limiter	16 (16-1048560) Kbps

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

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

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

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

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

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

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

Action: Deny or permit the action.

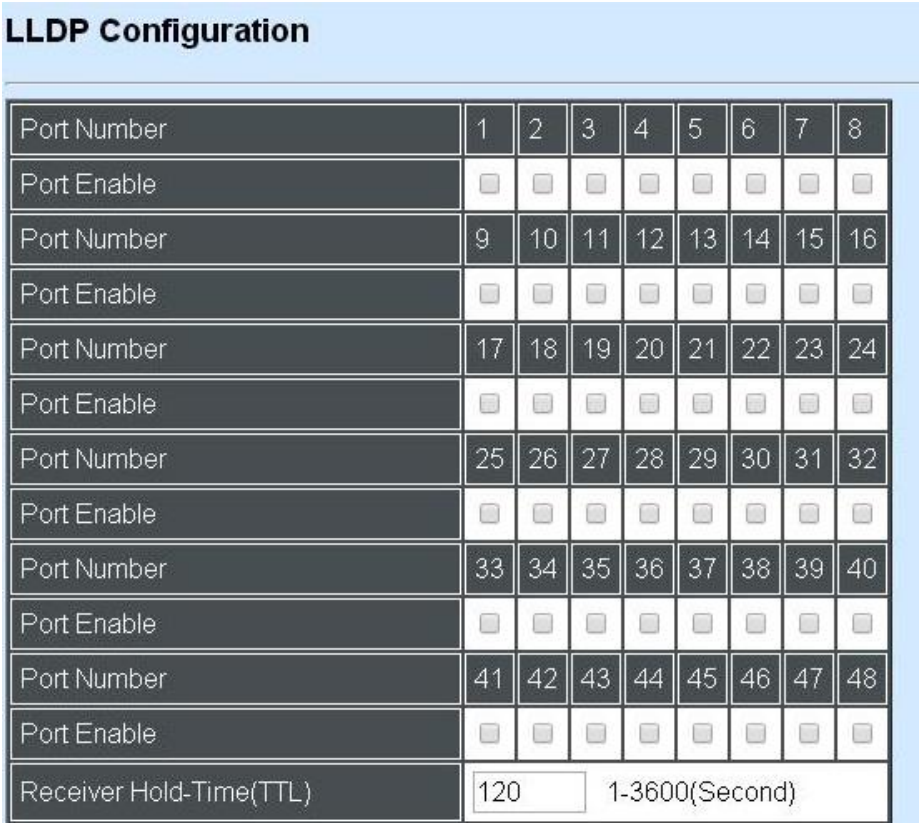
Port number: Specify a port number that you would like to configure.

Rate Limiter: Disable or enable rate limiter. When rater limiter is enabled, you can further set up each Rate Limiter’s rate.

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 TLVs. Details such as port description, system name, system description, system capabilities, management address can be sent and received on this Managed Switch. Use Spacebar to select “ON” if you want to receive and send the TLV.

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



LLDP Configuration

Port Number	1	2	3	4	5	6	7	8
Port Enable	☐	☐	☐	☐	☐	☐	☐	☐
Port Number	9	10	11	12	13	14	15	16
Port Enable	☐	☐	☐	☐	☐	☐	☐	☐
Port Number	17	18	19	20	21	22	23	24
Port Enable	☐	☐	☐	☐	☐	☐	☐	☐
Port Number	25	26	27	28	29	30	31	32
Port Enable	☐	☐	☐	☐	☐	☐	☐	☐
Port Number	33	34	35	36	37	38	39	40
Port Enable	☐	☐	☐	☐	☐	☐	☐	☐
Port Number	41	42	43	44	45	46	47	48
Port Enable	☐	☐	☐	☐	☐	☐	☐	☐
Receiver Hold-Time(TTL)	120	1-3600(Second)						

Port: Check the checkbox to enable LLDP.

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

Sending LLDP Packet Interval	5	1-180(Second)
Sending LLDP Packets Per Discover	1	1-16(Packet)
Delay LLDP Initialization	0	0-300(Second)
Selection of LLDP TLVs to send		
Port Description	☑	
System Name	☑	
System Description	☑	
System Capabilities	☑	
Management Address	☑	

OK

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

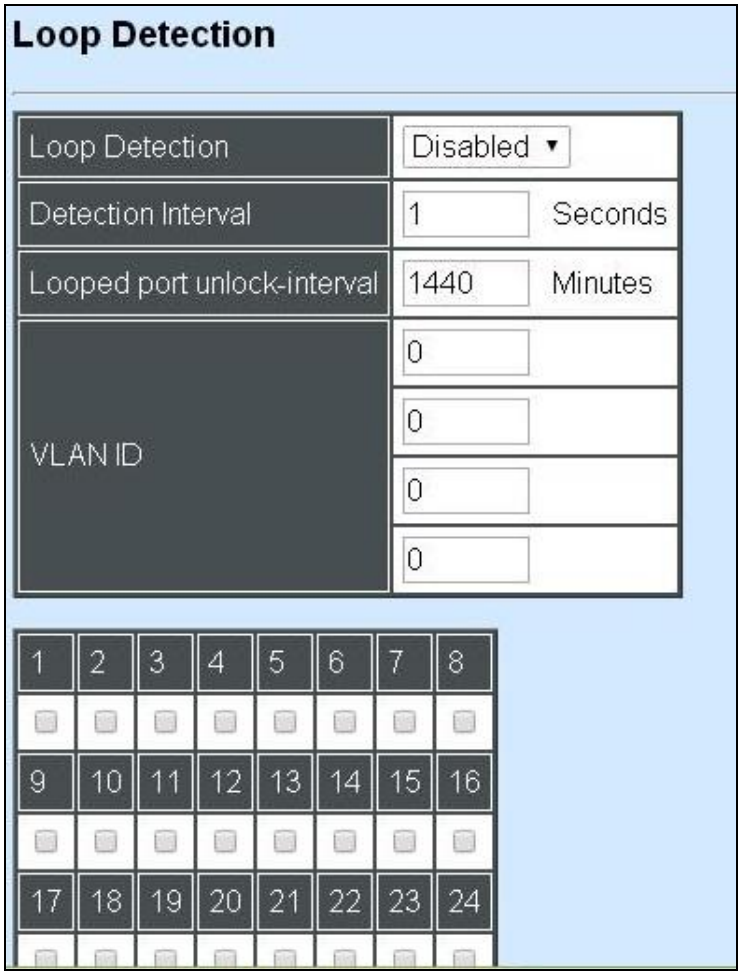
Sending Packets Per Discover: Enter the amount of packets sent in each discover.

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

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

4.4.15 Loop Detection Configuration

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 or disable Loop Detection function.

Detection Interval: Specify the time interval of performing Loop Detection. The maximum time interval is 180 seconds.

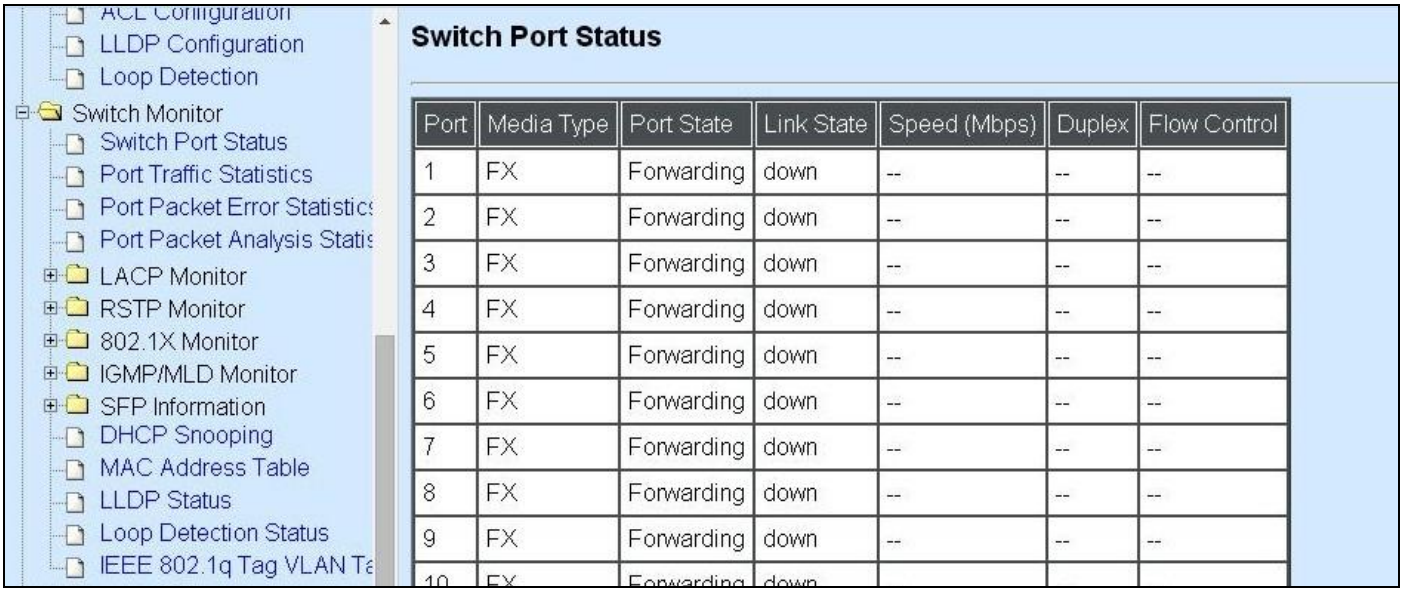
Looped port unlock-interval: Specify the time interval of unlocking looped ports. The maximum time interval is 1440 minutes.

VLAN ID: Specify the VLANs where Loop Detection will be performed.

Port 1~48: Enable or disabled Loop Detection function on the specific port(s).

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 the following screen page appears.



Port	Media Type	Port State	Link State	Speed (Mbps)	Duplex	Flow Control
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	down	--	--	--
10	FX	Forwarding	down			

1. **Switch Port State:** View current port media type, port state, etc.

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

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

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

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

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

7. **802.1X Monitor:** View port status and Statistics.

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

9. **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..

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

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

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

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

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

4.5.1 Switch Port State

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
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	down	--	--	--
10	FX	Forwarding	down	--	--	--
11	FX	Forwarding	down	--	--	--
12	FX	Forwarding	down	--	--	--
13	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

4.5.2 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 Traffic Statistics

Select Rate

Port	Bytes Received	Frames Received	Received Utilization	Bytes Sent	Frames Sent	Sent Utilization	Total Bytes	Total Utilization
1	0	0	0.00%	0	0	0.00%	0	0.00%
2	0	0	0.00%	0	0	0.00%	0	0.00%
3	0	0	0.00%	0	0	0.00%	0	0.00%
4	0	0	0.00%	0	0	0.00%	0	0.00%
5	0	0	0.00%	0	0	0.00%	0	0.00%
6	0	0	0.00%	0	0	0.00%	0	0.00%
7	0	0	0.00%	0	0	0.00%	0	0.00%
8	0	0	0.00%	0	0	0.00%	0	0.00%
9	0	0	0.00%	0	0	0.00%	0	0.00%
10	0	0	0.00%	0	0	0.00%	0	0.00%
11	0	0	0.00%	0	0	0.00%	0	0.00%

Select: Choose the Traffic Statistics from the pull-down menu.

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.

4.5.3 Port Packet Error Statistics

Port Packet Error Statistics mode counters allow users to view the port error of the Managed Switch. The event mode 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 Packet Error Statistics

Select Rate

Port	Rx CRC Error	Rx Align Error	Rx Undersize	Rx Fragments	Rx Jabbers	RX Oversize Frames	RX Dropped Frames	Tx Collisions	TX Dropped Frames	Total Errors
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0

Select: Choose the Packet Error Statistics from the pull-down menu.

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.

4.5.4 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 Packet Analysis Statistics

Select Rate

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

Select: Choose the Packet Error Statistics from the pull-down menu.

Frames 64 Bytes: 64 bytes frames received.

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

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

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

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

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

Frames 1519-MAX Bytes: Over 1519 bytes frames received.

RX Multicast Frames: Good multicast frames received.

TX Multicast Frames: Good multicast packets sent.

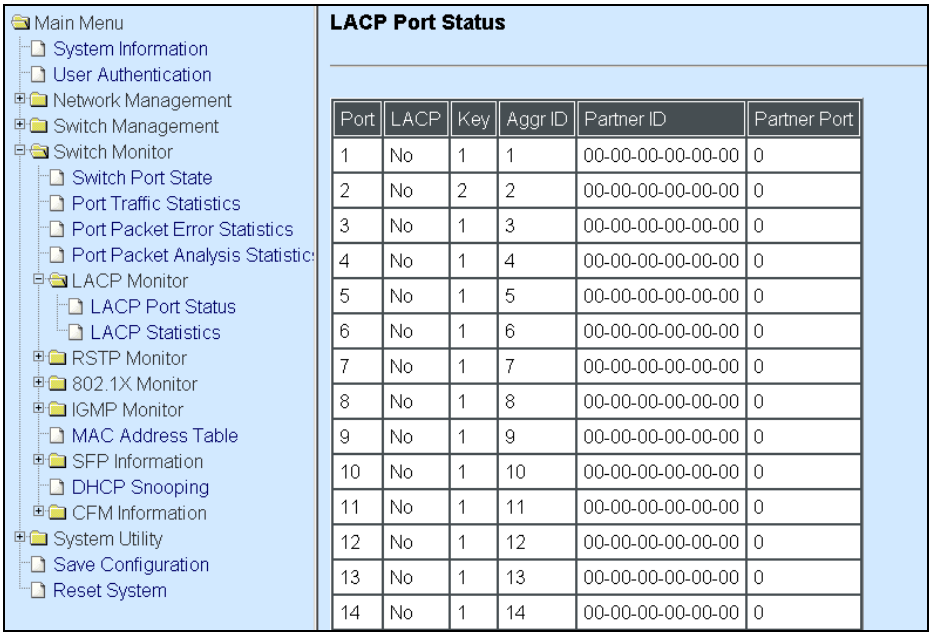
RX Broadcast Frames: Good broadcast frames received.

TX Broadcast Frames: Good broadcast packets sent.

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

4.5.5 LACP Monitor

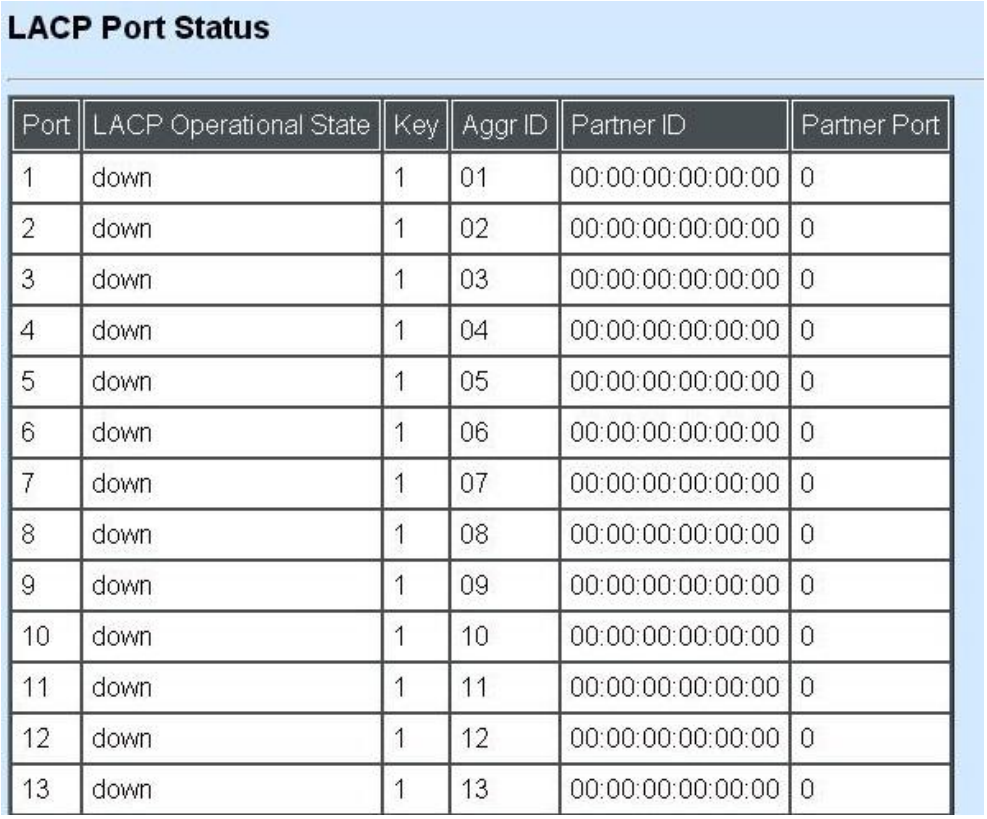
Click the **LACP Monitor** folder and then the two options will appears.



Port	LACP	Key	Aggr ID	Partner ID	Partner Port
1	No	1	1	00-00-00-00-00-00	0
2	No	2	2	00-00-00-00-00-00	0
3	No	1	3	00-00-00-00-00-00	0
4	No	1	4	00-00-00-00-00-00	0
5	No	1	5	00-00-00-00-00-00	0
6	No	1	6	00-00-00-00-00-00	0
7	No	1	7	00-00-00-00-00-00	0
8	No	1	8	00-00-00-00-00-00	0
9	No	1	9	00-00-00-00-00-00	0
10	No	1	10	00-00-00-00-00-00	0
11	No	1	11	00-00-00-00-00-00	0
12	No	1	12	00-00-00-00-00-00	0
13	No	1	13	00-00-00-00-00-00	0
14	No	1	14	00-00-00-00-00-00	0

4.5.5.1 LACP Port Status

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



Port	LACP Operational State	Key	Aggr ID	Partner ID	Partner Port
1	down	1	01	00:00:00:00:00:00	0
2	down	1	02	00:00:00:00:00:00	0
3	down	1	03	00:00:00:00:00:00	0
4	down	1	04	00:00:00:00:00:00	0
5	down	1	05	00:00:00:00:00:00	0
6	down	1	06	00:00:00:00:00:00	0
7	down	1	07	00:00:00:00:00:00	0
8	down	1	08	00:00:00:00:00:00	0
9	down	1	09	00:00:00:00:00:00	0
10	down	1	10	00:00:00:00:00:00	0
11	down	1	11	00:00:00:00:00:00	0
12	down	1	12	00:00:00:00:00:00	0
13	down	1	13	00:00:00:00:00:00	0

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

Port Number: The number of the port.

LACP Operational State: Current operational state of LACP

Key: The current operational key for the LACP group.

Aggr ID: The ID of the LACP group.

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

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

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

4.5.5.2 LACP Statistics

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

LACP Statistics

Clear All

Port	LACP Transmitted	LACP Received	Illegal Received	Unknown Received	Clear Counters
1	0	0	0	0	Clear
2	0	0	0	0	Clear
3	0	0	0	0	Clear
4	0	0	0	0	Clear
5	0	0	0	0	Clear
6	0	0	0	0	Clear
7	0	0	0	0	Clear
8	0	0	0	0	Clear
9	0	0	0	0	Clear
10	0	0	0	0	Clear
11	0	0	0	0	Clear

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

LACP Transmitted: Packets transmitted from current port.

