CONNECTION TECHNOLOGY SYSTEMS

HES-5105SFP+

1 x 10G/5G/2.5G/1G/100MBase-T RJ-45 + 3 x 2.5G/1G/100M Base-T RJ45 + 1 x 10G/1GBase-X SFP+ Managed CPE Switch

Network Management

User's Manual

Version 1.1

Revision History

Version	F/W	Date	Description
1.0	1.00.01	2025/2/19	First release.
1.1	1.00.07	2026/1/16	**Revised:** 2.4.1 Copy-cfg Command 2.4.8 Show Command 2.5.3 Show Command 2.5.21 Switch-info Command 2.5.24 User Command 4.1 System Setup 4.1.1 System Information 4.2.6 LAN Follow WAN 4.6.1.4 IGMP Group Table 4.6.1.6 MLD Group Table 4.11.2 User Account **Removed:** Show interface status Command (Integrated into 2.5.26 Interface Command) Show interface statistics Command (Integrated into 2.5.26 Interface Command) Show running-config & start-up-config & default-config Command (Integrated into 2.5.3 Show Command)

Trademarks

CTS is a registered trademark of Connection Technology Systems Inc.
All trademarks belong to their respective proprietors.

Contents subject to change without prior notice.

Copyright Statement

Copyright © 2025 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 B 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 the equipment is not installed and used in accordance with the instructions, it 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 © 2025-2026 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.

CTS Contact Information

■ Headquarters/Manufacturer:

Connection Technology Systems Inc.

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

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

Tel: +886-2-2698-9661

Fax: +886-2-2698-3960

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

www.ctsystem.com

■ Global Offices:

Connection Technology Systems NE AB

E A Rosengrens gata 31,

421 31 Västra Frölunda,

Sweden

Tel: +46 31 22 19 80

E-mail: info@ctsystem.se

Connection Technology Systems Japan Ltd.

Higobashi Bldg. No.3 R503, 1-23-13,

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

Tel: +81-6-6450-8890

E-mail: cts_japan@ctsystem.com

Connection Technology Systems CE GmbH

Wienerbergstraße 11 / Tower B / 6th Floor / Office 2

1100 Vienna

AUSTRIA

Tel: +43 1 343 9553 50

E-mail: cts_ce@ctsystem.com

Connection Technology Systems India Private Limited

No.1, 1st Floor, RK Residency Vajarahalli,

Uttarahalli, Talgatpura, Kanakpura MN

Rd, Bangalore, Karnataka, India, 560062

E-mail: cts_in@ctsystem.com

Table of Content

CTS Contact Information **4**

Table of Content **5**

1. INTRODUCTION **10**

1.1 Management Options 10

1.2 Management Software 11

1.3 Management Preparations 12

2. Command Line Interface (CLI) **14**

2.1 Remote Management – Telnet/SSH 14

2.2 Navigating CLI 15

2.2.1 General Commands 15

2.2.2 Quick Keys 15

2.2.3 Command Format 16

2.2.4 Login Username & Password 17

2.3 User Mode 19

2.3.1 Ping Command 19

2.3.2 Traceroute Command 20

2.4 Privileged Mode 20

2.4.1 Copy-cfg Command 21

2.4.2 Firmware Command 22

2.4.3 Ping Command 22

2.4.4 Reload Command 23

2.4.5 Traceroute Command 23

2.4.6 Write Command 23

2.4.7 Configure Command 24

2.4.8 Show Command 24

2.5 Configuration Mode 25

2.5.1 Entering Interface Numbers 25

2.5.2 No Command 26

2.5.3 Show Command 26

2.5.4 Archive Command 32

2.5.5 Event-record Command 33

2.5.6 IP Command 33

2.5.7 IPv6 Command 40

2.5.8 lan-follow-wan Command 43

2.5.9 LLDP Command 44

2.5.10 Loop Detection Command 46
2.5.11 LED Command 47
2.5.12 MAC Command 47
2.5.13 Management Command 50
2.5.14 Mirror Command 57
2.5.15 NTP Command 58
2.5.16 QoS Command 59
2.5.17 Security Command 64
2.5.18 SFP Command 67
2.5.19 SNMP-Server Command 73
2.5.20 Switch Command 79
2.5.21 Switch-info Command 79
2.5.22 Syslog Command 82
2.5.23 Terminal Command 83
2.5.24 User Command 83
2.5.25 VLAN Command 85
2.5.25.1 Port-Based VLAN 85
2.5.25.2 802.1Q VLAN 85
2.5.25.3 Introduction to Q-in-Q (ISP Mode) 88
2.5.26 Interface Command 93
2.5.27 Diagnostics Command 97
2.5.27.1 Configure Diagnostics Details 97
2.5.27.1.1 Cable Diagnostics 97
2.5.27.1.2 DHCP client Diagnostics. 97
2.5.27.1.3 DNS Diagnostics. 98
2.5.27.1.4 IPTV Diagnostics. 100
2.5.27.1.5 Ping Diagnostics. 110
2.5.27.1.6 Throughput Diagnostics. 112
2.5.27.2 Perform Diagnostics 116
3. SNMP NETWORK MANAGEMENT 122
4. WEB MANAGEMENT 123
1.1 System Setup 125
4.1.1 System Information 126
4.1.2 IP Setup 128
4.1.3 IP Source Binding 131
4.1.4 Time Server Setup 132
4.1.5 Syslog Setup 133

4.1.6 DHCP Client Setup 134
4.2 Port Management 135
4.2.1 Port Setup & Status 136
4.2.2 Port Traffic Statistics 138
4.2.3 Port Packet Error Statistics 139
4.2.4 Port Packet Analysis Statistics 140
4.2.5 Port Mirroring 141
4.2.6 LAN Follow WAN 143
4.3 VLAN Setup 144
4.3.1 VLAN Mode 145
4.3.2 Port Based VLAN 146
4.3.3 IEEE 802.1q Tag VLAN 148
4.3.3.1 Trunk VLAN Setup 151
4.3.3.2 VLAN Interface 151
4.3.3.3 VLAN Table 154
4.4 MAC Address Management 155
4.4.1 MAC Table Learning 156
4.4.2 MAC Address Table 157
4.5 QoS Setup 159
4.5.1 QoS Priority 160
4.5.2 QoS Remarking 162
4.5.3 QoS Rate Limit 164
4.6 Multicast 165
4.6.1 IGMP/MLD Snooping 165
4.6.1.1 IGMP/MLD Setup 167
4.6.1.2 IGMP/MLD VLAN Setup 168
4.6.1.3 IGMP Snooping Status 169
4.6.1.4 IGMP Group Table 170
4.6.1.5 MLD Snooping Status 171
4.6.1.6 MLD Group Table 172
4.7 Security Setup 173
4.7.1 DHCP Snooping 174
4.7.1.1 DHCP Snooping Setup 174
4.7.1.2 DHCP Option 82 / DHCPv6 Option 37 Setup 175
4.7.1.3 DHCP Snooping Table 178
4.7.2 Port Isolation 179
4.7.3 Storm Control 180