LACP Received: Packets received form current port.

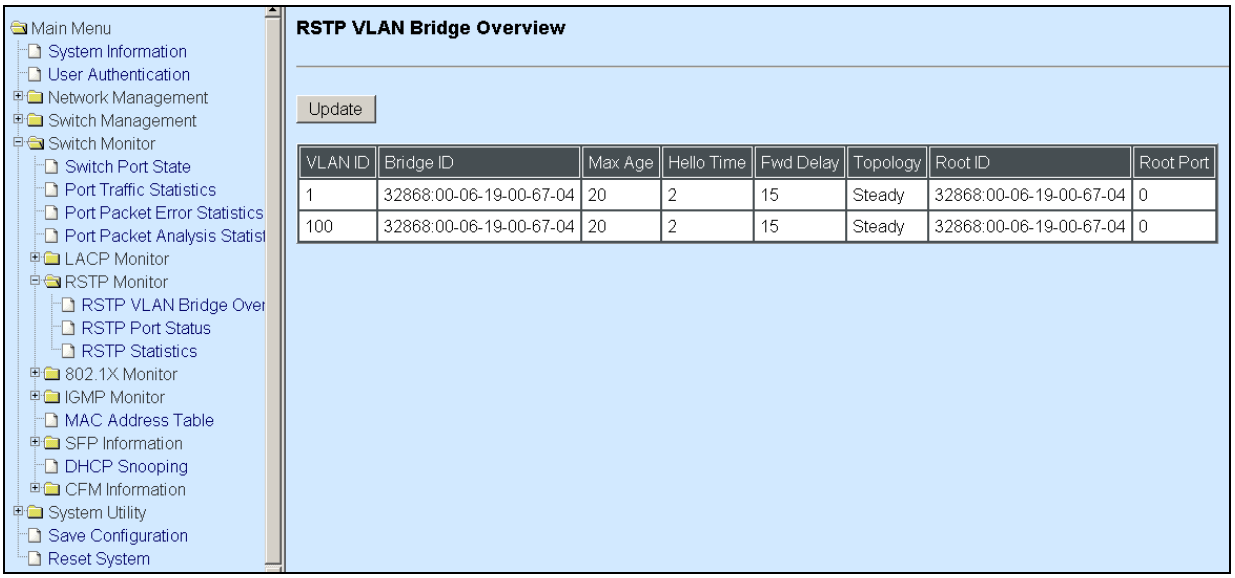
Illegal Received: Illegal packets received from current port.

Unknown Received: Unknown packets received from current port.

Clear Counter: Clear the statistics of the current port.

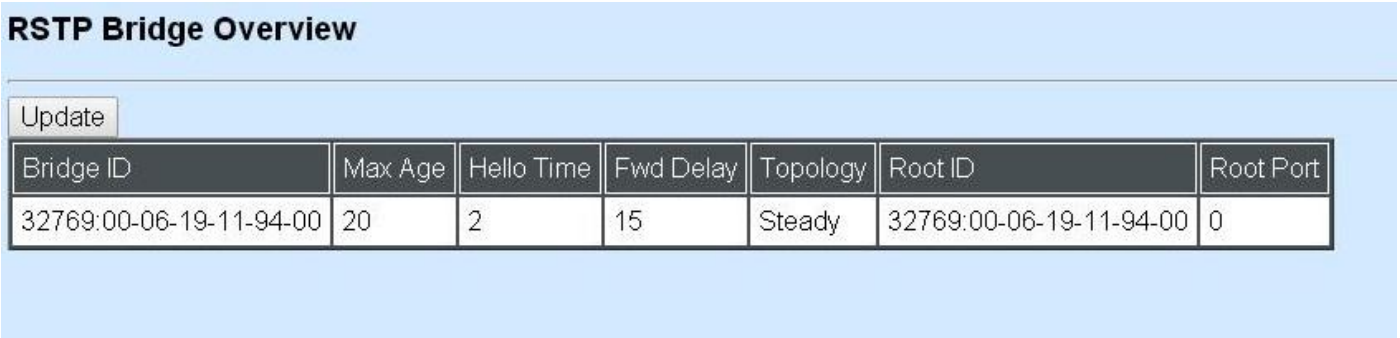
4.5.6 RSTP Monitor

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



4.5.6.1 RSTP Bridge Overview

RSTP Bridge Overview allows users to view a list of all RSTP VLANs' brief information, such as Bridge ID, topology status and Root ID. Select **RSTP Bridge Overview** from the **RSTP Monitor** menu and then the following screen page appears.



In this page, you can find the following information about RSTP bridge:

Update: Update the current status.

Bridge ID: RSTP Bridge ID of the Managed Switch

Max Age: Max Age setting of the Managed Switch.

Hello Time: Hello Time setting of the Managed Switch.

Forward Delay: The Managed Switch's setting of Forward Delay Time.

Topology: The state of the topology.

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

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

4.5.6.2 RSTP Port Status

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

RSTP Port Status

Port	Path Cost	Edge Port	P2p Port	Protocol	Role	Port State
1	0	yes	yes	RSTP	Non-STP	Non-STP
2	0	yes	yes	RSTP	Non-STP	Non-STP
3	0	yes	yes	RSTP	Non-STP	Non-STP
4	0	yes	yes	RSTP	Non-STP	Non-STP
5	0	yes	yes	RSTP	Non-STP	Non-STP
6	0	yes	yes	RSTP	Non-STP	Non-STP
7	0	yes	yes	RSTP	Non-STP	Non-STP
8	0	yes	yes	RSTP	Non-STP	Non-STP
9	0	yes	yes	RSTP	Non-STP	Non-STP
10	0	yes	yes	RSTP	Non-STP	Non-STP
11	0	yes	yes	RSTP	Non-STP	Non-STP
12	0	yes	yes	RSTP	Non-STP	Non-STP
13	0	yes	yes	RSTP	Non-STP	Non-STP

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

Port Number: The number of the port.

Path Cost: The Path Cost of the port.

Edge Port: "Yes" is displayed if the port is the Edge port connecting to an end station and does not receive BPDU.

P2p Port: "Yes" is displayed if the port link is connected to another STP device.

Protocol: Display RSTP or STP.

Role: Display the Role of the port (non-STP, forwarding or blocked).

Port State: Display the state of the port (non-STP, forwarding or blocked).

4.5.6.3 RSTP Statistics

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

RSTP Statistics

Port	RSTP Transmitted	STP Transmitted	TCN Transmitted	RSTP Recevied	STP Recevied	TCN Recevied	Illegal Recevied	Unknown Recevied
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0

Port Number: The number of the port.

RSTP Transmitted: The total transmitted RSTP packets from current port.

STP Transmitted: The total transmitted STP packets from current port.

TCN Transmitted: The total transmitted TCN (Topology Change Notification) packets from current port.

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

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

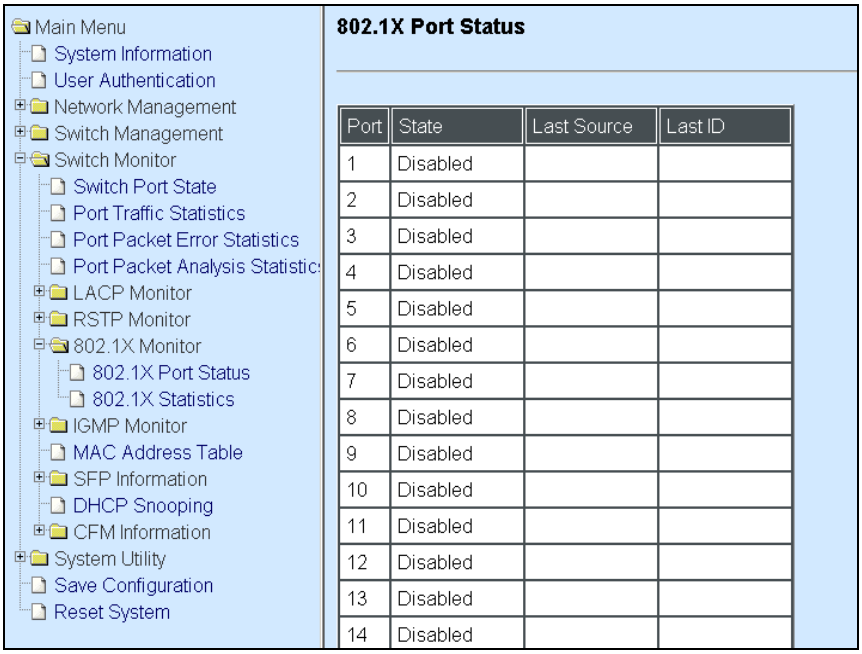
TCN Received: The total received TCN packets from current port.

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

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

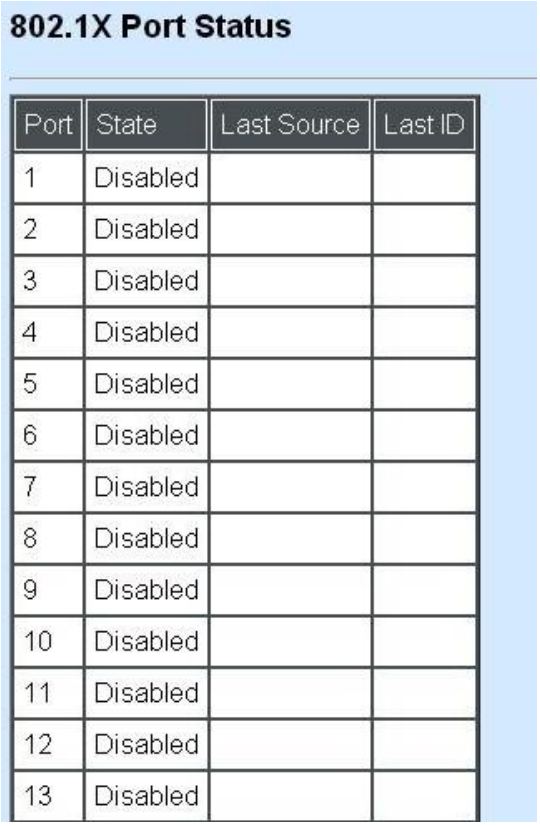
4.5.7 802.1X Monitor

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



4.5.7.1 802.1X Port Status

802.1X Port Status allows users to view a list of all 802.1x ports' information. Select **802.1X port status** from the **802.1x Monitor** menu and then the following screen page appears.



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

Port: The number of the port.

State: Display the number of the port 802.1x link state LinkDown or LinkUp.

Last Source: Display the number of the port's Last Source.

Last ID: Display the number of the port's Last ID.

4.5.7.2 802.1X Statistics

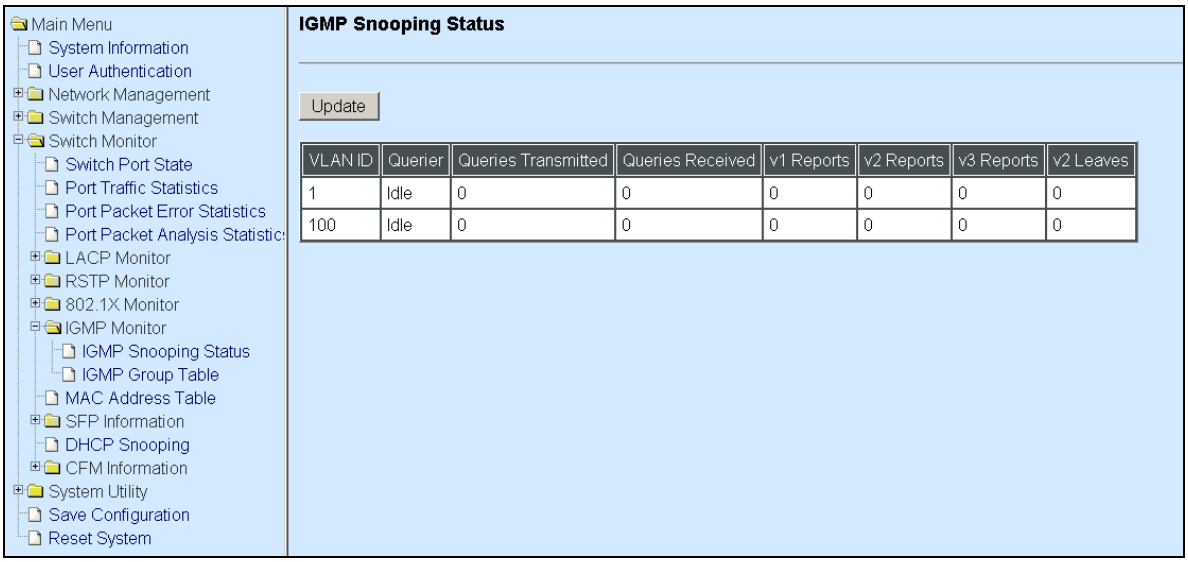
In order to view the real-time 802.1X port statistics status of the Managed Switch, select **802.1x Statistics** from the **802.1x Monitor** menu and then the following screen page shows up.

802.1X 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
1	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
3	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
5	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
7	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
9	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
11	0	0	0	0	0	0	0	0	0	0	0	0	0

4.5.8 IGMP/MLD Monitor

Click the **IGMP/MLD Monitor** folder and then the following screen page appears.



4.5.8.1 IGMP Snooping Status

IGMP Snooping Status allows users to view a list of IGMP queries' information in VLAN(s) such as VLAN ID, Querier and Queries Transmitted/Received packets. Select **IGMP Snooping Status** from the **IGMP Monitor** menu and then the following screen page appears.

Update: Click "Update" to update the table.

VLAN ID: VID of the specific VLAN

The IGMP querier periodically sends IGMP general queries to all hosts and routers (224.0.0.1) on the local subnet to find out whether active multicast group members exist on the subnet.

Upon receiving an IGMP general query, the Managed Switch forwards it through all ports in the VLAN except the receiving port.

Querier: The state of IGMP querier in the VLAN.

Queries Transmitted: The total IGMP general queries transmitted will be sent to IGMP hosts.

Queries Received: The total received IGMP general queries from IGMP querier.

v1 Reports: IGMP Version 1 reports.

v2 Reports: IGMP Version 2 reports.

v3 Reports: IGMP Version 3 reports.

v2 Leaves: IGMP Version 2 leaves.

4.5.8.2 IGMP Group Table

In order to view the real-time IGMP multicast group status of the Managed Switch, select **IGMP Group Table** from the **IGMP monitor** menu and then the following screen page appears.

Update: Click “Update” to update the table.

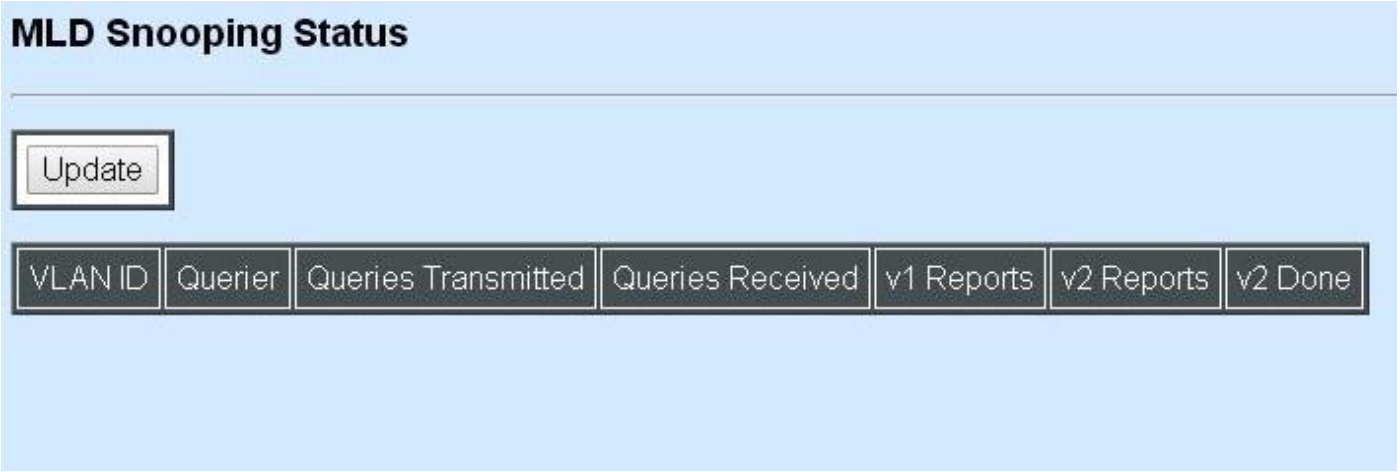
VLAN ID: VID of the specific VLAN

Group: The multicast IP address of IGMP querier.

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

4.5.8.3 MLD Snooping Status

MLD Snooping Status allows users to view a list of IGMP queries’ information in VLAN(s) such as VLAN ID, Querier and Queries Transmitted/Received packets. Select **MLD Snooping Status** from the **IGMP/MLD Monitor** menu and then the following screen page appears.



Update: Click “Update” to update the table.

VLAN ID: VID of the specific VLAN

Queries Transmitted: The total IGMP general queries transmitted will be sent to IGMP hosts.

Queries Received: The total received IGMP general queries from IGMP querier.

v1 Reports: IGMP Version 1 reports.

v2 Reports: IGMP Version 2 reports.

v2 Done: IGMP Version 2 dones

4.5.8.4 MLD Group Table

In order to view the real-time IGMP multicast group status of the Managed Switch, select **MLD Group Table** from the **IGMP/MLD monitor** menu and then the following screen page appears.

Update: Click “Update” to update the table.

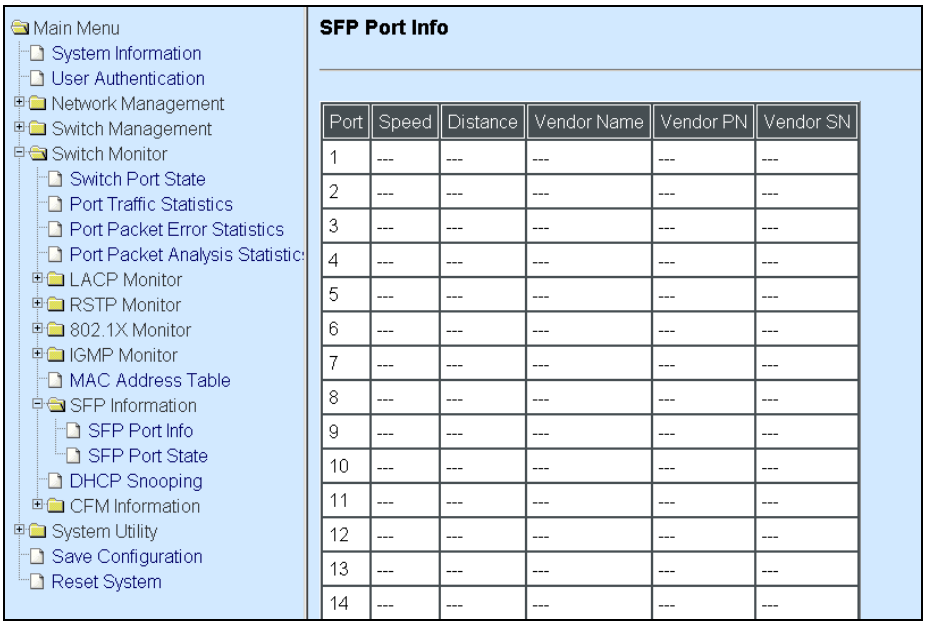
VLAN ID: VID of the specific VLAN

Group: The multicast IP address of IGMP querier.

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

4.5.9 SFP Information

Click the **SFP Information** folder and then the following screen page appears.



4.5.9.1 SFP Port Info

SFP Port Info displays each port’s slide-in SFP Transceiver information e.g. Speed, Length, Vendor Name, Vendor PN, Vendor SN, and detection Temperature, Voltage , TX Bias, etc.. Select **SFP Port Info** from the **SFP Information** menu and then the following screen page appears.

SFP Port Info

Port	Speed	Distance	Vendor Name	Vendor PN	Vendor SN
1	-----	-----	-----	-----	-----
2	-----	-----	-----	-----	-----
3	-----	-----	-----	-----	-----
4	-----	-----	-----	-----	-----
5	-----	-----	-----	-----	-----
6	-----	-----	-----	-----	-----
7	-----	-----	-----	-----	-----
8	-----	-----	-----	-----	-----
9	-----	-----	-----	-----	-----
10	-----	-----	-----	-----	-----
11	-----	-----	-----	-----	-----
12	-----	-----	-----	-----	-----
13	-----	-----	-----	-----	-----

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.

4.5.9.2 SFP Port State

Select **SFP Port Status** from the **SFP Information** menu and then the following screen page appears.

SFP Port State

Port	Temperature(C)	Voltage(V)	TX Bias(mA)	TX Power(dbm)	RX Power(dbm)
1	-----	-----	-----	-----	-----
2	-----	-----	-----	-----	-----
3	-----	-----	-----	-----	-----
4	-----	-----	-----	-----	-----
5	-----	-----	-----	-----	-----
6	-----	-----	-----	-----	-----
7	-----	-----	-----	-----	-----
8	-----	-----	-----	-----	-----
9	-----	-----	-----	-----	-----
10	-----	-----	-----	-----	-----
11	-----	-----	-----	-----	-----
12	-----	-----	-----	-----	-----
13	-----	-----	-----	-----	-----

Port Number: The number of the SFP module slide-in port.

Temperature (C): The Slide-in SFP module operation temperature.

Voltage (V): The Slide-in SFP module operation voltage.

TX Bias (mA): The Slide-in SFP module operation current.

TX Power (dbm): The Slide-in SFP module optical Transmission power.

RX Power (dbm): The Slide-in SFP module optical Receiver power.

4.5.10 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.

DHCP Snooping Table

Update

Index	CliPort	SrvPort	VID	CliIPAddr	CliMACAddr	SrvIPAddr	TimeLeft

Update: Click “Update” to update the DHCP snooping table.

Cli Port: View-only field that shows where the DHCP client binding port is.

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

CliIP Addr: View-only field that shows client IP address.

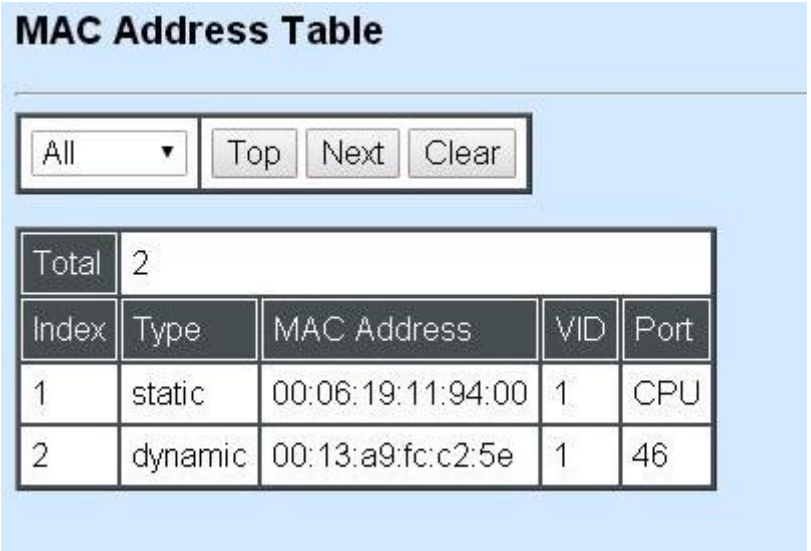
Cli MAC Addr: View-only field that shows client MAC address.

SrvIPAddr: View-only field that shows DHCP server IP address.

TimeLeft: View-only field that shows DHCP client lease time.

4.5.11 MAC Address Table

MAC Address Table displays MAC addresses learned when System Reset and MAC Address Learning are 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.

4.5.12 LLDP Status

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

LLDP Status

Update

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

Click **"Update"** to refresh LLDP Status table.

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

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

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

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

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

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

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

4.5.13 Loop Detection Status

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

Loop Detection Status

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

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.

4.5.14 IEEE 802.1q Tag VLAN Table

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

IEEE 802.1q Tag VLAN Table

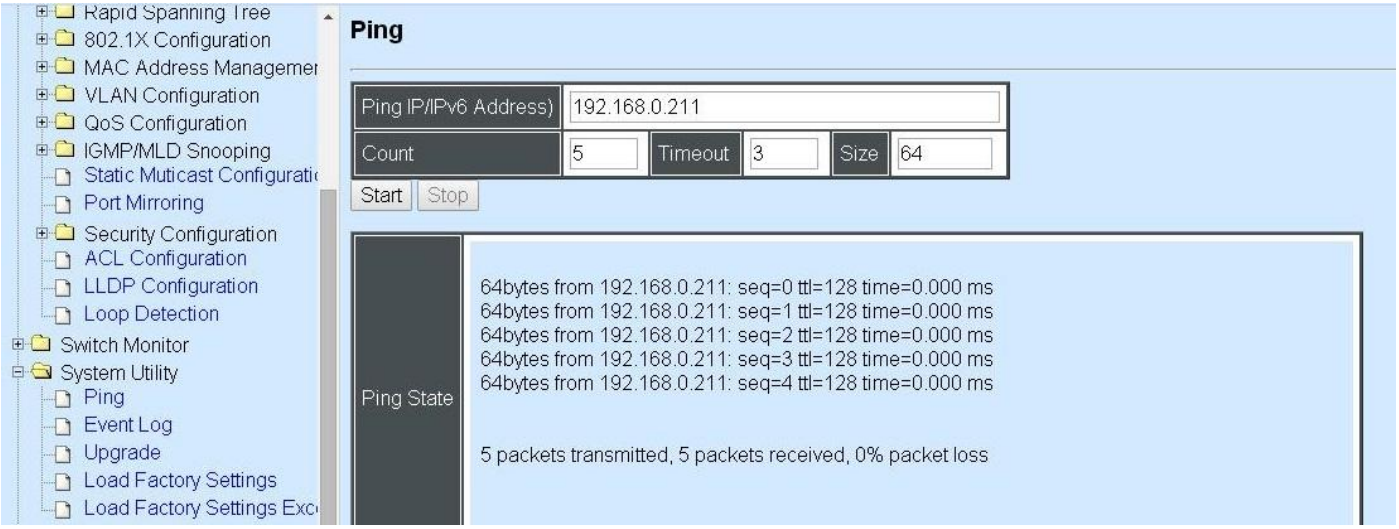
VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Default_VLAN	1	V	V	V	-	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
	130	-	-	-	V	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

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

VID: View-only filed that shows the VID.

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.

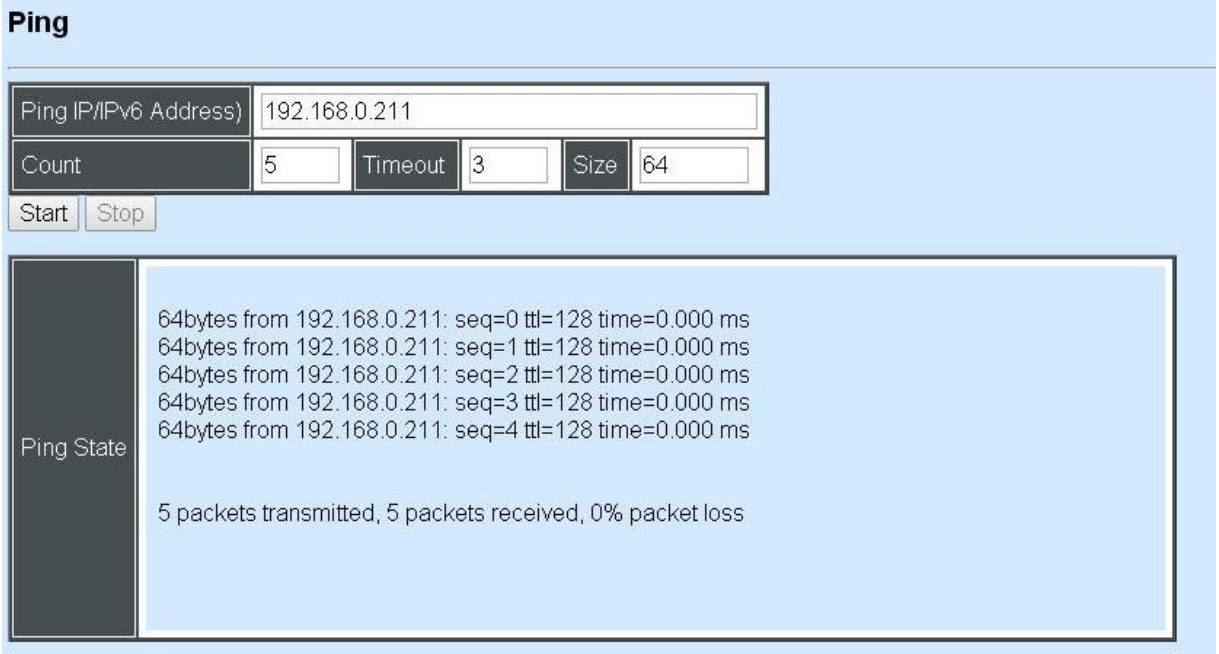
3. **Upgrade:** This allows users to update the latest firmware, save current configuration or restore previous configuration to the Managed Switch.

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

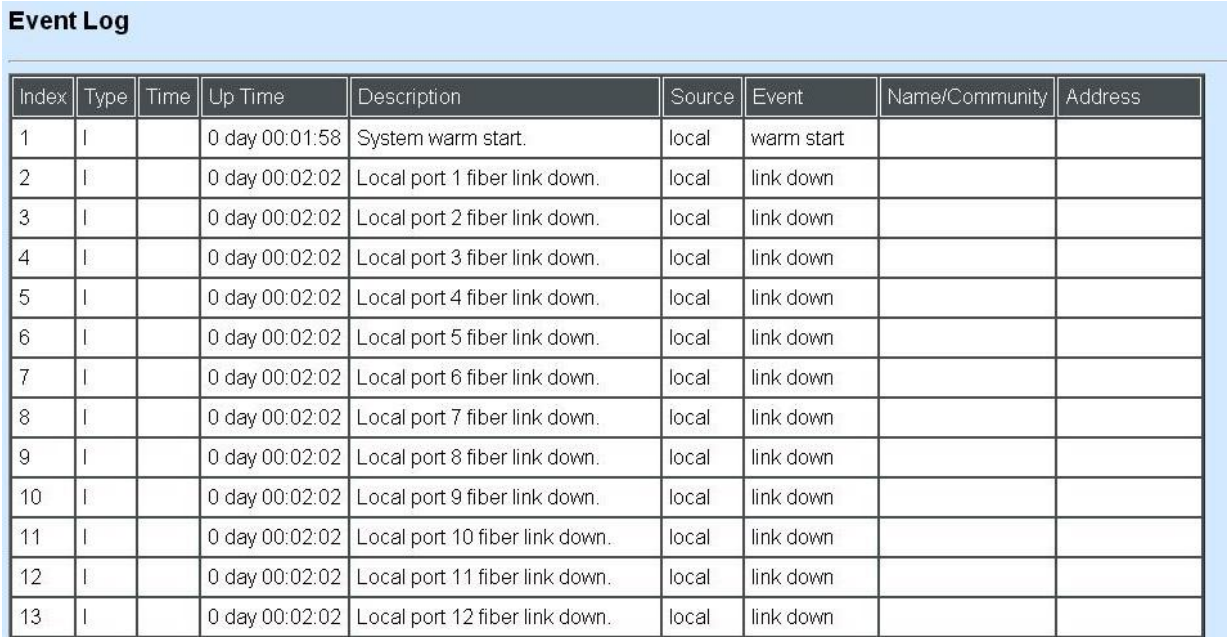
Ping can help you test the network connectivity between the Managed Switch and the host.
Select **Ping** from the **System Utility** menu and then the following screen page appears.



You can also specify count s, timeout and size of the Ping packets.
Click **Start** to start the Ping process.

4.6.2 Event Log

Event log keep a record of user login and logout timestamp information. Select **Event Log** from the **System Utility** menu and then the following screen page appears.



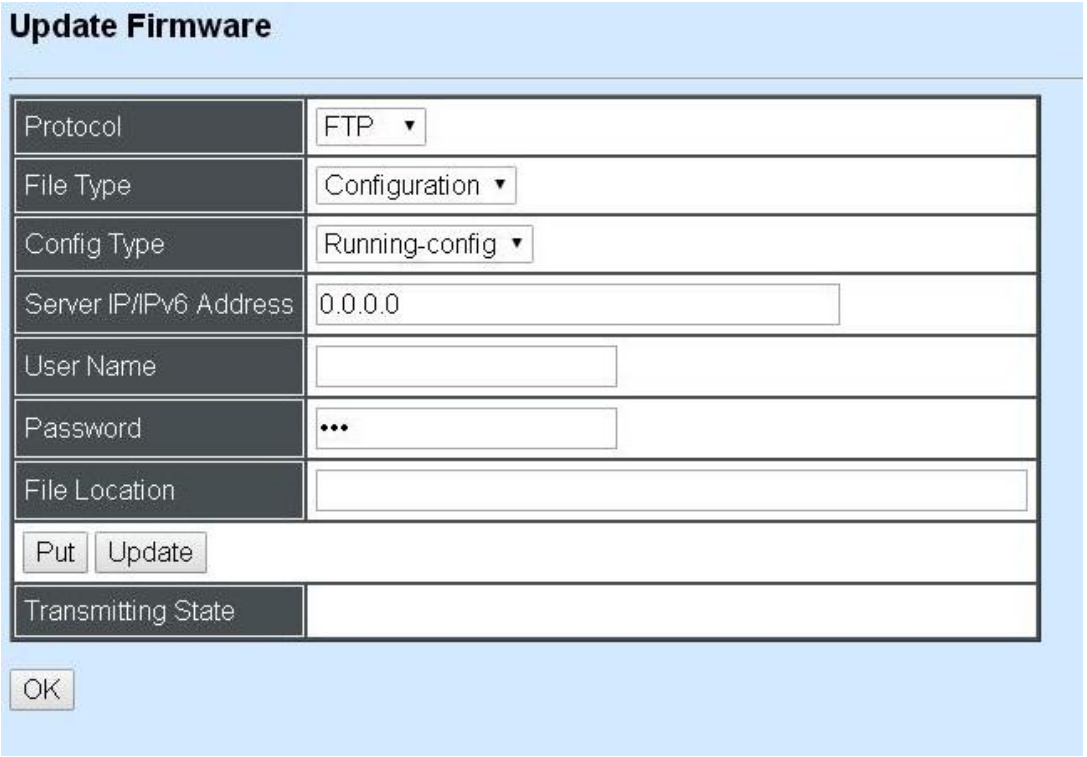
Event Log

Index	Type	Time	Up Time	Description	Source	Event	Name/Community	Address
1	I		0 day 00:01:58	System warm start.	local	warm start		
2	I		0 day 00:02:02	Local port 1 fiber link down.	local	link down		
3	I		0 day 00:02:02	Local port 2 fiber link down.	local	link down		
4	I		0 day 00:02:02	Local port 3 fiber link down.	local	link down		
5	I		0 day 00:02:02	Local port 4 fiber link down.	local	link down		
6	I		0 day 00:02:02	Local port 5 fiber link down.	local	link down		
7	I		0 day 00:02:02	Local port 6 fiber link down.	local	link down		
8	I		0 day 00:02:02	Local port 7 fiber link down.	local	link down		
9	I		0 day 00:02:02	Local port 8 fiber link down.	local	link down		
10	I		0 day 00:02:02	Local port 9 fiber link down.	local	link down		
11	I		0 day 00:02:02	Local port 10 fiber link down.	local	link down		
12	I		0 day 00:02:02	Local port 11 fiber link down.	local	link down		
13	I		0 day 00:02:02	Local port 12 fiber link down.	local	link down		

Click **Clear** to clear all Event log records.

4.6.3 Upgrade

The Managed Switch has both built-in TFTP and FTP clients. Users may save or restore their configuration and update their Firmware on-line. Select **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 file to process, either Firmware or Configuration.

Upgrade Image Option: Choose Image1 or Image2 which the firmware will be upgraded to.

Config Type: Choose “Running-config”, “Default-config” or “Start-up-config” which the config file will be saved or restored to

Server IP/IPv6 Address: Enter the specific IP/IPv6 address of the File Server.

User Name: Enter the specific username to access the File Server.

Password: Enter the specific password to access the File Server.

File Location: Enter the specific path and filename within the File Server.
Click **OK** 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.

Click **Stop** to abort the current operation.

Select **Update** then press **Enter** to instruct the Managed Switch to update existing firmware/configuration to the latest firmware/configuration received. After a successful update, a message will pop up. The Managed Switch will need a reset to make changes effective.

4.6.4 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.

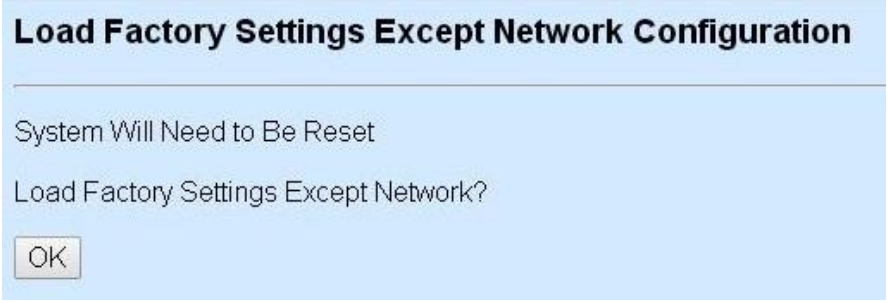
Select **Load Factory Setting** from the **System Utility** menu and then the following screen page appears.

Click **OK** to start loading factory settings.

4.6.5 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.