4.7.4 Loop Detection 181
4.8 LLDP 183
4.8.1 LLDP Setup 184
4.8.2 LLDP Status 185
4.9 Maintenance 186
4.9.1 CPU Loading 187
4.9.2 System Memory 189
4.9.3 Ping 190
4.9.4 Event Log 191
4.9.5 SFP Information 194
4.9.4.1 SFP Port Info 195
4.9.4.2 SFP Port State 196
4.9.4.3 SFP Port Threshold Configuration 197
4.10 Advanced Diagnostics 200
4.10.1 Network Diagnostics 201
4.10.1.1 Cable Diagnostics 202
4.10.1.2 DHCP Client Diagnostics 204
4.10.1.3 DNS Diagnostics 207
4.10.1.4 IPTV Diagnostics 210
4.10.1.4.1 MPEG-Loss 210
4.10.1.4.2 PCR-Jitter 213
4.10.1.4.3 Throughput 216
4.10.1.4.4 General Query Interval 219
4.10.1.4.5 Genaral Query Response 222
4.10.1.4.6 Zapping Time 224
4.10.1.5 Ping Diagnostics 227
4.10.1.6 Throughput Diagnostics 230
4.10.2 Diagnostics Schedule 234
4.11 Management 236
4.11.1 Management Access Setup 238
4.11.2 User Account 239
4.11.3 RADIUS/TACACS+ 241
4.11.4 Management Authentication 243
4.11.5 SNMP 244
4.11.5.1 SNMPv3 USM User 244
4.11.5.2 Device Community 247
4.11.5.3 Trap Destination 249

4.11.5.4 Trap Setup 250
4.11.6 LED Control Setup 251
4.11.7 Firmware upgrade 252
4.11.7.1 Configuration Backup/Restore via HTTP 252
4.11.7.2 Firmware Upgrade via HTTP 253
4.11.7.3 Configuration Backup/Restore via FTP/TFTP 254
4.11.7.4 Firmware Upgrade via FTP/TFTP 255
4.11.8 Load Factory Settings 256
4.11.9 Auto-Backup Setup 257
4.11.10 Save Configuration 258
4.11.11 Reset System 259
APPENDIX A: FreeRADIUS Readme 260
APPENDIX B: Set Up DHCP Auto-Provisioning 262

1. INTRODUCTION

Thank you for using the 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 remotely. This User's Manual will explain how to use command-line interface and Web Management to configure your Managed Switch. The readers of this manual should have knowledge about their network typologies and about basic networking concepts so as to make the best of this user's manual and maximize the Managed Switch's performance for your personalized networking environment.

1.1 Management Options

Switch management options available are listed below:

- Telnet Management
- SNMP Management
- WEB Management
- SSH Management

Telnet Management

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

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. Web management in the local site, especially for the first time use of the Managed Switch to set up the needed IP, can be done through one of the 8-pin RJ-45 ports located at the front panel of the Managed Switch. Direct RJ-45 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

Command Line Interface Program

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

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

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

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

SNMP Management System

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

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

Web Browser Application

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

1.3 Management Preparations

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

Connecting the Managed Switch

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

10/1GBase-X SFP+ Port

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

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

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

2.5G/1G/100MBase-T and 10G/5G/2.5G/1G/100MBase-T RJ-45 Auto-MDI/MDIX Port

2.5G/1G/100MBase-T and 10G/5G/2.5G/1G/100MBase-T RJ-45 Auto-MDI/MDIX ports are located at the front of the Managed Switch. These RJ-45 ports allow user to connect their traditional copper-based Ethernet / Fast Ethernet devices to the network. All these ports support auto-negotiation and MDI/MDIX auto-crossover, i.e. either crossover or straight through CAT-5E UTP or STP cable may be used. As to Multi-Gigabit RJ-45 port can be plugged with CAT-5E/CAT.6/CAT-6A (22~24 AWG) or better cabling.

IP Addresses

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

IP addresses are made up of two parts:

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

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

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

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

MIB for Network Management Systems

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

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

2. Command Line Interface (CLI)

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

- Telnet
- Configuring the system
- Resetting the system

2.1 Remote Management – Telnet/SSH

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

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

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

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

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

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

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

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

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

2.2 Navigating CLI

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

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

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

2.2.1 General Commands

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

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

2.2.2 Quick Keys

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

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

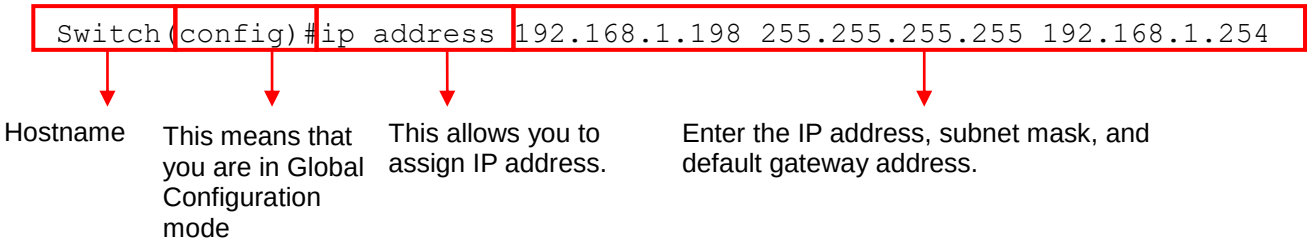
Unfinished command followed by ?	Enter an unfinished command or keyword and press “?” key to complete the command and get command syntax help.
	
	Example: List all available commands starting with the characters that you enter.
	
	`Switch#h?`
	`help` `Show available commands`
	`history` `Show history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

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

2.2.3 Command Format

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

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



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

Symbols	**Brief Description**
>	Currently, the device is in User mode.
#	Currently, the device is in Privileged mode.
(config)#	Currently, the device is in Global Configuration mode.
Syntax	**Brief Description**
[ ]	Reference parameter.
[-s size] [-c count]	These two parameters are used in ping command and are optional, which means that you can ignore these tho parameters if they are unnecessary when executing ping command.
[A.B.C.D]	Brackets represent that this is a required field. Enter an IP address or gateway address.
[255.X.X.X]	Brackets represent that this is a required

	field. Enter the subnet mask.
[port]	Enter one port number. See Section 2.5.26 for detailed explanations.
[port_list]	Enter a range of port numbers or several discontinuous port numbers. See Section 2.5.26 for detailed explanations.
[forced_true | forced_false | auto]	There are three options that you can choose. Specify one of them.
[1-8191]	Specify a value between 1 and 8191.

[0-7] 802.1p_list
[0-63] dscp_list
	Specify one value, more than one value or a range of values.
	
	Example 1: specifying one value
	
	`Switch(config)#qos 802.1p-map 1 0`
	
	`Switch(config)#qos dscp-map 10 3`
	Example 2: specifying three values (separated by commas)
	
	`Switch(config)#qos 802.1p-map 1,3 0`
	
	`Switch(config)#qos dscp-map 10,13,15 3`
	
	Example 3: specifying a range of values (separated by a hyphen)
	
	`Switch(config)#qos 802.1p-map 1-3 0`
	
	`Switch(config)#qos dscp-map 10-15 3`

2.2.4 Login Username & Password

Default Login

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

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

Privileged Mode Password

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

Forgot Your Login Username & Password

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

2.3 User Mode

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

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

2.3.1 Ping Command

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

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

2.3.2 Traceroute Command

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

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

2.4 Privileged Mode

The only place where you can enter the Privileged mode is in User mode. When you successfully enter the Privileged mode (this mode is password protected), the prompt will be changed to Switch# (the model name of your device together with a pound sign). Enter the question mark (?) or help command to view a list of commands available for use.

Command	Description
copy-cfg	Restore or backup configuration file via FTP or TFTP server.
disable	Exit Privileged mode and return to User Mode.
exit	Exit Privileged mode and return to User Mode.
firmware	Allow users to update firmware via FTP or TFTP.
help	Display a list of available commands in Privileged mode.
history	Show commands that have been used.
ip	Set up the DHCP recycle.
logout	Logout from the Managed Switch.
ping	Test whether a specified network device or host is reachable or not.
reload	Restart the Managed Switch.
traceroute	Trace the route to HOST
write	Save your configurations to Flash.
configure	Enter the Global Configuration mode.
show	Show a list of commands or show the current setting of each listed command.
diagnostics	Perform advanced diagnostics.
no	Disable a command or reset it back to its default setting.

2.4.1 Copy-cfg Command

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

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

Command	Parameter	Description
Switch# copy-cfg from ftp [A.B.C.D | A:B:C:D:E:F:G:H] [file name] [user_name] [password]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IP/IPv6 address of your FTP server.
	[file name]	Enter the configuration file name that you would like to restore.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
Switch# copy-cfg from tftp [A.B.C.D | A:B:C:D:E:F:G:H] [file_name]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IP/IPv6 address of your TFTP server.
	[file name]	Enter the configuration file name that you would like to restore.
Example		
Switch# copy-cfg from ftp 192.168.1.198 HS_0600_file.conf misadmin1 abcxyz Switch# copy-cfg from tftp 192.168.1.198 HS_0600_file.conf		

2. Backup a configuration file to FTP or TFTP server.

Command	Parameter	Description
Switch# copy-cfg to ftp [A.B.C.D | A:B:C:D:E:F:G:H] [file name] [running | default | startup] [user_name] [password]	[A.B.C.D | A:B:C:D:E:F:G:H]	Enter the IP address of your FTP server.
	[file name]	Enter the configuration file name that you want to backup.
	[running | default | startup]	Specify backup config to be running, default or startup
	[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	Description
Switch# copy-cfg from default	Enter the IPv4/IPv6 address of your FTP server.
Switch# copy-cfg from default keep event	Restore the Managed Switch back to default settings but keep the entire data of event log.

Switch# copy-cfg from default keep event ip	Restore the Managed Switch back to default settings but keep both of the IP configurations and the entire data of event log.
Switch# copy-cfg from default keep ip	Restore the Managed Switch back to default settings but keep IP configurations.
Switch# copy-cfg from default keep ip event	Restore the Managed Switch back to default settings but keep both of the IP configurations and the entire data of event log.

2.4.2 Firmware Command

To upgrade firmware via TFTP or FTP server.

Command	Parameter	Description
Switch# firmware upgrade ftp [A.B.C.D | A:B:C:D:E:F:G:H] [file_name] [alternate-image] [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.
	[alternate-image]	The firmware will be upgraded to the other image on which the system is not currently running.
	[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] [alternate-image]	[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.
	[alternate-image]	The firmware will be upgraded to the other image on which the system is not currently running.
Example		
Switch# firmware upgrade ftp 192.168.1.198 HS_0600_file.bin alternate-image edgeswitch10 abcxyz		
Switch# firmware upgrade tftp 192.168.1.198 HS_0600_file.bin alternate-image		

2.4.3 Ping Command

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

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

Switch# ping 8.8.8.8 Switch# ping 8.8.8.8 –s 128 –c 10 Switch# ping 2001:4860:4860::8888 Switch# ping 2001:4860:4860::8888 –s 128 –c 10

2.4.4 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

2.4.5 Traceroute Command

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

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

2.4.6 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!

2.4.7 Configure Command

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

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

2.4.8 Show Command

The “show” command is an essential tool for network administrators to retrieve device information, verify configurations, and troubleshoot network issues. It can be used in both Privileged and Configuration modes.
For details on the show command, please refer to section 2.5.3. The command is available in both privileged and configuration modes but is documented only in the configuration mode section to avoid duplication.

2.5 Configuration Mode

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

Command	Description
archive	Manage archive configuration files.
event-record	Configure the Event Record function.
exit	Exit the global configuration mode.
help	Display a list of available commands in the global configuration mode.
history	Show commands that have been used.
ip	Set up the IPv4 address and enable DHCP mode & IGMP snooping.
ipv6	To enable ipv6 function and set up IP address.
lan-follow-wan	Set up LAN port(s) to follow WAN port’s linkup/linkdown commands.
lldp	LLDP global configuration mode.
loop-detection	Configure loop-detection to prevent loop between switch ports by locking them.
led	Enable or disable the LED status light on the Managed Switch.
mac	Set up MAC learning function of each port.
management	Set up telnet/web/SSH access control and timeout value, RADIUS/TACACS+, and authentication method management.
mirror	Set up target port for mirroring.
ntp	Set up required configurations for Network Time Protocol.
qos	Set up the priority of packets within the Managed Switch.
security	Configure broadcast, unknown multicast, unknown unicast storm control settings.
sfp	Configure SFP monitored items’ parameters and view the current value of each item.
snmp-server	Create a new SNMP community and trap destination and specify the trap types.
switch	Set up acceptable frame size and address learning, etc.
switch-info	Edit the system information.
syslog	Set up required configurations for Syslog server.
terminal	Set up Terminal functions.
user	Create a new user account.
vlan	Set up VLAN mode and VLAN configuration.
no	Disable a command or reset it back to its default setting.
interface	Select a single interface or a range of interfaces.
show	Show a list of commands or show the current setting of each listed command.
diagnostics	Perform advanced diagnostics.