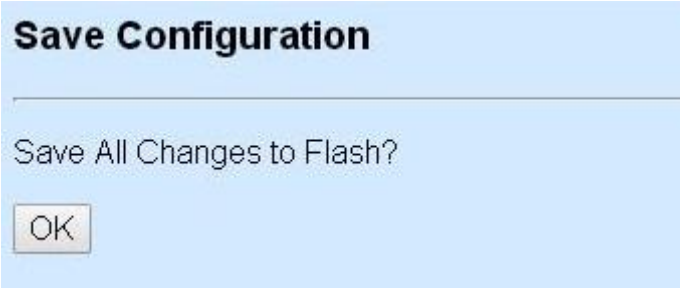
Select **Load Factory Setting Except Network Configuration** from the **System Utility** menu, the following screen page shows up.



Click **OK** to start loading factory settings except network configuration.

4.7 Save Configuration

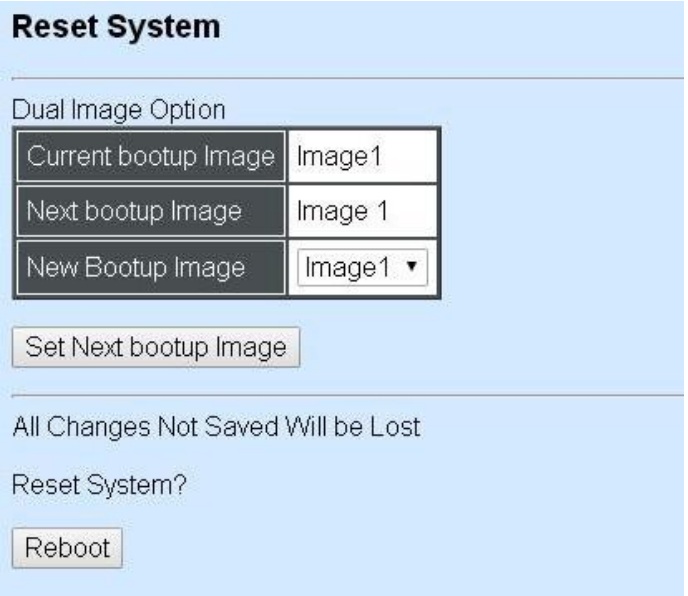
In order to save configuration setting permanently, users need to save configuration first before resetting the Managed Switch. Select **Save Configuration** from the Console main menu and then the following screen page appears.



Click **OK** to save the configuration.

4.8 Reset System

After any configuration change, **Reset System** can make it effective. Select **Reset System** from the Console main menu and then the following screen page appears.



Click **Set Next bootup Image** to change the boot-up image if needed.
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

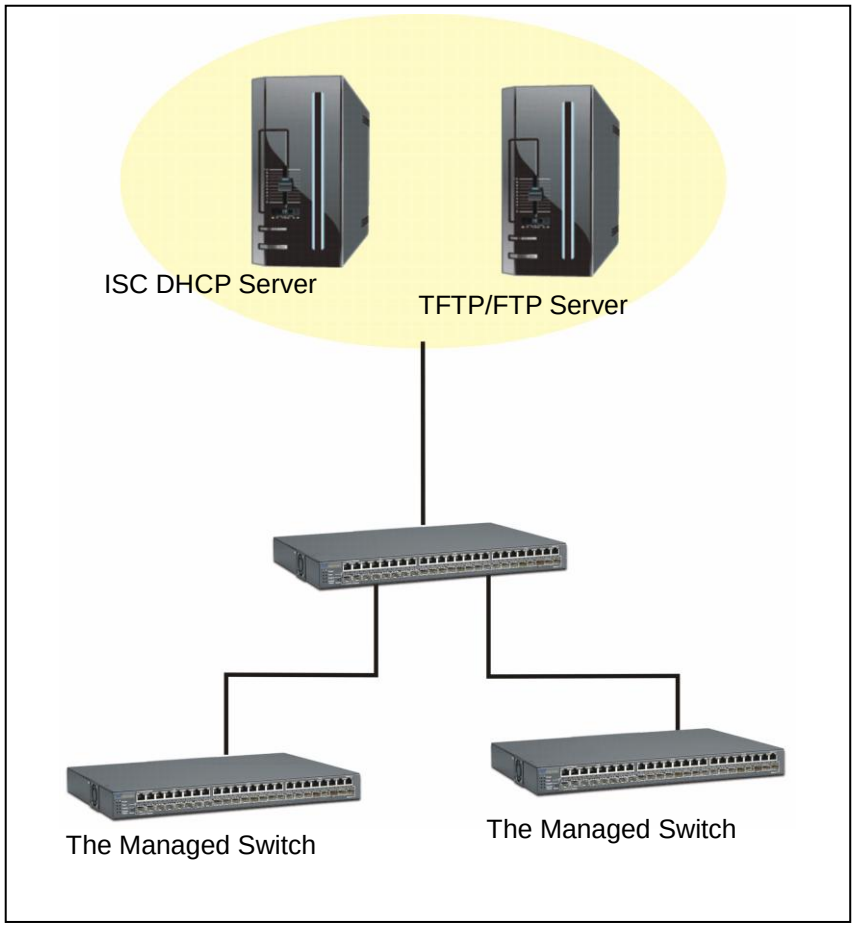
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the Managed Switch that you purchased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

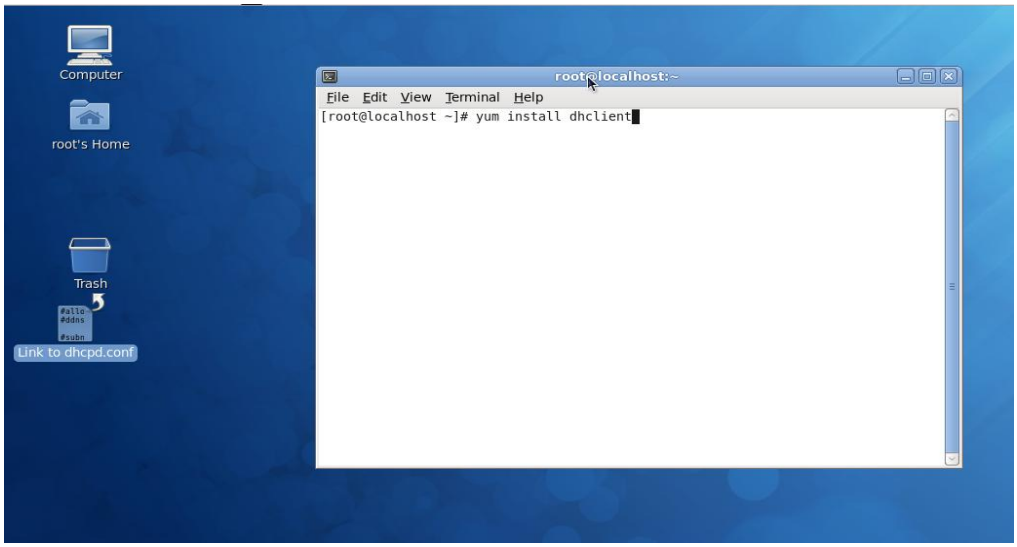
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Topology Example

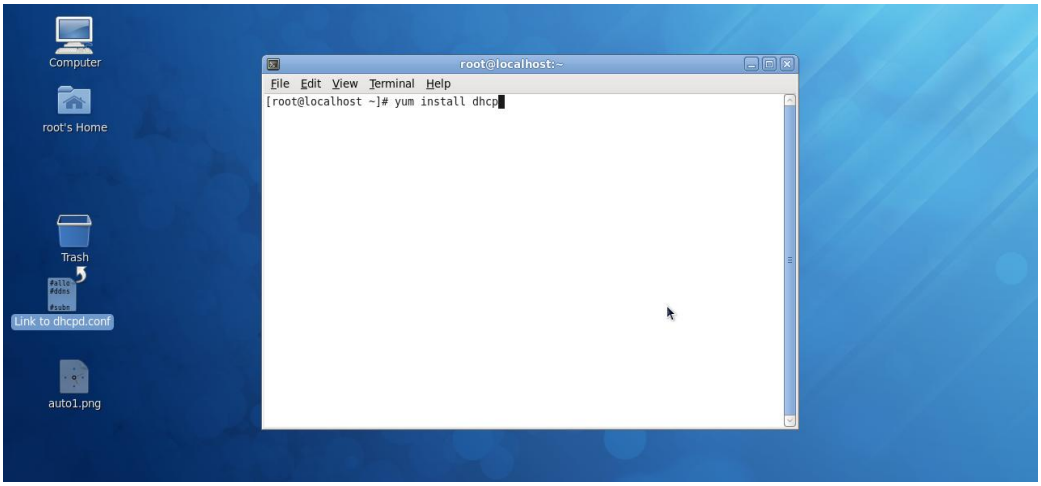
Step 2. Set up Auto Provision Server

- **Update DHCP Client**



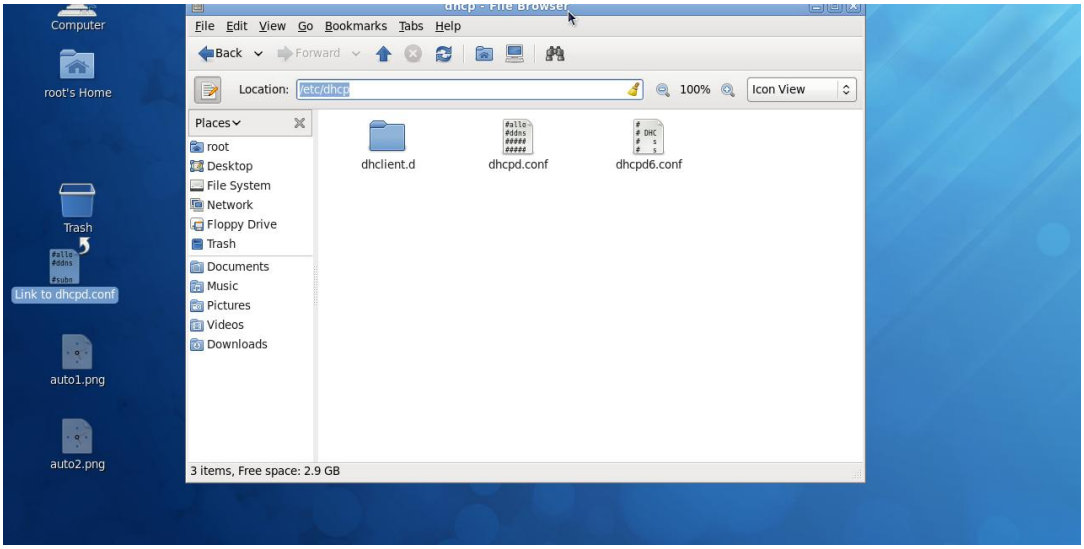
Linux Fedora 12 supports “yum” function by default. First of all, update DHCP client function by issuing “yum install dhclient” command.

- **Install DHCP Server**



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

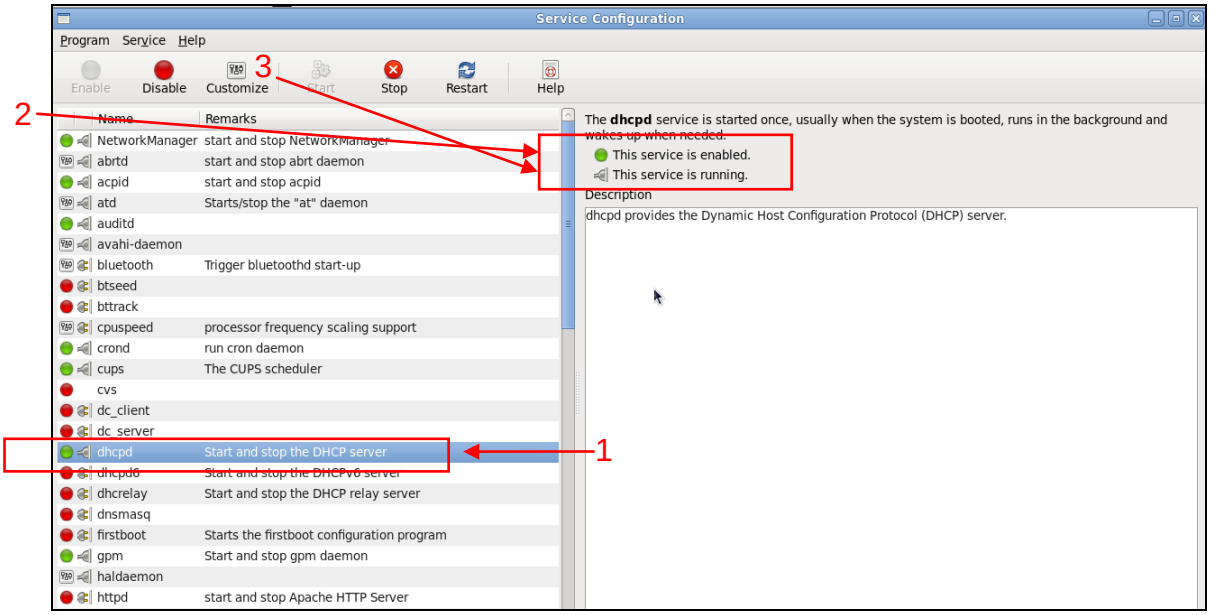
- **Copy dhcpd.conf to /etc/dhcp/ directory**



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

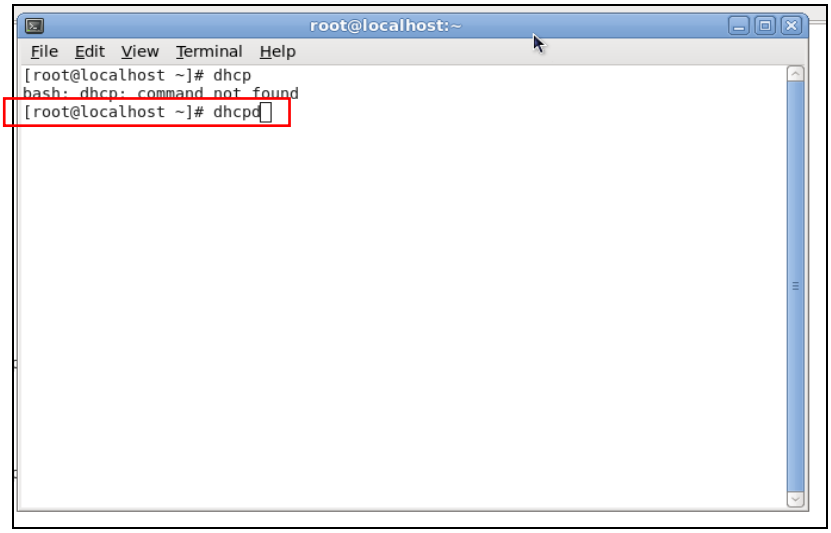
Please note that each vendor has their own way to define auto provisioning. Make sure to use the file provided by the vendor.

- **Enable and run DHCP service**



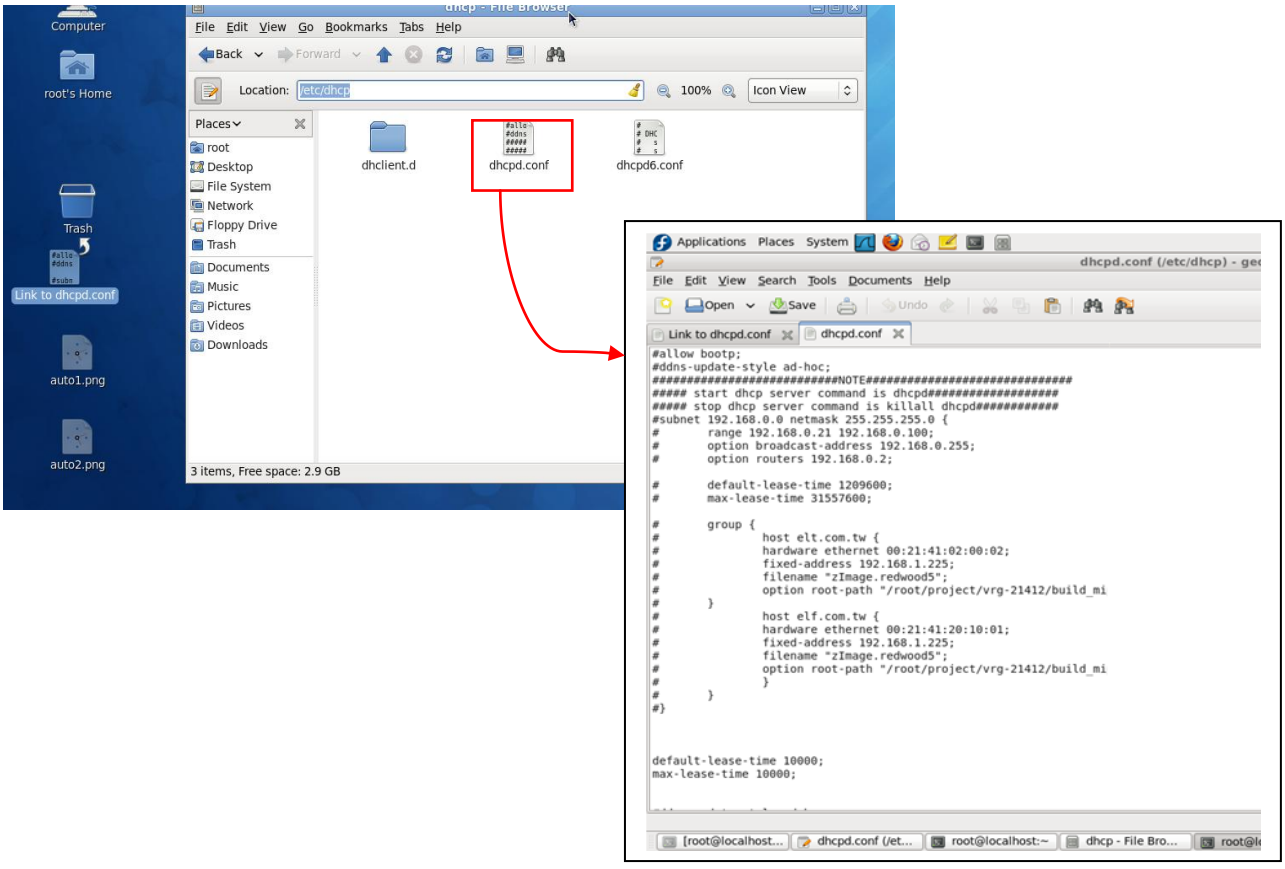
1. Choose dhcpd.
2. Enable DHCP service.
3. Start running DHCP service.

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.

```
default-lease-time 10000;
max-lease-time 10000;                                   → 1

#ddns-update-style ad-hoc;
ddns-update-style interim;

subnet 192.168.0.0 netmask 255.255.255.0 {
        range 192.168.0.118 192.168.0.230;
    option subnet-mask   255.255.255.0;
        option broadcast-address 192.168.0.255;
        option routers 192.168.0.251;                   → 2
    option domain-name-servers 168.95.1.1, 168.95.192.1;

host FAE {
   hardware ethernet 00:06:19:03:A2:40;                 → 3
   fixed-address 192.168.0.118;

   }
host HS-0600 {
   hardware ethernet 00:06:19:65:18:FE;                 → 4
   fixed-address 192.168.0.1;

   }

}
```

1. Define DHCP default and maximum lease time in seconds.

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

   Maximum lease time: This is the maximum length of time that the server will lease for.

2. Define subnet, subnet mask, IP range, broadcast address, router address and DNS server address.

3. Map a host's MAC address to a fixed IP address.

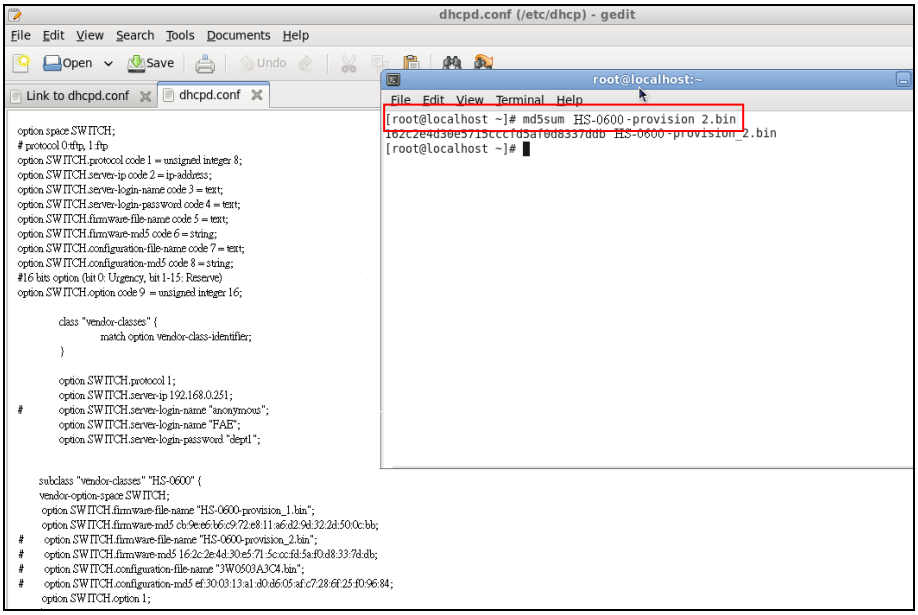
4. Map a host's MAC address to a fixed IP address. Use the same format to create multiple MAC-to-IP address bindings.

```
option space SWITCH;                                                    5
# protocol 0:tftp, 1:ftp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
option SWITCH.server-login-password code 4 = text;
option SWITCH.firmware-file-name code 5 = text;
option SWITCH.firmware-md5 code 6 = string;
option SWITCH.configuration-file-name code 7 = text;
option SWITCH.configuration-md5 code 8 = string;
#16 bits option (bit 0: Urgency, bit 1-15: Reserve)
option SWITCH.option code 9  = unsigned integer 16;

        class "vendor-classes" {
                match option vendor-class-identifier;
        }

        option SWITCH.protocol 1;                                       6
        option SWITCH.server-ip 192.168.0.251;                          7
#       option SWITCH.server-login-name "anonymous";                    8
        option SWITCH.server-login-name "FAE";
        option SWITCH.server-login-password "dept1";                    9

    subclass "vendor-classes" "HS-0600" {                               10
    vendor-option-space SWITCH;
     option SWITCH.firmware-file-name "HS-0600-provision_1.bin";        11
     option SWITCH.firmware-md5 cb:9e:e6:b6:c9:72:e8:11:a6:d2:9d:32:2d:50:0c:bb;   12
#     option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
#     option SWITCH.firmware-md5 16:2c:2e:4d:30:e5:71:5c:cc:fd:5a:f0:d8:33:7d:db;
#     option SWITCH.configuration-file-name "3W0503A3C4.bin";           13
#     option SWITCH.configuration-md5 ef:30:03:13:a1:d0:d6:05:af:c7:28:6f:25:f0:96:84;   14
     option SWITCH.option 1;
    }
```

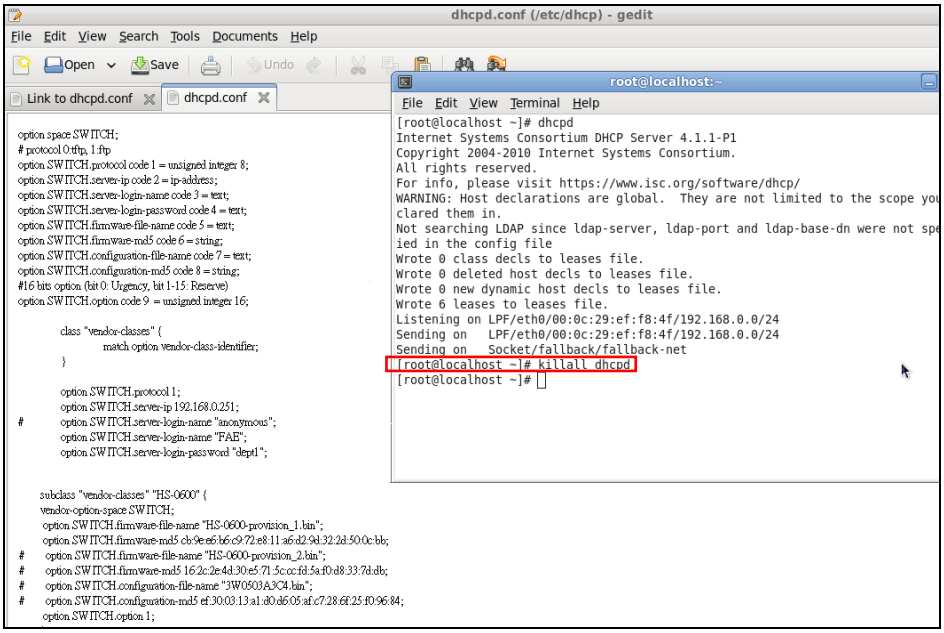
5. This value is configurable and can be defined by users.
6. Specify the protocol used (Protocol 1: FTP; Protocol 0: TFTP).
7. Specify the FTP or TFTP IP address.
8. Login TFTP server anonymously (TFTP does not require a login name and password).
9. Specify FTP Server login name and password.
10. Specify the product model name.
11. Specify the firmware filename.
12. Specify the MD5 for firmware image.
13. Specify the configuration filename.
14. Specify the MD5 for configuration file.

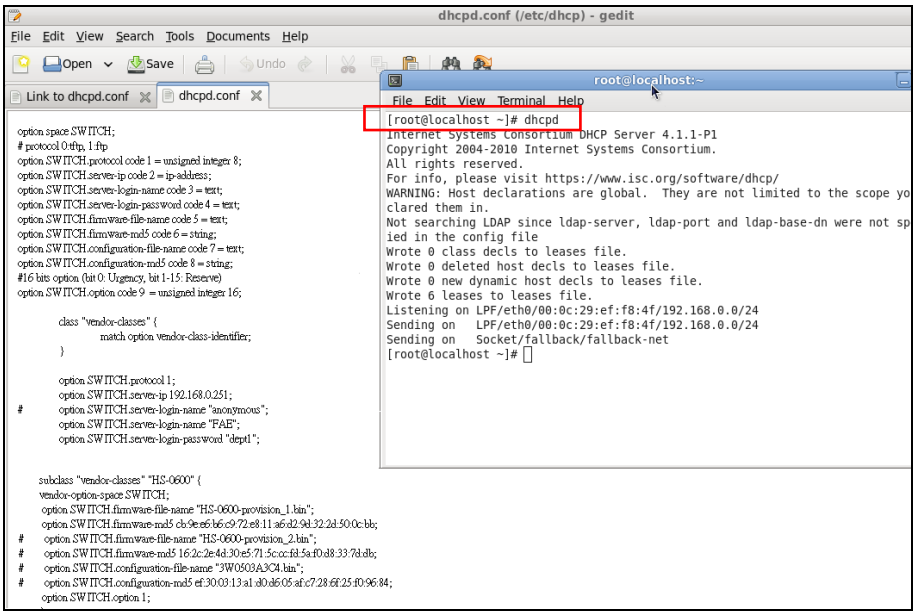
NOTE 1: *The text beginning with a pound sign (#) will be ignored by the DHCP server. For example, in the figure shown above, firmware-file-name "HS-0600-provision_2.bin" and firmware-md5 (line 5 & 6 from the bottom) will be ignored. If you want DHCP server to process these two lines, remove pound signs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

NOTE 2: *You can use either free software program or Linux default md5sum function to get MD5 checksum for firmware image and configuration file.*



- **Restart DHCP service**





Every time when you modify dhcpd.conf file, DHCP service must be restarted. Issue “killall dhcpd” command to disable DHCP service and then issue “dhcpd” command to enable DHCP service.

Step 4. Backup a Configuration File

Before preparing a configuration file in TFTP/FTP Server, make sure the device generating the configuration file is set to **“Get IP address from DHCP”** assignment. This is because that DHCP Auto-provisioning is running under DHCP mode, so if the configuration file is uploaded by the network type other than DHCP mode, the downloaded configuration file has no chance to be equal to DHCP when provisioning, and it results in MD5 never matching and causing the device to reboot endless.

In order for your Managed Switch to retrieve the correct configuration image in TFTP/FTP Server, please make sure the filename of your configuration file is defined exactly the same as the one specified in in **dhcpd.conf**. For example, if the configuration image’s filename specified in dhcpd.conf is “metafile”, the configuration image filename should be named to “metafile” as well.

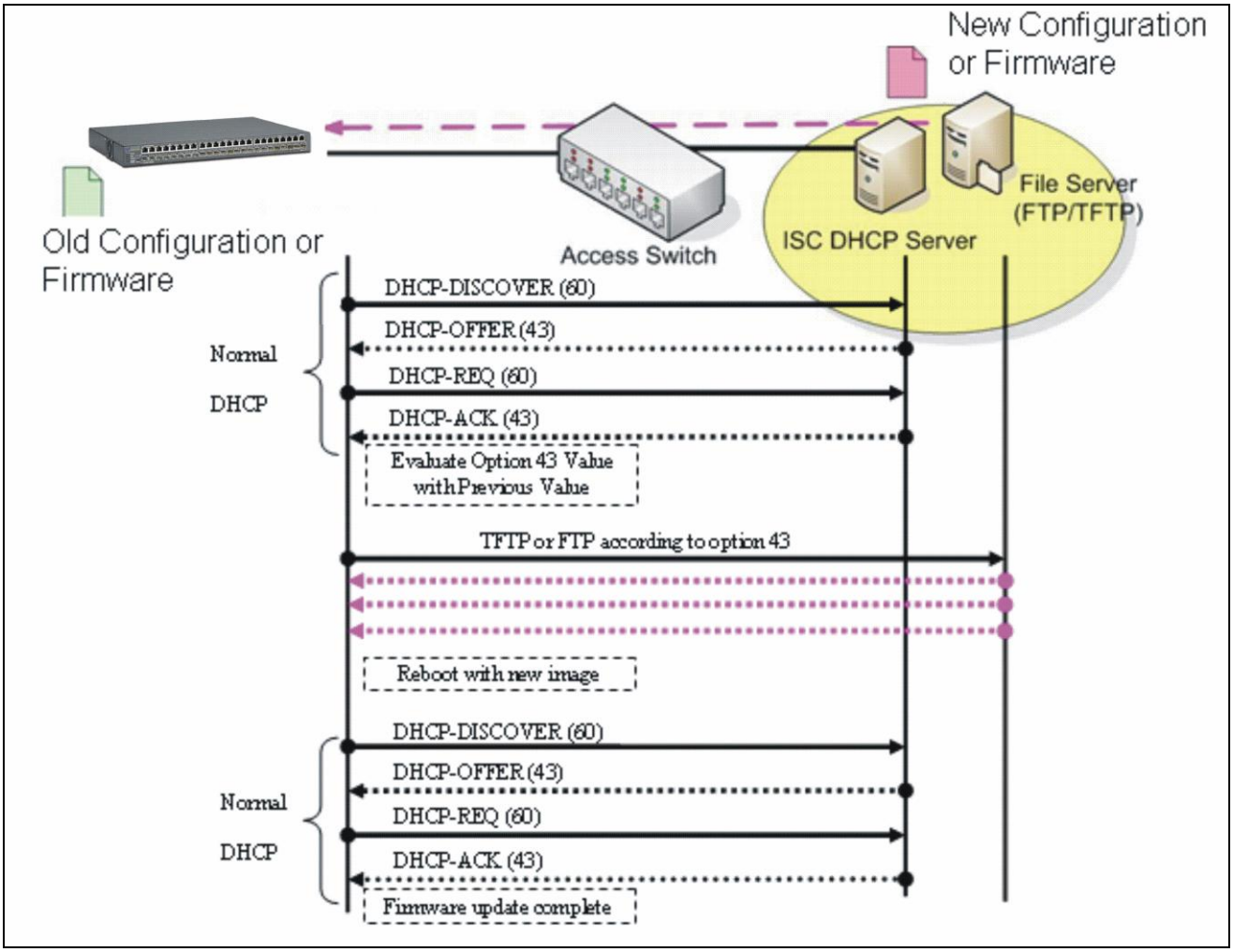
Step 5. Place a copy of Firmware and Configuration File in TFTP/FTP

The TFTP/FTP File server should include the following items:
1. Firmware image (This file is provided by the vendor.)
2. Configuration file (This file is generally created by users.)
3. User account for your device (For FTP server only.)

B. Auto-Provisioning Process

This switching device is setting-free (through auto-upgrade and configuration) and its upgrade procedures are as follows:

1. The ISC DHCP server will recognize the device whenever it sends an IP address request to it, and it will tell the device how to get a new firmware or configuration.
2. The device will compare the firmware and configuration MD5 code form of DHCP option every time when it communicates with DHCP server.
3. If MD5 code is different, the device will then upgrade the firmware or configuration. However, it will not be activated right after.
4. If the Urgency Bit is set, the device will be reset to activate the new firmware or configuration immediately.
5. The device will retry for 3 times if the file is incorrect, and then it gives up until getting another DHCP ACK packet again.



APPENDIX C: VLAN Application Note

Overview

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

Generally, end nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. In this way, the use of VLANs can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another VLAN. This allows VLAN to accommodate network moves, changes and additions with the utmost flexibility.

The Managed Switch supports Port-based VLAN implementation and IEEE 802.1Q standard tagging mechanism that enables the switch to differentiate frames based on a 12-bit VLAN ID (VID) field. Besides, the Managed Switch also provides double tagging function. The IEEE 802.1Q double tagging VLAN is also referred to Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1Q VLAN space by tagging the inner tagged packets. In this way, a "double-tagged" frame is created so as to separate customer traffic within a service provider network. Moreover, the addition of double-tagged space increases the number of available VLAN tags which allow service providers to use a single SP-VLAN (Service Provider VLAN) tag per customer over the Metro Ethernet network.

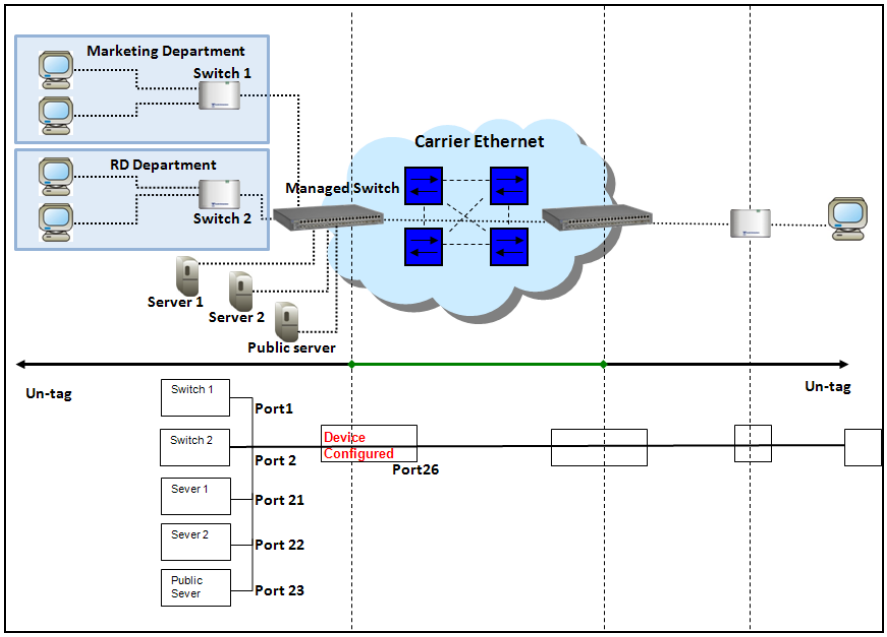
While this application note can not cover all of the real-life applications that are possible on this Managed Switch, it does provide the most common applications largely deployed in most situations. In particular, this application note provides a couple of network examples to help users implement Port-Based VLAN, Data VLAN, Management VLAN and Double-Tagged VLAN. Step-by-step configuration instructions using CLI and Web Management on setting up these examples are also explained. Examples described below include:

Examples	Configuration Procedures	
I. Port-Based VLAN	CLI	WEB
II. Data VLAN	CLI	WEB
III. Management VLAN	CLI	WEB
IV. Q-in-Q	CLI	WEB

I. Port-Based VLAN

Port-Based VLAN is uncomplicated in implementation and is useful for network administrators who wish to quickly and easily set up VLANs to isolate the effect of broadcast packets on their network. In the network diagram provided below, the network administrator is required to set up VLANs to separate traffic based on the following design conditions:

- Switch 1 is used in the Marketing Department to provide network connectivity to client PCs or other workstations. Switch 1 also connects to Port 1 in Managed Switch.
- Client PCs in the Marketing Department can access the Server 1 and Public Server.
- Switch 2 is used in the RD Department to provide network connectivity to Client PCs or other workstations. Switch 2 also connects to Port 2 in Managed Switch.
- Client PCs in the RD Department can access the Server 2 and Public Server.
- Client PCs in the Marketing and RD Department can access the Internet.



Port-Based VLAN Network Diagram

Based on design conditions described above, port-based VLAN assignments can be summarized in the table below.