2.5.1 Entering Interface Numbers

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

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

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

2.5.2 No Command

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

2.5.3 Show Command

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

The “show” command is an essential tool for network administrators to retrieve device information, verify configurations, and troubleshoot network issues. It can be used in both Privileged and Configuration modes. The following sections describe different uses of the show command and list relevant commands with brief descriptions. Where a command has a dedicated chapter, a reference is provided for detailed information.

1. Display system-related information

Show switch-info: Display system-related information and hardware status, such as system name, model, firmware version, CPU loading, memory usage, temperature, fan speed, and internal voltages. See Section Switch-info for details.

2. Display currently-configured settings or statistics

Show archive: Display the current auto-backup configuration for system files. See Section Archive Command for details.

Show event-record: Display the configuration of the Event Record function. See Section Event Record Command for details.

Show ip: Display IP-related configuration and status, including system IP settings, DHCP client and snooping, IGMP/MLD snooping, IGMP filtering, multicast settings, and IP source guard information. These commands help monitor multicast behavior and DHCP protection on ports. See Section IP Command for details.

Show ipv6: Display IPv6-related configuration and current IPv6 status of the Managed Switch. Use this command to verify IPv6 addressing and operation. See Section IPv6 Command for details.

Show lldp: Display LLDP (Link Layer Discovery Protocol) settings, per-interface configurations, and current LLDP status. Useful for network topology discovery and neighbor device information. See Section LLDP Command for details.

Show lan-follow-wan: Display the current lan-follow-wan configuration. See Section lan-follow-wan Command for details.

Show loop-detection: Display the current Loop Detection configuration and the status of all or specific ports. Useful for identifying and preventing Layer 2 network loops.
See Section Loop Detection Command for details.

Show led: Display the current state of the LED status light. See Section LED Command for details.

Show mac: Display MAC address table entries, including learned and static MAC addresses, aging time, and per-interface MAC learning settings. Supports sorting and filtering by MAC, VLAN, or port. See Section MAC Command for details.

Show management: Display the management access configuration of the switch, including RADIUS, TACACS+, and authentication method settings.See Section Management Command for details.

Show mirror: Display the port mirroring configuration of the switch. Use this command to verify mirroring settings for traffic monitoring on specific interfaces. See Section Mirror Command for details.

Show ntp: Display the current configuration of the NTP (Network Time Protocol) time server. This command helps ensure accurate time synchronization across the network. See Section NTP Command for details.

Show qos: Display QoS (Quality of Service) configuration, including interface-specific settings, queue statistics, and priority remarking mappings. Use these commands to verify traffic prioritization and bandwidth management. See Section QoS Command for details.

Show security: Display various Layer 2 security settings, including MAC limit, storm protection, link flap detection, port isolation, delay linkup, and L2 protocol filter configurations. These commands help monitor port-level security controls. See Section Security Command for details.

Show sfp: Display SFP module information such as vendor details, operational status, environmental metrics (temperature, voltage, power levels), and threshold settings. Useful for monitoring transceiver health and link integrity. See Section SFP Command for details.

Show snmp-server: Display SNMP server settings including community strings, trap destinations, SNMPv3 user accounts, and trap types. Use these commands to verify SNMP access control and monitoring targets. See Section SNMP Server Command for details.

Show switch: Display the current maximum transmission unit (MTU) configuration, which defines the largest allowable frame size on the switch. See Section Switch MTU Command for details.

Show terminal: Display the current terminal length configuration, which affects how many lines are shown in command-line output before a prompt to continue appears. See Section Terminal Command for details.

Show user: Display local user account configurations, including usernames, roles, and privileges. Useful for auditing access control settings.
See Section User Command for details.

Show vlan: Display VLAN-related configuration including IEEE 802.1Q VLAN table, port-based VLANs, VLAN mappings, interface VLAN assignments, and Selective Q-in-Q settings. Useful for reviewing VLAN membership and tag handling on ports. See Section VLAN Command for details.

Show interface: Display physical interface configuration and statistics, including port status, traffic counters, error analysis, and per-port event/rate metrics. These commands are essential for monitoring interface health and troubleshooting port-related issues. See Section Interface Command for details.

Show diagnostics: Display diagnostics configuration and diagnostics results. See Section diagnostics for details.

3. Show default, running, and startup configurations

Show default configuration:

Show default-config Command	Parameters	Description
Switch(config)# show default-config		Display the system factory default configuration.
Switch(config)# show default-config include [string]	[string]	Specify the keyword to search for the matched information from the system factory default configuration.

Show running configuration:

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

		Switch for the the specific port(s).
Switch(config)# show running-config interface [port_list] include [string]		Specify the keyword to search for the matched information from the running configuration of the specific port(s).

Show start-up configuration:

Show start-up-config Command	Parameters	Description
Switch(config)# show start-up-config		Show the difference between the startup configuration and the default configuration.
Switch(config)# show start-up-config include [string]	[string]	Specify the keyword to search for the matched information from the difference between the startup configuration and the default configuration.
Switch(config)# show start-up-config full		Display the system configuration stored in Flash.
Switch(config)# show start-up-config full include [string]	[string]	Specify the keyword to search for the matched information from the full startup configuration.

4. Display logs:

Show syslog: Display the current syslog configuration including the enable/disable status of each logging type. Use this command to verify system logging settings and troubleshoot log-related issues. See Section Syslog Command for details.

Show log:

Show Log Command	Parameters	Description
Switch(config)# show log		Display the entire event log currently stored in the Managed Switch, by each time showing 10 events from the newest to the oldest.
Switch(config)# show log clear		Remove the entire event log currently stored in the Managed Switch.
Switch#(config) show log index [ID_range]	[ID_range]	Display a certain part of the event log from a specified index to another according to the specified ID range, by each time showing 10 events from the newest to the oldest. **ID range:** Enter a range of event indexes with a hyphen. For example: 2-4 or 4-500
Switch#(config) show log terminal-length [terminal_length]	[terminal_length]	Display the entire event log, by each time showing a specified number of events from the newest to the oldest.
Switch#(config) show log reverse		Display the entire event log, by each time showing 10 events from the

		oldest to the newest.
Switch#(config) show log log-item [exclude | include] [item_list]	[exclude | include]	Display events by filtering out or encompassing events of the specified category.
	[item_list]	Specify the event category from the item list for log filtering. **item_list:** Enter several discontinuous numbers separated by commas or a range of items with a hyphen. For example:1,3 or 2-4 **Note:** Use quick key: a “space” followed by “?” to view the comprehensive item list.
Switch#(config) show log log-item [exclude | include] [item_list] time-range [exclude | include] [ntp-time] start [hh:mm dd MMM yyyy] end [hh:mm dd MMM yyyy]	[exclude | include]	Display events by filtering out or encompassing events of the specified category.
	[item_list]	Specify the event category from the item list for log filtering.
	[exclude | include]	Display events that occurred (didn’t occur) during a specified NTP time period.
	[ntp-time]	Filter the events according to NTP time.
	[hh:mm dd MMM yyyy]	Specify the starting point of an NTP time period. **hh:** 0-23 **mm:** 0-59 **dd:** 1-31 **MMM:** jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec **yyyy:** 2021-2037
	[hh:mm dd MMM yyyy]	Specify the ending point of an NTP time period. **hh:** 0-23 **mm:** 0-59 **dd:** 1-31 **MMM:** jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec **yyyy:** 2021-2037
Switch#(config) show log log-item [exclude | include] [item_list] time-range [exclude | include] [up-time] start [hh:mm dddd] end [hh:mm dddd]	[exclude | include]	Display events by filtering out or encompassing events of the specified category.
	[item_list]	Specify the event category from the item list for log filtering.
	[exclude | include]	Display events that occurred (didn’t occur) during a specified uptime period.
	[up-time]	Filter the events according to the

		Managed Switch’s uptime.
	[hh:mm dddd]	Specify the starting point of a Managed Switch’s uptime period. **hh:** 0-23 **mm:** 0-59 **dddd:** 0-9999
	[hh:mm dddd]	Specify the ending point of a Managed Switch’s uptime period. **hh:** 0-23 **mm:** 0-59 **dddd:** 0-9999

2.5.4 Archive Command

Archive Command	Parameter	Description
Switch(config)# archive auto-backup		Enable the auto-backup configuration files function.
Switch(config)# archive auto-backup path ftp [A.B.C.D | A:B:C:D:E:F:G:H] [file_directory] [user_name] [password]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the IPv4/IPv6 address of the FTP server.
	[file_directory]	Specify the file directory of the FTP server to save the start-up configuration files.
	[user_name]	Specify the user name to login the FTP server.
	[password]	Specify the password for FTP server's authentication.
Switch(config)# archive auto-backup path tftp [A.B.C.D | A:B:C:D:E:F:G:H] [file_directory]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the IP/ IPv6 address of the TFTP server.
	[file_directory]	Specify the file directory of the TFTP server to save the start-up configuration files.
Switch(config)# archive auto-backup time [0-23]	[0-23]	Specify the time to begin the automatic backup of the start-up configuration files everyday.
No command		
Switch(config)# no archive auto-backup		Disable the auto-backup function.
Switch(config)# no archive auto-backup path		Remove TFTP / FTP server settings.
Switch(config)# no archive auto-backup time		Reset the Auto-backup time back to the default (0 o'clock).
Show command		**Description**
Switch# show archive auto-backup		Display the auto-backup configuration.
Switch(config)# show archive auto-backup		Display the auto-backup configuration.

2.5.5 Event-record Command

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

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

2.5.6 IP Command

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

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

2. Enable IPv4 DHCP Auto Recycle function.

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

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

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

4. Enable DHCP client host name assigned by server function.

DHCP client host name assigned-by-server Command	Parameter	Description
Switch(config)# ip dhcp client hostname assigned-by-server		Enable the DHCP client host name assigned by server function. **NOTE:** If the DHCP Option 12 value received from the server differs from the current host name, the system will automatically update the host name in the running configuration based on the received value. To retain the updated host name after a reboot, you must manually save the configuration.
No command		
Switch(config)# no ip dhcp client hostname assigned-by-server		Disable the DHCP client host name assigned by server function.

5. Enable DHCPv4/DHCPv6 relay function.

DHCP Snooping Command	Parameter	Description
Switch(config)# ip dhcp snooping		Enable DHCPv4/DHCPv6 snooping function.
Switch(config)# ip dhcp snooping dhcp-server-ip		Globally enable DHCPv4/DHCPv6 server trust IPv4/IPv6 address.
Switch(config)# ip dhcp snooping dhcp-server-ip [1-4] ip-address [A.B.C.D | A:B:C:D:E:F:G:H]	[1-4]	Specify DHCPv4/DHCPv6 server trust IPv4/IPv6 address number.
	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify DHCPv4/ DHCPv6 server trust IPv4/IPv6 address.
Switch(config)# ip dhcp snooping initiated [0-9999]	[0-9999]	Specify the DHCPv4/DHCPv6 snooping Initiated Time value (0~9999 seconds) that packets might be received.
Switch(config)# ip dhcp snooping leased [180-259200]	[180-259200]	Specify the DHCPv4/DHCPv6 snooping Leased Time for DHCP clients. (Range:180~259200 seconds).
Switch(config)# ip dhcp snooping option		Globally enable DHCPv4 Option 82 / DHCPv6 Option 37 relay agent.
Switch(config)# ip dhcp snooping remote		Globally enable DHCPv4 Option 82 / DHCPv6 Option 37 Manual Remote Id.
Switch(config)# ip dhcp snooping remote formatted		Enable the Formatted DHCPv4 Option 82 / DHCPv6 Option 37 Remote Id.
Switch(config)# ip dhcp snooping remote id [remote_id]	[remote_id]	You can configure the DHCPv4 Option 82 / DHCPv6 Option 37 remote ID to be a string of up to 63 characters. The default remote ID is the switch's MAC address.
No command		
Switch(config)# no ip dhcp snooping		Disable DHCPv4/DHCPv6 snooping function.
Switch(config)# no ip dhcp snooping dhcp-server-ip		Globally disable DHCPv4/DHCPv6 server trust IPv4/IPv6 address.
Switch(config)# no ip dhcp snooping dhcp-server-ip [1-4] ip-address		Remove DHCPv4/DHCPv6 server trust IPv4/IPv6 address from the specified trust IPv4/IPv6 address number.
Switch(config)# no ip dhcp snooping initiated		Reset the initiated time value back to the default. (4 seconds)
Switch(config)# no ip dhcp snooping leased		Reset the leased time value back to the default.(86400 seconds)
Switch(config)# no ip dhcp snooping option		Disable DHCPv4 Option 82 / DHCPv6 Option 37 relay agent.
Switch(config)# no ip dhcp snooping remote		Globally disable DHCPv4 Option 82 / DHCPv6 Option 37 Manual Remote Id.
Switch(config)# no ip dhcp snooping remote formatted		Disable the Formatted DHCPv4 Option 82 / DHCPv6 Option 37 Remote Id.
Switch(config)# no ip dhcp snooping remote id		Clear Remote ID description.
Show command		
Switch(config)# show ip dhcp snooping		Show DHCPv4/DHCPv6 snooping configuration.