VLAN Name	Member ports
Marketing	1, 21, 23, 26
RD	2, 22, 23, 26

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 26 to configure.	`SWH(config)# interface 1,21,23,26` `SWH(config-if-1,21,23,26)#`
4. Assign the ports to the port-based VLAN “Marketing”.	`SWH(config-if-1,21,23,26)# vlan port-based Marketing` `OK !`

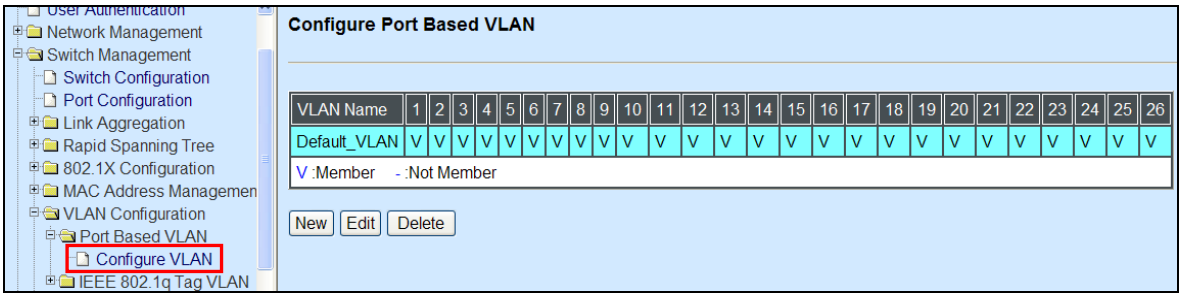
5. Return to Global Configuration mode, and select port 2, 22, 23 and 26 to configure.	`SWH(config-if-1,21,23,26)# exit`
	`SWH(config)# interface 2,22,23,26`
	`SWH(config-if-2,22,23,26)#`

6. Assign the ports to the port-based VLAN “RD”.	`SWH(config-if-2,22,23,26)# vlan port-based RD` `OK !`

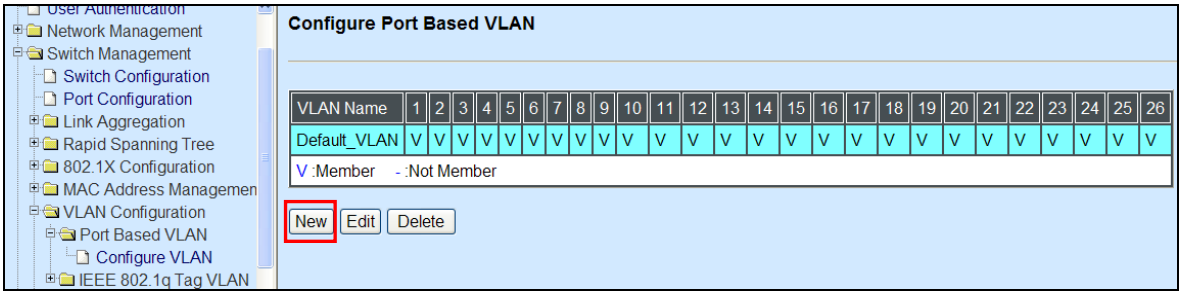
7. Return to Global Configuration mode, and show currently configured port-based VLAN membership.	`SWH(config-if-2,22,23,26)# exit`
	`SWH(config)# show vlan port-based`
	`==========`
	`Port Based VLAN :`
	`==========`
	`Index VLAN Name 1 8 9 16 17 24 25 26`
	`----- ---------- -------- -------- -------- -- --`
	`1 Default_VLAN VVVVVVVV VVVVVVVV VVVVVVVV V V`
	`2 Marketing V------- -------- ----V-V- - V`
	`3 RD -V------ -------- -----VV- - V`
	
	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.

Web Management Configuration:

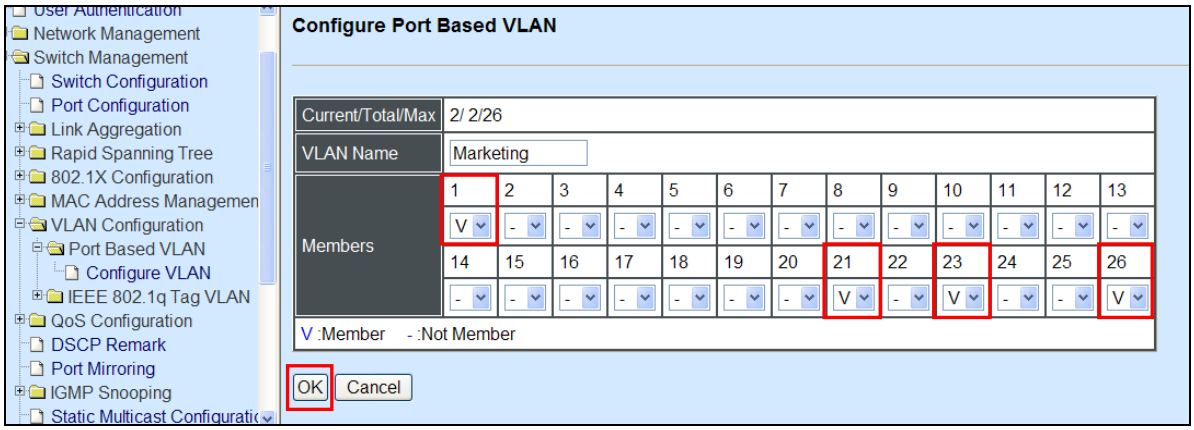
1. **Select “Configure VLAN” option in Port Based VLAN menu.**
   Switch Management>VLAN Configuration>Port Based VLAN>Configure VLAN



2. **Click “New” to add a new Port-Based VLAN**
   Switch Management>VLAN Configuration>Port Based VLAN>Configure VLAN

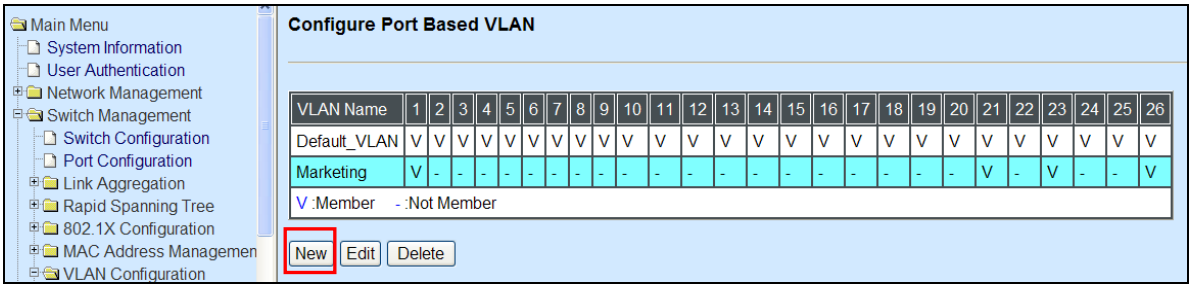


3. Add Port 1, 21, 23 and 26 in a group and name it to "Marketing".
Switch Management>VLAN Configuration>Port Based VLAN>Configure VLAN

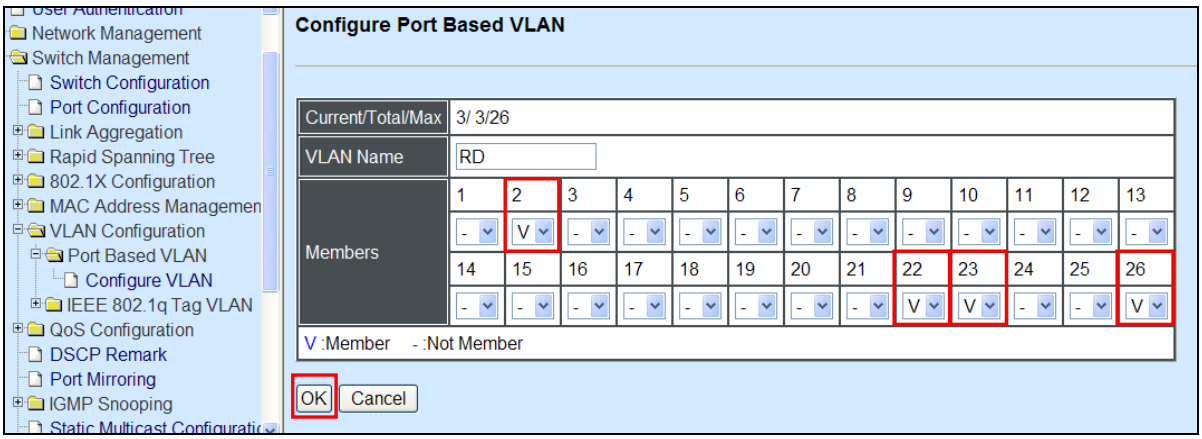


Click "OK" to apply the settings.

4. Click "New" to add a new Port-Based VLAN
Switch Management>VLAN Configuration>Port Based VLAN>Configure VLAN

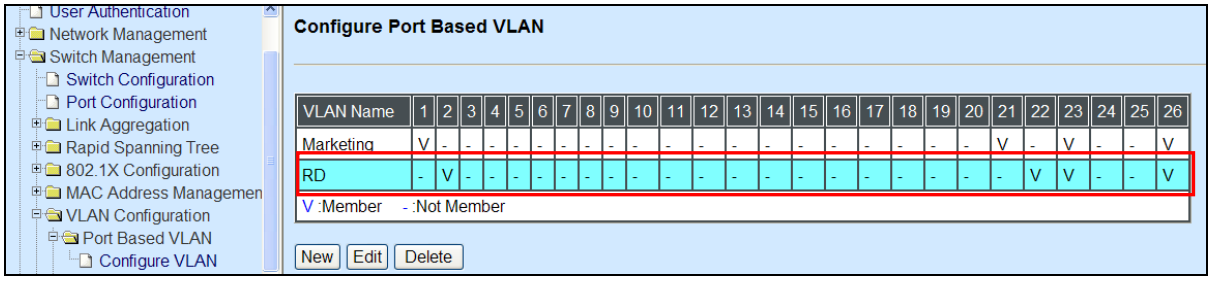


5. Add Port 2, 22, 23 and 26 in a group and name it to "RD".
Switch Management>VLAN Configuration>Port Based VLAN>Configure VLAN



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 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 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 26.

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 26.

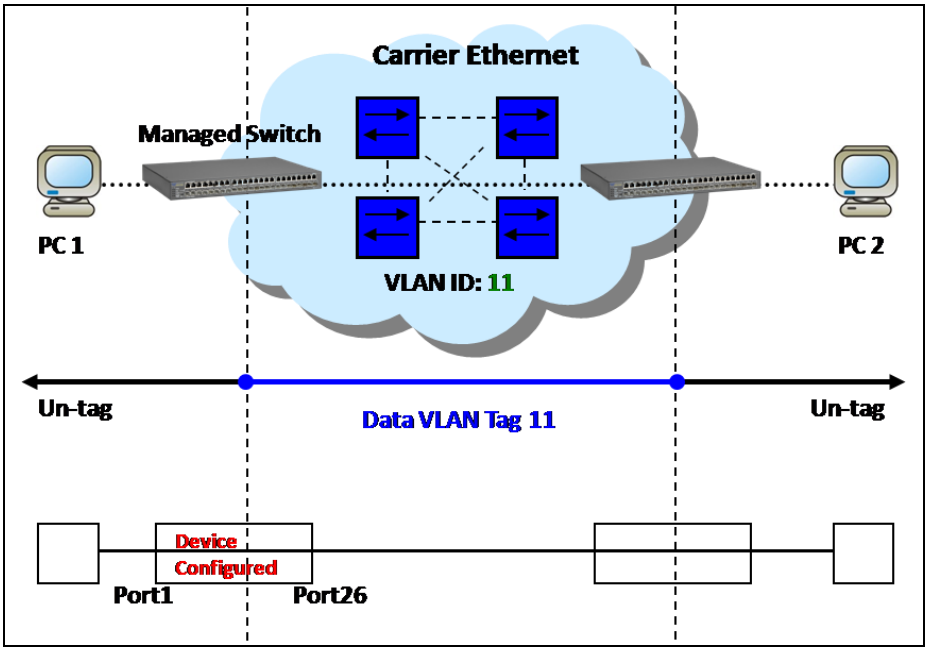
3. A tagged packet with any permissible VID arrives at Port 1
Tagged packets received on the Managed Switch will be forwarded out tagged. Therefore, in this example, the Managed Switch will look at the Port-Based forwarding table for Port 1 and forward tagged packets to member port 21, 23, and 26.

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 26.

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.	`SWH(config)# vlan dot1q-vlan 11` `OK !`

3. Name VLAN 11 to Data_VLAN.	`SWH(config-vlan-11)# name Data_VLAN`
	`OK !`
	`SWH(config-vlan-11)# exit`

4. Assign Port 1 and Port 26 to VLAN 11.	`SWH(config)# interface 1,26`
	`SWH(config-if-1,26)# vlan dot1q-vlan trunk-vlan 11`
	`OK !`

5. Show currently configured dot1q VLAN membership.	`SWH(config)# show vlan dot1q-vlan`
	`==========`
	`IEEE 802.1q Tag VLAN :`
	`==========`
	`CPU VLAN ID : 1`
	`VLAN Name VLAN 1 8 9 16 17 24 25 26 CPU`
	`---------- --- -------- -------- -------- -- -- ---`
	`Default_VLAN 1 VVVVVVVV VVVVVVVV VVVVVVVV V V V`
	`Data_VLAN 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 PVID configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.

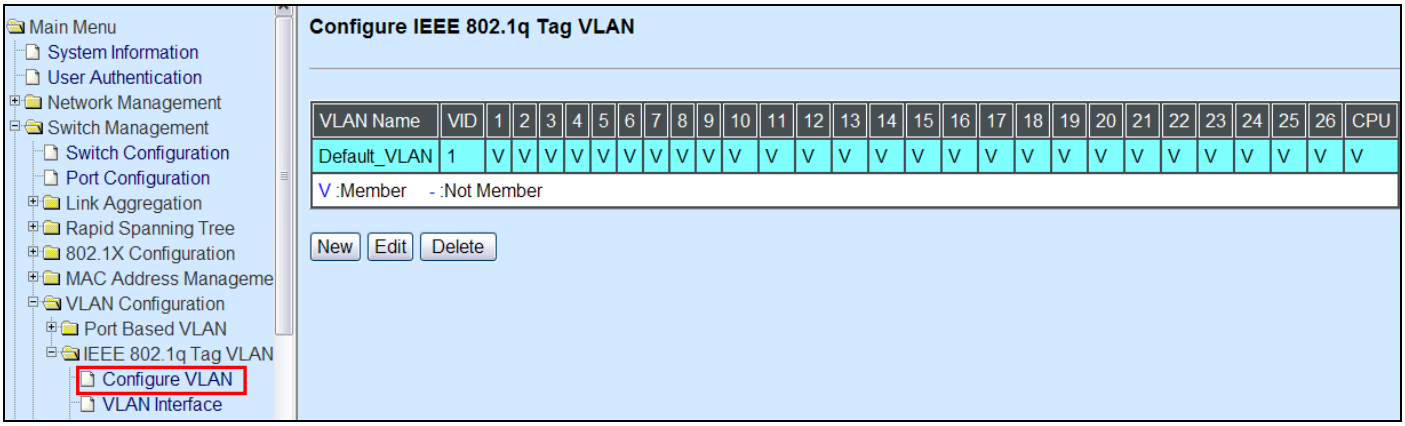
6. Set Port 26 to trunk mode.	`SWH(config)# interface 26`
	`SWH(config-if-26)# vlan dot1q-vlan mode trunk`
	`OK !`
	`SWH(config-if-26)# exit`

7. Change Port 1's PVID to "11".	`SWH(config)# interface 1`
	`SWH(config-if-1)# vlan dot1q-vlan access-vlan 11`
	`OK !`
	`SWH(config-if-1)# exit`

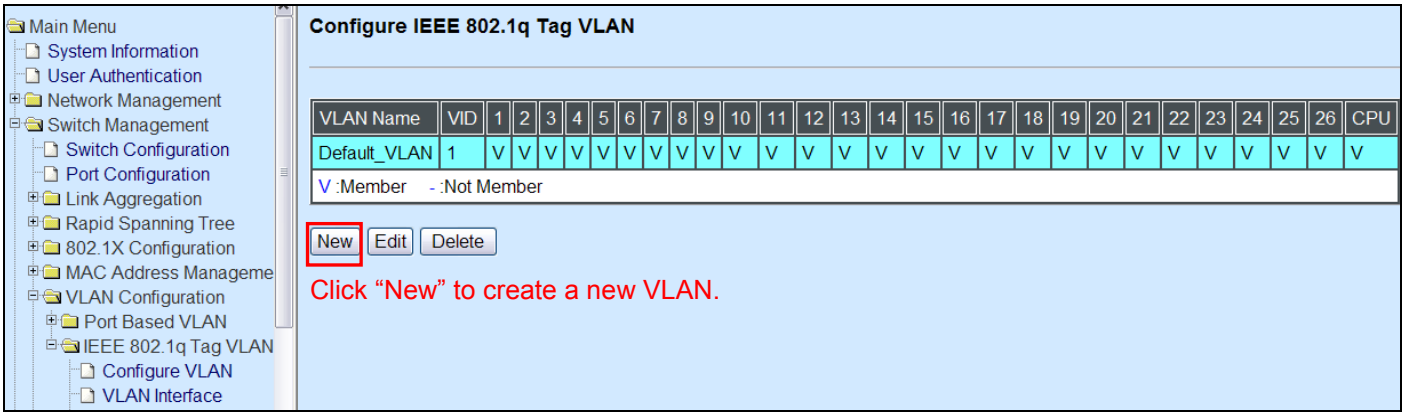
8. Show currently configured VLAN tag settings.	`SWH(config)# show vlan interface`
	`==========`
	`IEEE 802.1q Tag VLAN Interface :`
	`==========`
	
	`Port  Mode  PVID  VLAN Member`
	`------  --------  ------  ----------`
	`1  access  11  1,11`
	`2  access  1  1`
	`3  access  1  1`
	`4  access  1  1`
	`5  access  1  1`
	`6  access  1  1`
	`7  access  1  1`
	`8  access  1  1`
	`9  access  1  1`
	`10  access  1  1`
	`11  access  1  1`
	`12  access  1  1`
	`13  access  1  1`
	`14  access  1  1`
	`15  access  1  1`
	`16  access  1  1`
	`17  access  1  1`
	`18  access  1  1`
	`19  access  1  1`
	`20  access  1  1`
	`21  access  1  1`
	`22  access  1  1`
	`23  access  1  1`
	`24  access  1  1`
	`25  access  1  1`
	`26  trunk  1  1,11`

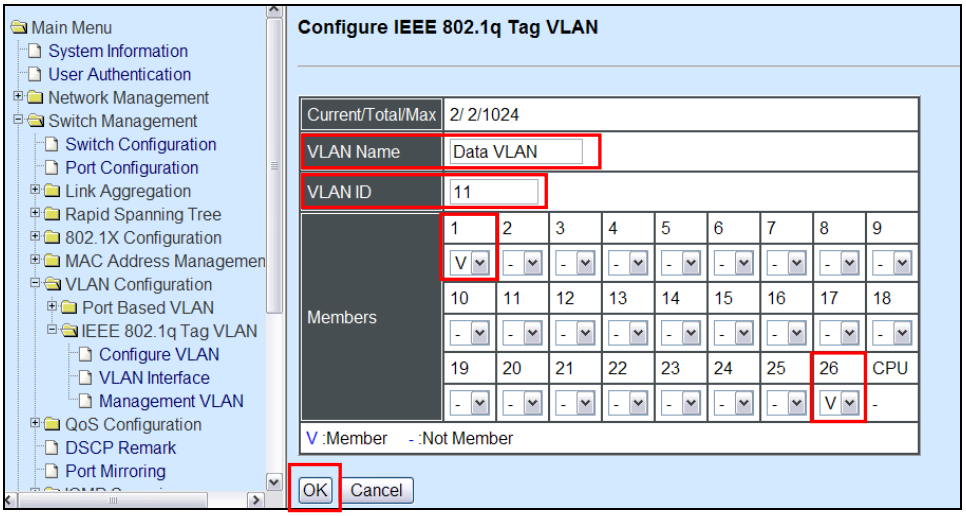
Web Management Configuration:

1. Select "Configure VLAN" option in IEEE 802.1Q Tag VLAN menu.
Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>Configure VLAN



2. Create a new Data VLAN 11 that includes Port 1 and Port 26 as members.
Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>Configure VLAN

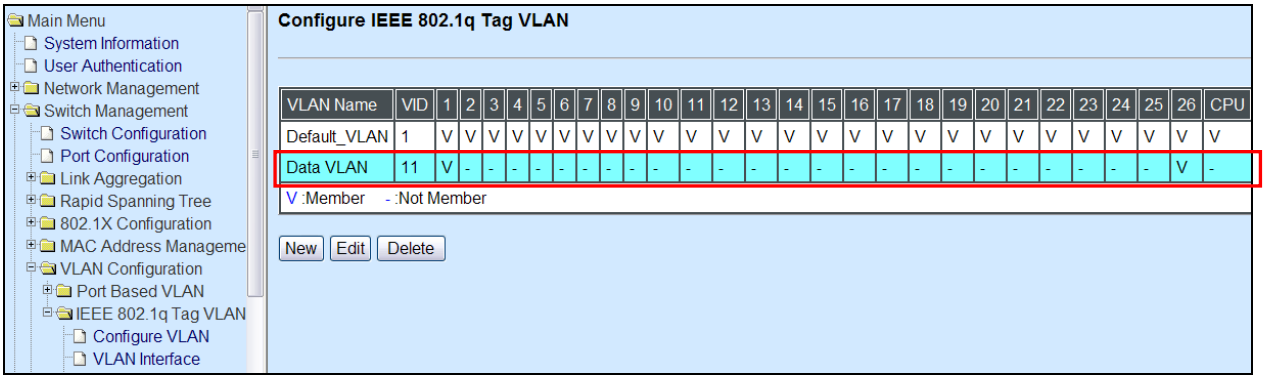




Data VLAN 11 that includes Port 1 and Port 26 as member ports.