Switch(config)# show ip dhcp snooping interface		Show each port's DHCP Snooping Option 82/Option 37 and trust port settings.
Switch(config)# show ip dhcp snooping interface [port_list]	[port_list]	Show the specified port's DHCP Snooping Option 82/Option 37 and trust port settings.
Switch(config)# show ip dhcp snooping opt82 circuit		Show each port's DHCP snooping opt82 Circuit ID.
Switch(config)# show ip dhcp snooping opt82 circuit [port_list]	[port_list]	Show the specified port's DHCP snooping opt82 Circuit ID.
Switch(config)# show ip dhcp snooping opt82 remote		Show DHCP snooping opt82 Remote ID.
Switch(config)# show ip dhcp snooping status		Show DHCPv4/DHCPv6 snooping current status.
Examples of IP DHCP Snooping		
Switch(config)# ip dhcp snooping		Enable DHCP snooping function.
Switch(config)# ip dhcp snooping initiated 10		Specify the time value that packets might be received to 10 seconds.
Switch(config)# ip dhcp snooping leased 240		Specify packets' expired time to 240 seconds.
Switch(config)# ip dhcp snooping option		Enable DHCP Option 82 Relay Agent.
Switch(config)# ip dhcp snooping remote id 123		The remote ID is configured as "123".

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

DHCP Snooping & Interface Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# ip dhcp snooping circuit		Enable the selected interfaces' DHCPv4 Option 82 / DHCPv6 Option 37 Manual Circuit Id.
Switch(config-if-PORT-PORT)# ip dhcp snooping circuit formatted		Enable the Formatted DHCPv4 Option 82 / DHCPv6 Option 37 Circuit Id for the selected interfaces.
Switch(config-if-PORT-PORT)# ip dhcp snooping circuit id [circuit_id]	[circuit_id]	Specify the VLAN and port identifier using a VLAN ID in the range of 1 to 4094 as DHCPv4 Option 82 / DHCPv6 Option 37 Circuit ID. Besides, you can configure the circuit ID to be a string of up to 63 characters.
Switch(config-if-PORT-PORT)# ip dhcp snooping option		Enable the selected interfaces' DHCPv4 Option 82 / DHCPv6 Option 37 relay agent.
Switch(config-if-PORT-PORT)# ip dhcp snooping trust		Enable the selected interfaces as DHCPv4 Option 82 / DHCPv6 Option 37 trust ports.

Switch(config-if-PORT-PORT)# ip dhcp snooping server-trust		Enable the selected interfaces as DHCPv4/DHCPv6 server trust ports. **Note: A port / ports cannot be configured as option 82/option 37 trust and server trust at the same time.**
No command		
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit		Disable the selected interfaces' DHCPv4 Option 82 / DHCPv6 Option 37 Manual Circuit Id.
Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit formatted		Disable the Formatted DHCPv4 Option 82 / DHCPv6 Option 37 Circuit Id for the selected interfaces.
Switch(config-if-PORT-PORT)# no ip dhcp snooping circuit id		Clear DHCPv4 Option 82 / DHCPv6 Option 37 Circuit Id.
Switch(config-if-PORT-PORT)# no ip dhcp snooping option		Disable the selected interfaces' DHCPv4 Option 82 / DHCPv6 Option 37 relay agent.
Switch(config-if-PORT-PORT)# no ip dhcp snooping trust		Reset the selected interfaces back to non-DHCPv4 Option 82 / DHCPv6 Option 37 trust ports.
Switch(config-if-PORT-PORT)# no ip dhcp snooping server-trust		Reset the selected interfaces back to non-DHCPv4/DHCPv6 server trust ports.
Examples of DHCP Snooping & Interface		
Switch(config)# interface 1-3		Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-1-3)# ip dhcp snooping option		Enable DHCPv4 Option 82 / DHCPv6 Option 37 relay agent for Port 1~3.
Switch(config-if-1-3)# ip dhcp snooping trust		Configure Port 1~3 as DHCPv4 Option 82 / DHCPv6 Option 37 trust ports.

7. Enable or disable IGMP/MLD snooping globally.

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

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

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

IGMP snooping can very effectively reduce multicast traffic from streaming and other bandwidth intensive IP applications. A switch using IGMP snooping will only forward multicast traffic to the

hosts interested in that traffic. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also reduces the workload at the end hosts since their network cards (or operating system) will not have to receive and filter all the multicast traffic generated in the network.

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

IGMP/MLD Snooping Command	Parameter	Description
Switch(config)# ip igmp snooping		Enable IGMP/MLD snooping. When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic. This is for IGMPv1, v2 and MLDv1 only.
Switch(config)# ip igmp snooping version-3		Enable IGMPv3/MLDv2 snooping. When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic. This is for IGMPv3 and MLDv2 only.
Switch(config)# ip igmp snooping immediate-leave		Enable immediate leave function.
Switch(config)# ip igmp snooping stream-life-time		Enable IGMP/MLD snooping stream life time function. The multicast packet stream will be stopped once reaching the end of its specified lifespan. **Note:** **The length of stream life time is determined by the total amount of the specified query-interval and max-response-time (125 and 10 seconds in default, respectively).**
Switch(config)# ip igmp snooping max-response-time [1-255]	[1-255] (Unit:1/10secs)	Specify the IGMP/MLD querier maximum response time. This determines the maximum amount of time can be allowed before sending an IGMP/MLD response report.
Switch(config)# ip igmp snooping query-interval [1-6000]	[1-6000]	Specify the query time interval of IGMP/MLD querier. This is used to set up the time interval between transmitting IGMP/MLD queries. (Range:1-6000 seconds)
Switch(config)# ip igmp snooping vlan [1-4094]	[1-4094]	Specify a VLAN ID. This enables IGMP/MLD Snooping for the specified VLAN.
Switch(config)# ip igmp snooping vlan [1-4094] query	[1-4094]	Enable a querier for the specified VLAN.
No command		
Switch(config)# no ip igmp snooping		Disable IGMP/MLD snooping function.
Switch(config)# no ip igmp snooping immediate-leave		Disable immediate leave function.

Switch(config)# no ip igmp snooping stream-life-time		Disable IGMP/MLD snooping stream life time function.
Switch(config)# no ip igmp snooping max-response-time		Reset the IGMP/MLD querier maximum response time back to the default.
Switch(config)# no ip igmp snooping query-interval		Reset the query time interval value back to the default. (100 seconds)
Switch(config)# no ip igmp snooping version-3		Disable IGMPv3/MLDv2 snooping.
Switch(config)# no ip igmp snooping vlan [1-4094]	[1-4094]	Disable IGMP/MLD snooping for the specified VLAN.
Switch(config)# no ip igmp snooping vlan [1-4094] query	[1-4094]	Disable a querier for the specified VLAN.
Show command		
Switch(config)# show ip igmp snooping		Show the current IGMP/MLD snooping configuration.
Switch(config)# show ip igmp snooping groups		Show IGMP snooping groups table.
Switch(config)# show ip igmp snooping status		Show IGMP Snooping status.
Switch(config)# show ip mld snooping groups		Show MLD snooping groups table.
Switch(config)# show ip mld snooping status		Show MLD Snooping status.

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

IGMP/MLD Snooping & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# ip igmp snooping mcast-router		Specify the selected port(s) as the multicast router port.
No command		
Switch(config-if-PORT-PORT)# no ip igmp snooping mcast-router		Remove the selected port(s) from the multicast router port list.
Examples of IP IGMP Snooping & Interface		
Switch(config)# interface 4,5		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-4,5)# ip igmp snooping mcast-router		Configure Port 4,5 as the multicast router port.

9. Set Up IP Source Binding Function.

IP Source Binding Command	Parameter	Description
Switch(config)# ip source binding [1-5] ip-address [A.B.C.D | A:B:C:D:E:F:G:H]	[1-5]	Specify the IPv4/IPv6 address security binding number.
	[A.B.C.D |	Specify IPv4/IPv6 address.

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

2.5.7 IPv6 Command

Brief Introduction to IPv6 Addressing

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

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

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

Stateless Autoconfiguration

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

Autoconfigured address format

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

Link local address

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

Global address

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

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

DHCPv6

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

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

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

	Switch.
Examples of IPv6 command	
Switch(config)# ipv6 address autoconfig	Enable IPv6 autoconfiguration.
Switch(config)# ipv6 address dhcp auto	Enable DHCPv6 auto mode.
Switch(config)# ipv6 enable	Enable IPv6 address processing.

2.5.8 lan-follow-wan Command

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

1. Set up LAN ports.

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

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

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

2.5.9 LLDP Command

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

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

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

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

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

2.5.10 Loop Detection Command

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

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

1. It blocks the relevant port to prevent broadcast storms, and send out SNMP trap to inform the network administrator. In other words, the system stops forwarding all the traffic via the looped port, and the system will not process any packets received on the looped port.
2. The LED of the looped port will be OFF.
3. Until the configured time of Unlock Interval ends, it periodically sends loop detection packets to detect the existence of loop condition.

When the system does not receive any loop detection packet from itself for a period of configured **Unlock Interval**. The system claims the loop condition disappears. Then, the system takes the following actions:

1. It does not unlock the relevant port until the configured time of **Unlock Interval** ends. In other words, the system normally forwards all the traffic via the relevant port.
2. The LED of the looped port returns into the normal status.
3. It periodically sends loop detection packets to detect the existence of loop condition.

Command	Parameter	Description
Switch(config)# loop-detection		Enable Loop Detection function.
Switch(config)# loop-detection unlock-interval [1-1440]	[1-1440]	This is the time interval for the system to detect the existence of loop condition. System un-blocks the looped port if it does not receive any loop-detection packet when the configured Unlock Interval ends. The unlock-interval can be set from 1 to 1440 minutes. The default setting is 1 minutes.
No command		
Switch(config)# no loop-detection		Disable Loop Detection function.
Switch(config)# no loop-detection unlock-interval		Reset Loop Detection unlock time interval back to the default.
Show command		
Switch(config)# show loop-detection		Show Loop Detection configuration.
Switch(config)# show loop-detection status		Show Loop Detection status of all ports.
Switch(config)# show loop-detection status [port_list]	[port_list]	Show Loop Detection status of specified port(s).
Examples of Loop Detection command		
Switch(config)# loop-detection unlock-interval 120		Set the Loop Detection unlock time interval to 120 minutes.
Switch(config)# loop-detection		Enable Loop Detection function.

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

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

2.5.11 LED Command

Users can turn on and off the LED status light on the top panel of the Managed Switch remotely by toggling between the on and off state of the LED status light.

LED Command	Parameter	Description
Switch(config)# led control state [off | on]	[off | on]	Enable or disable the LED status light. When disabled, the status light of the System Status LED and Port Link LEDs will be turned off. However, the Power LED indicator will always stay on regardless of the LED State configuration.
No Command		
Switch(config)# no led control state		Reset the state of the LED status light to the default (on).
Show Command		**Description**
Switch(config)# show led control		Show the current state of the LED status light.

2.5.12 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 [0-458s]	[0-458s]	Specify MAC address table aging time between 0 and 458 seconds. "0" means that MAC addresses will never age out.

No command		
Switch(config)# no mac address-table aging-time		Reset MAC address table aging time back to the default. (300 seconds).
Show command		
Switch(config)# show mac address-table all		Show all of MAC table information.
Switch(config)# show mac address-table all [mac | vid | port]	[mac | vid | port]	Show all learned MAC addresses sorted by specific option.
Switch(config)# show mac address-table clear		Clear MAC address table.
Switch(config)# show mac address-table clear [port_list]	[port_list]	Clear MAC addresses learned by the specified port.
Switch(config)# show mac address-table count		Show the statistics of MAC address table.
Switch(config)# show mac address-table interface [port_list] [mac | vid | port]	[port_list]	Show the MAC addresses learned by the specified port.
	[mac | vid | port]	Show the learned MAC addresses sorted by specific option.
Switch(config)# show mac address-table mac [xx:xx:xx | xx:xx:xx:xx:xx:xx] [mac | vid | port]	[xx:xx:xx]	Show the MAC address that its first 3 bytes starting with the specified MAC.
	[xx:xx:xx:xx:xx:xx]	Show the MAC address that its 6 bytes totally meet the specified MAC.
	[mac | vid | port]	Show the matched MAC addresses sorted by specific option.
Switch(config)# show mac address-table vlan [vlan_id] [mac | vid | port]	[vlan_id]	Show the MAC addresses that belongs to the specified VLAN ID.
	[mac | vid | port]	Show the specified VLAN's MAC addresses sorted by specific option.
Switch(config)# show mac learning		Show MAC learning setting of each interface.
Switch(config)# show mac aging-time		Show the current MAC address aging time.
Examples of MAC command		
Switch(config)# mac address-table aging-time 200		Set MAC address aging time to 200 seconds.