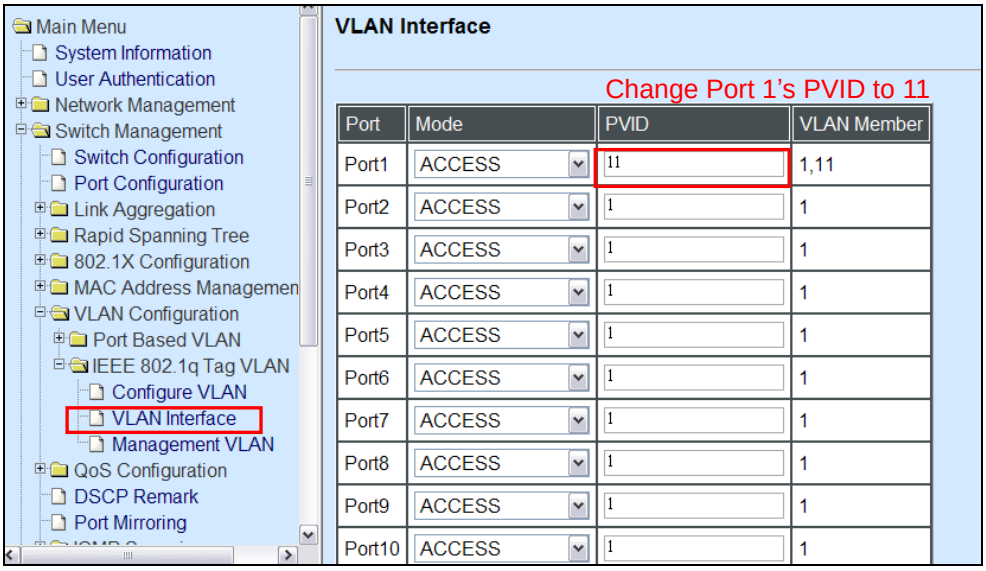
Click "OK" button to return to IEEE 802.1q Tag VLAN table.

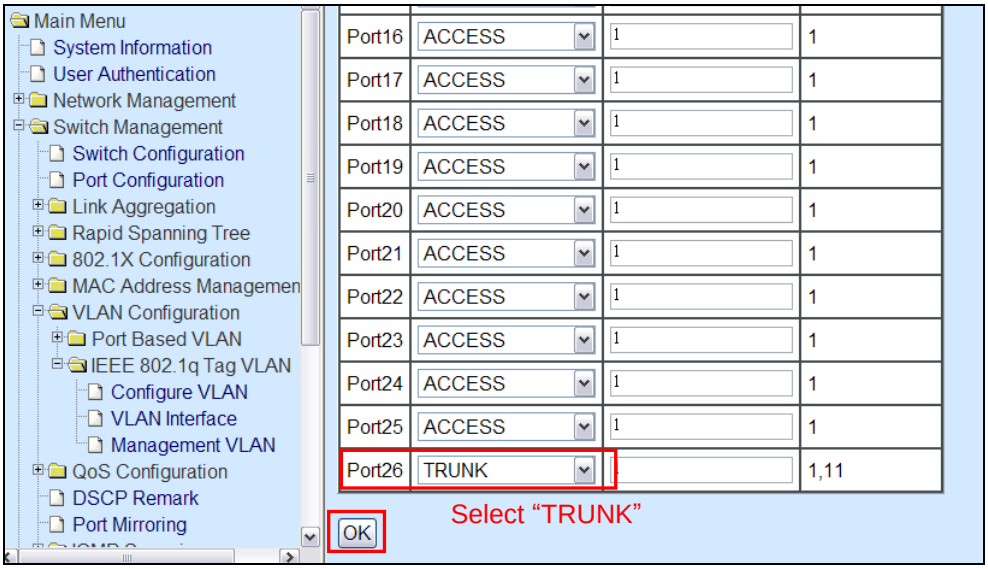
3. Check Data VLAN 11 settings.
Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>Configure VLAN



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 PVID configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.

4. Change Port 1's PVID to 11, and set Port 26 to trunk mode.
Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN> VLAN Interface





Click "OK" to apply the settings.

Treatments of Packets:

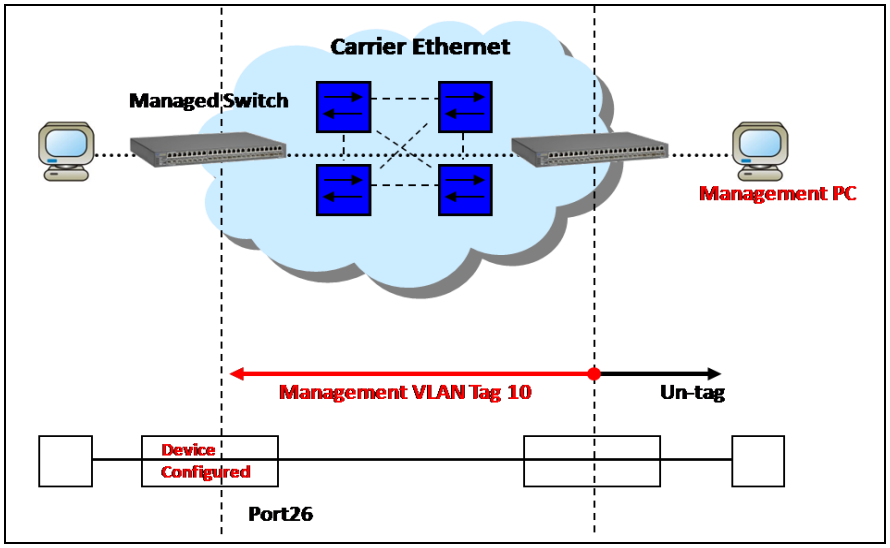
1. A untagged packet arrives at Port 1
When an untagged packet arrives at Port 1, port 1's Port VLAN ID (11) will be added to the original port. Because port 26 is set as a trunk port, it will forward the packet with tag 11 out to the Carrier Ethernet.

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.

In the network diagram provided, 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.



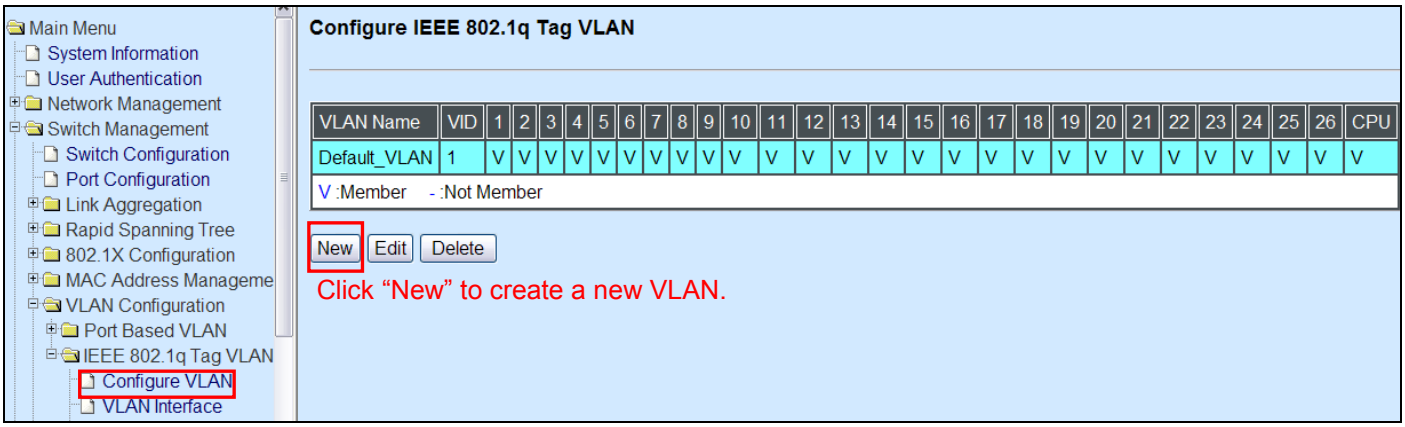
Management VLAN Network Diagram

CLI Configuration:

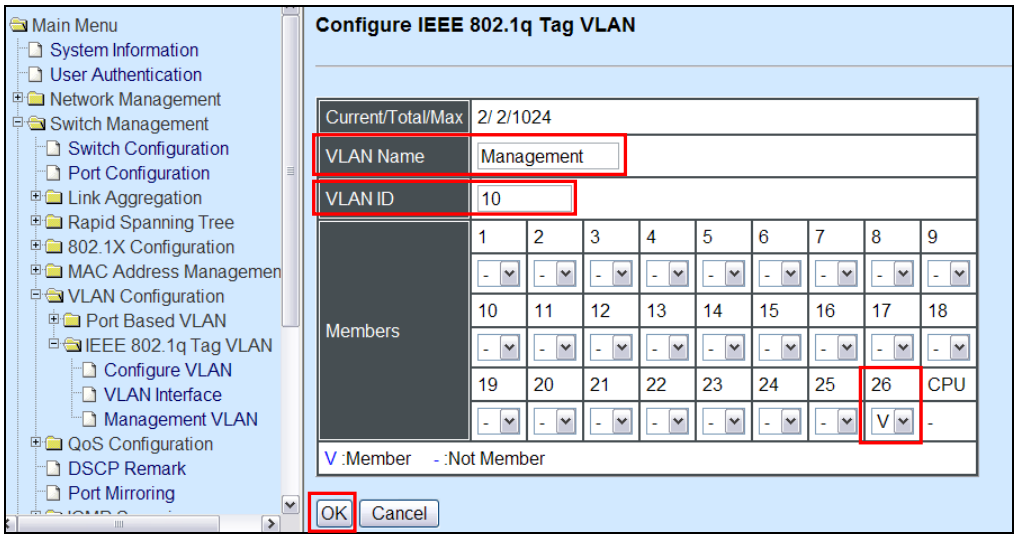
Steps…	Commands…
1. Enter Global Configuration mode.	SWH> enable Password: SWH# config SWH(config)#
2. Crate VLAN 10.	SWH(config)# vlan dot1q-vlan 10 OK ! SWH(config-vlan-10)#
3. Name VLAN 10 to Management	SWH(config-vlan-10)# name Management OK ! SWH(config-vlan-10)# exit
4. Assign Port 26 to VLAN 10.	SWH(config)# interface 26 SWH(config-if-26)# vlan dot1q-vlan trunk-vlan 10 OK !
5. Assign VLAN 10 to Management VLAN and Port 26 to Management port.	SWH(config)# vlan management-vlan 10 management-port 26 mode trunk OK !
6. Show currently configured dot1q settings and check CPU has been a member port in Management VLAN 10.	SWH(config)# show vlan dot1q-vlan ========== IEEE 802.1q Tag VLAN : ========== CPU VLAN ID : 10 VLAN Name VLAN 1 8 9 16 17 24 25 26 CPU ---------- ---- -------- -------- -------- -- -- --- Default_VLAN 1 VVVVVVVV VVVVVVVV VVVVVVVV V V - Management 10 -------- -------- -------- - 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 PVID 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 IEEE 802.1Q Tag VLAN menu.**
   Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>Configure VLAN



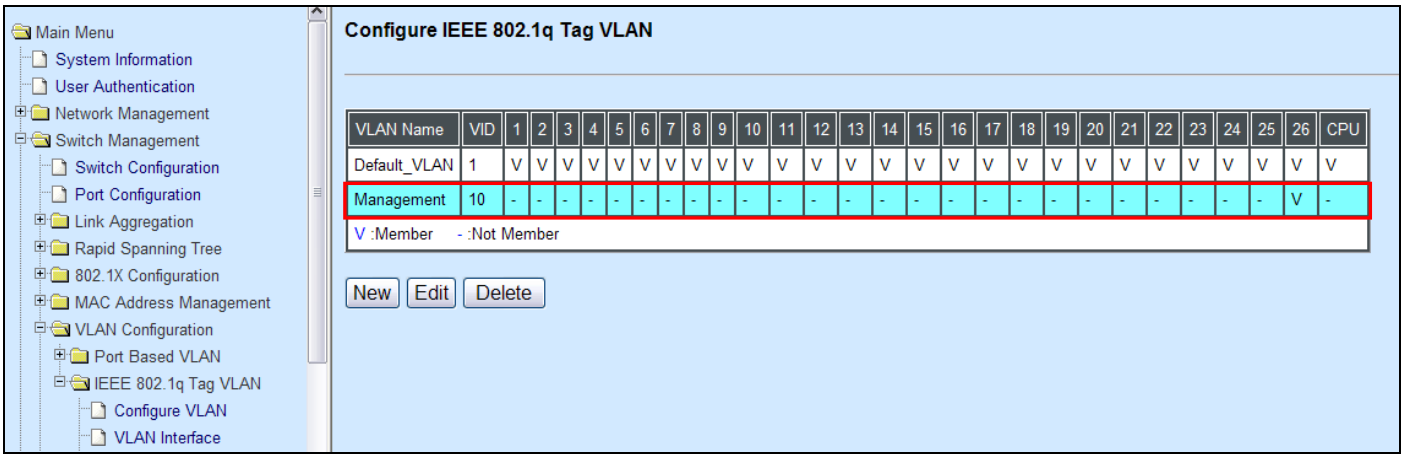
2. **Create a new Management VLAN 10 that includes only Port 26 as a member port.**
   Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>Configure VLAN



Management VLAN 10 that includes Port 26 as a member port.

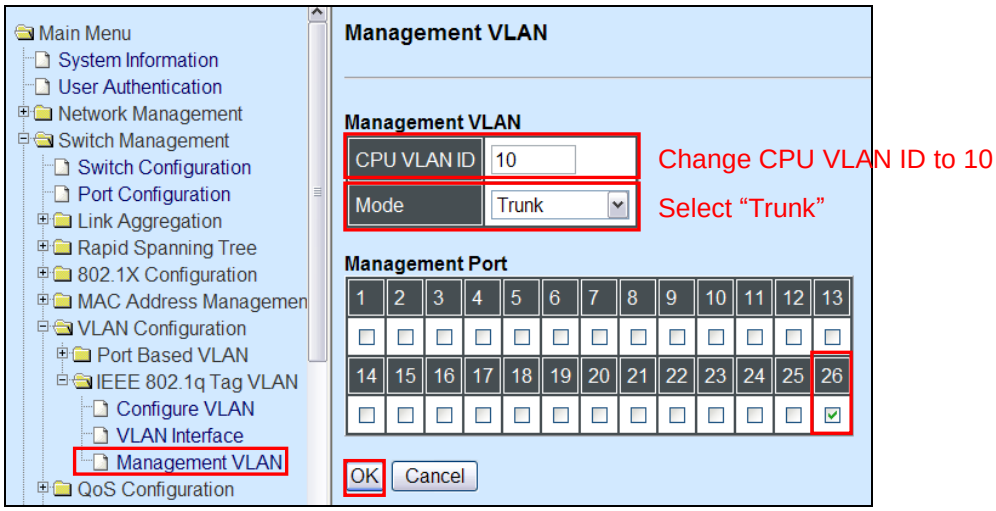
Click "OK" button to return to IEEE 802.1q Tag VLAN table.

3. **Check Management VLAN 10 settings.**
   Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>Configure VLAN



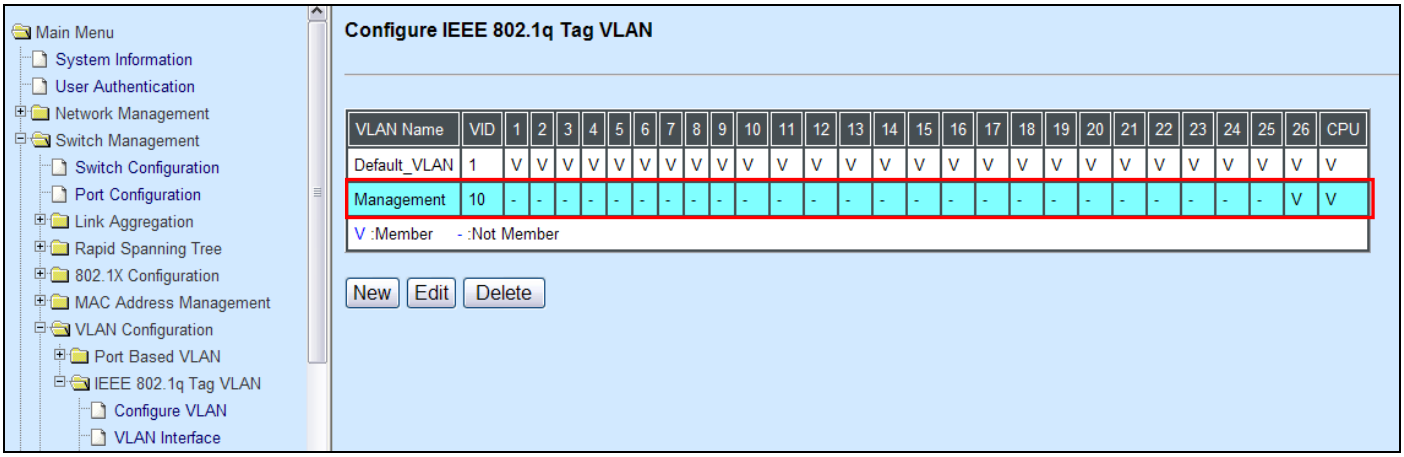
NOTE: By default, all ports are member ports of the Default_VLAN. Before removing the Deafult_VLAN from the VLAN table, make sure you have correct management VLAN and PVID configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.

4. **Change the Management VLAN to VLAN 10 and set Port 26 to Trunk mode**
   Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>Management VLAN



Click "OK" to apply the settings.

5. **Check Management VLAN 10 settings again.**
   Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>Configure VLAN



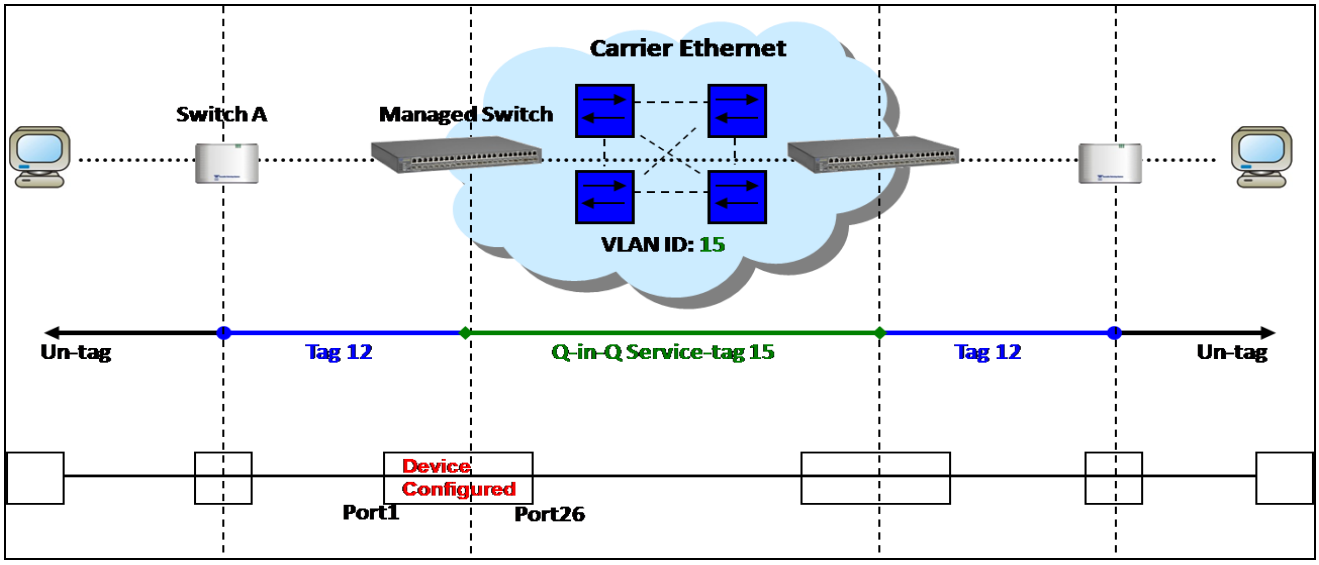
Now, Port 26 and CPU are member ports in Management VLAN 10.

Treatments of Packets:

1. **A tagged packet arrives at Port 26**
   In this example, port 26 is assigned as a management port. Therefore, the client can manage the Managed Switch remotely. When management traffic with tag 10 arrives at port 26, the tag will be removed. Then, untagged traffic is sent to CPU. When sending out management traffic out from port 26, it will be added a tag 10.

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. Create a VLAN 15.	`SWH(config)# vlan dot1q-vlan 15` `OK !`

3. Name VLAN 15 to S-VLAN.	`SWH(config-vlan-15)# name S-VLAN`
	`OK !`
	`SWH(config-vlan-15)# exit`

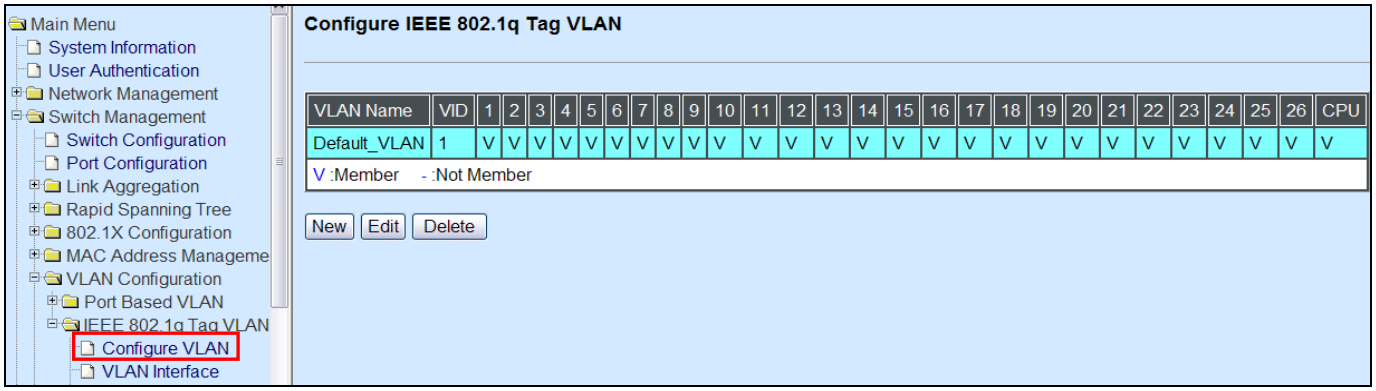
4. Assign Port 1 and Port 26 to VLAN 15.	`SWH(config)# interface 1,26`
	`SWH(config-if-1,26)# vlan dot1q-vlan trunk-vlan 15`
	`OK !`
	`SWH(config-if-1,26)# exit`

5. Show currently configured dot1q VLAN membership.	`SWH(config)# show vlan dot1q-vlan`
	`==========`
	`IEEE 802.1q Tag VLAN :`
	`==========`
	`CPU VLAN ID : 1`
	`VLAN Name  VLAN  1  8 9  16 17  24 25 26 CPU`
	`---  ---  --- --- --- -- -- ---`
	`Default_VLAN  1  VVVVVVVV VVVVVVVV VVVVVVVV  V  V  V`
	`S-VLAN  15  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 PVID configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.

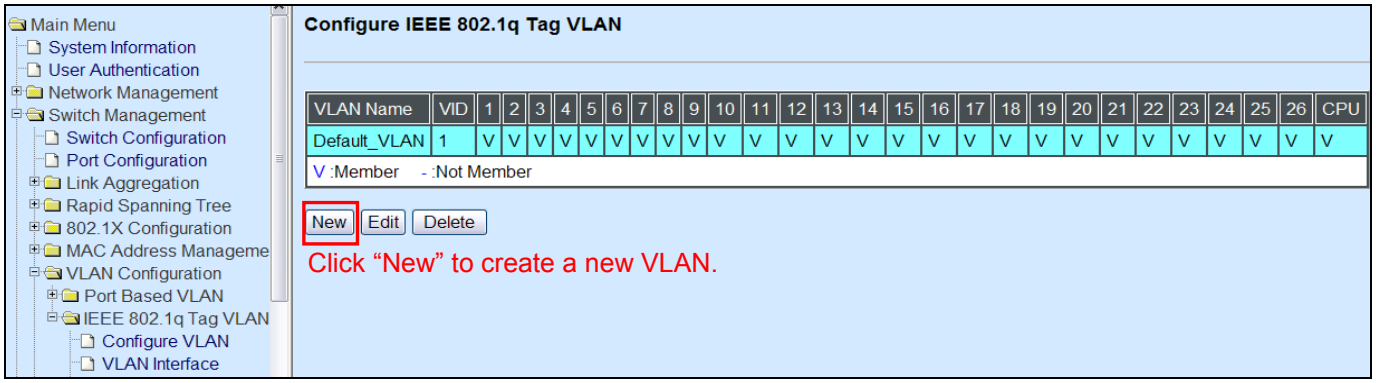
6. Set Port 1 to tunnel mode.	SWH(config)# interface 1 SWH(config-if-1)# vlan dot1q-vlan mode dot1q-tunnel OK !
7. Change Port 1's PVID to 15.	SWH(config-if-1)# vlan dot1q-vlan access-vlan 15 OK ! SWH(config-if-1)# exit
8. Set Port 26 to trunk mode.	SWH(config)# interface 26 SWH(config-if-26)# vlan dot1q-vlan mode trunk OK !
9. Show currently configured VLAN tag settings.	SWH(config)# show vlan interface ========== IEEE 802.1q Tag VLAN Interface : ========== Port Mode PVID VLAN Member ----- ------ ------ ---------- 1 dot1q-tunnel 15 1,15 2 access 1 1 3 access 1 1 4 access 1 1 5 access 1 1 6 access 1 1 7 access 1 1 8 access 1 1 9 access 1 1 10 access 1 1 11 access 1 1 12 access 1 1 13 access 1 1 14 access 1 1 15 access 1 1 16 access 1 1 17 access 1 1 18 access 1 1 19 access 1 1 20 access 1 1 21 access 1 1 22 access 1 1 23 access 1 1 24 access 1 1 25 access 1 1 26 trunk 1 1,15

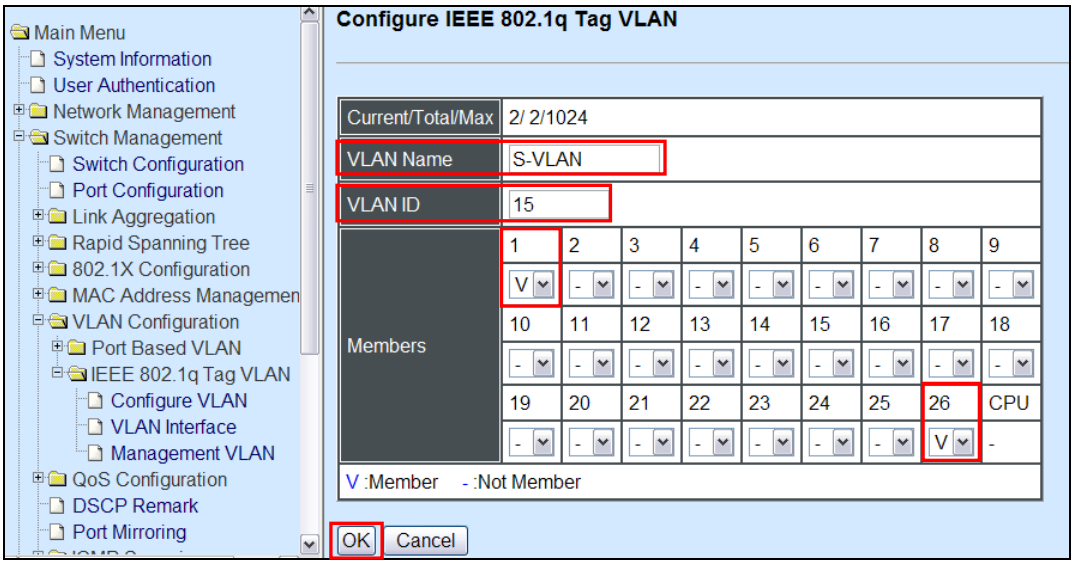
Web Management Configuration:

1. **Select "Configure VLAN" option in IEEE 802.1Q Tag VLAN menu.**
   Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>Configure VLAN



2. Create a new Service VLAN 15 that includes Port 1 and Port 26 as member ports.
Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>Configure VLAN

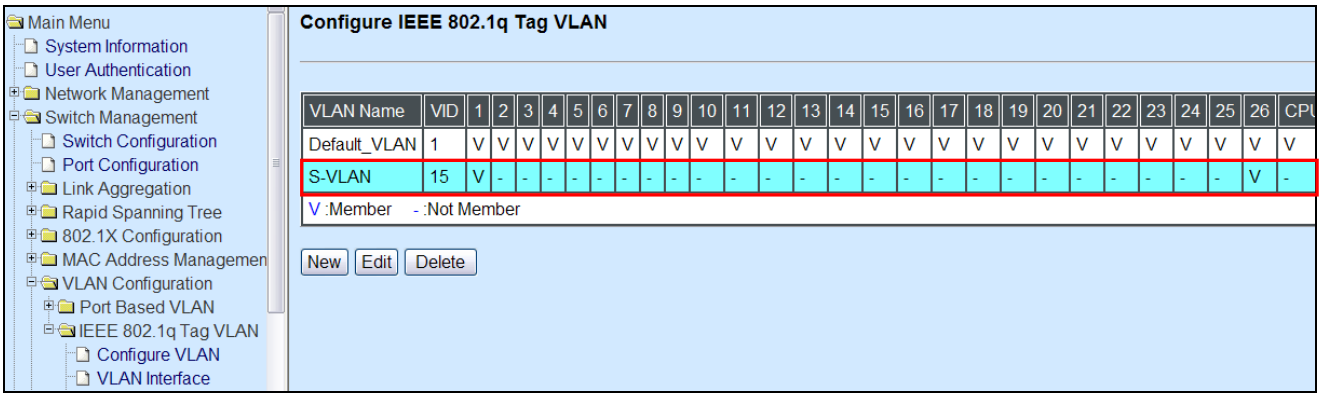




Create S-VLAN 15 that includes Port 1 and Port 26 as member ports.

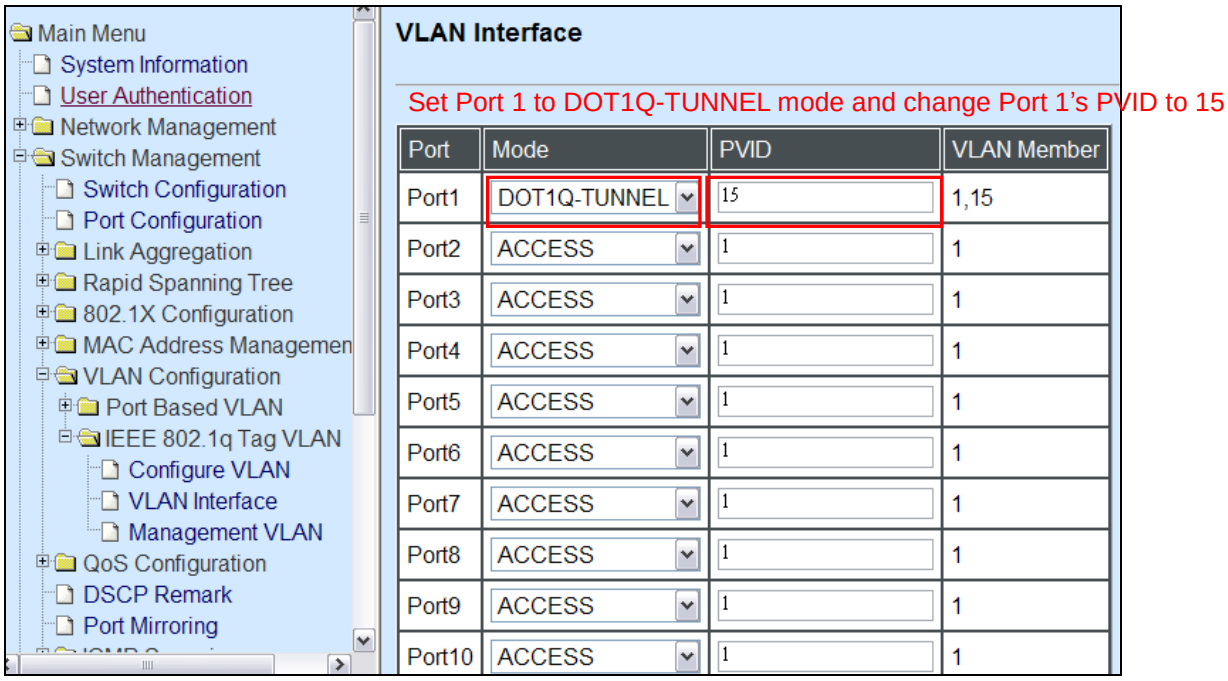
Click "OK" button to return to IEEE 802.1q Tag VLAN table.

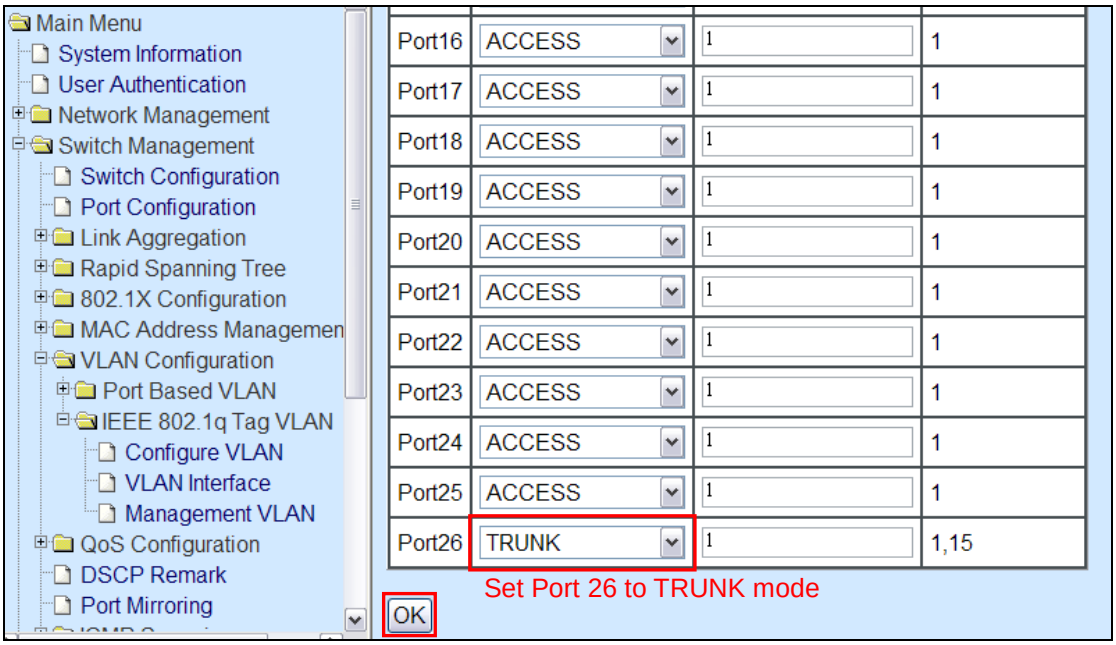
3. Check S-VLAN 15 settings.
Switch Management>VLAN Configuration>IEEE 802.1q Tag VLAN>Configure VLAN



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 PVID configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.

4. **Change Port 1's PVID to 15, and set Port 1 to DOT1Q-TUNNEL mode and Port 26 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 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 26, two tags will be forwarded out because Port 26 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.