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

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

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

Show mac filter Command	Parameter	Description
Switch(config)# show mac filter type [static | dynamic] sort-by [mac | port | vlan]	[static | dynamic]	Display the current MAC addresses that are either static or dynamic. **Note:** **To display both static and dynamic MAC addresses at the same time, simply skip this command.**
	[mac | port | vlan]	(Optional) Specify one particular sorting option to arrange the MAC address table. Entries will be displayed in ascending order according to the specified sort-by method.
Switch(config)# show mac filter mac [include | exclude] mac-address [xx:xx:xx:xx:xx:xx] mac-mask [xx:xx:xx:xx:xx:xx] sort-by [mac | port | vlan]	[include | exclude]	Display the intended MAC addresses that (don't) correspond to the result of the comparison between the specified MAC address and the specified MAC address mask.
	[xx:xx:xx:xx:xx:xx]	Specify a MAC address to allow the filter to compare it against the specified MAC address mask.
	[xx:xx:xx:xx:xx:xx]	Specify a MAC address mask to allow the filter to compare it against the specified MAC address. **mac-mask:** It indicates how many bits, from left to right, the filter checks against the MAC address. To require an exact match with the MAC address (to check all 48 bits), enter FF:FF:FF:FF:FF:FF; to check only the first 32 bits, enter FF:FF:FF:FF:00:00.
	[mac | port | vlan]	(Optional) Specify one particular sorting option to arrange the MAC address table. Entries will be displayed in ascending order according to the specified sort-by method.
Switch#(config) show mac filter port-list [include | exclude] [port-list] sort-by [mac | port | vlan]	[include | exclude]	Display the intended MAC addresses that (don't) correspond to the comparison result between the specified MAC address and the specified MAC address mask.
	[port-list]	Specify the port from which the intended MAC addresses were learned. Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
	[mac | port | vlan]	(Optional) Specify one particular sorting option to arrange the MAC

		address table. Entries will be displayed in ascending order according to the specified sort-by method.
Switch#(config) show mac filter vlan [include | exclude] [vlan-id] sort-by [mac | port | vlan]	[include | exclude]	Display the MAC addresses that belong to the specified VLAN ID.
	[1-4094]	Specify a single VLAN ID to which the intended MAC addresses belong.
	[mac | port | vlan]	(Optional) Specify one particular sorting option to arrange the MAC address table. Entries will be displayed in ascending order according to the specified sort-by method.

Example of show mac filter Command	Description
Switch#(config) show mac filter type static vlan include 5 sort-by port	Only the static MAC addresses that belong to VLAN 5 will be displayed, and the MAC address table will be displayed in a way that MAC addresses learned by the same port are grouped together and arranged in ascending order.
Switch#(config) show mac filter type dynamic mac exclude mac-address 9C:EB:E8:EA:5E:84 mac-mask FF:FF:FF:00:00:00 port-list include 5-10 vlan exclude 100	Only the dynamic MAC addresses of which the first 6 digits are not “9C:EB:E8” will be displayed, yet MAC addresses that belong to VLAN 100 and learned not by port 5, 6, 7, 8, 9, and 10 will not be displayed.

2.5.13 Management Command

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

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

Switch(config)# management web [http | https | disable]	[http | https | disable]	Enable or disable Web Management. You can enable this management and manage the Managed Switch via the specified web management method between http and https.
Switch(config)# management web timeout [1-1440]	[1-1440]	To disconnect the Managed Switch when web management is inactive for a certain period of time. The allowable value is from 1 to 1440 (minutes).
No command		
Switch(config)# no management cli timeout		Reset cli timeout value back to the default (300 seconds).
Switch(config)# no management ssh		Disable SSH management.
Switch(config)# no management telnet		Disable Telnet management.
Switch(config)# no management telnet port		Reset Telnet port back to the default. The default port number is 23.
Switch(config)# no management web		Disable Web management.
Switch(config)# no management web timeout		Reset web timeout value back to the default (20 minutes).
Show command		
Switch(config)# show management		Show the current management configuration of the Managed Switch.
Examples of Management command		
Switch(config)# management telnet		Enable Telnet management.
Switch(config)# management telnet port 23		Set Telnet port to port 23.

Configure RADIUS server authentication method.

Management Radius Command	Parameter	Description
Switch(config)# management radius secret-key-encryption [aes-128]	[aes-128]	Specify AES-128 as the encryption method to secure the secret key against potential malicious attacks. **aes-128 (advanced encryption method):** An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data.
Switch(config)# management radius retry-time [0-3]	[0-3]	Specify the retry time value. This is the number of times that the Managed Switch will try to reauthenticate if the RADIUS server is not reachable.
Switch(config)# management radius timeout [1-3]	[1-3]	Specify the timeout value (second). This is the amount of time that the Managed Switch will wait if the RADIUS server is not responding.
Switch(config)# management radius [1-2]	[1-2]	Specify a RADIUS server number to configure.

Switch(config-radius-NUMBER)# enable		Enable the RADIUS server.
Switch(config-radius-NUMBER)# port [1025-65535]	[1025-65535]	Specify the RADIUS server's port number.
Switch(config-radius-NUMBER)# secret [secret]	[secret]	Specify a secret, up to 32 alphanumeric characters, for the RADIUS server. This secret key is used to validate communications with the RADIUS server.
Switch(config-radius-NUMBER)# secret aes-128 [base64]	[base64]	Specify the secret encrypted by aes-128. **aes-128 (advanced encryption method):** An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data.
Switch(config-radius-NUMBER)# server-ip [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the RADIUS server's IPv4/IPv6 address.
No Command		
witch(config)# no management radius secret-key-encryption		Disable encryption on RADIUS secret key.
Switch(config)# no management radius retry-time		Reset the RADIUS server retry time setting back to default.
Switch(config)# no management radius timeout		Reset the RADIUS server timeout setting back to default.
Switch(config-radius-NUMBER)# no enable		Disable the RADIUS server.
Switch(config-radius-NUMBER)# no port		Reset the radius port setting back to default (port number 1812).
Switch(config-radius-NUMBER)# no secret		Remove the configured secret value of the RADIUS server.
Switch(config-radius-NUMBER)# no server-ip		Delete the IPv4/IPv6 address of the RADIUS server.
Show Command		
Switch(config)# show management radius		Show the current configuration of both 1st and 2nd RADIUS servers.
Switch(config)# show management radius 1		Show the current configuration of the 1st RADIUS server.
Switch(config)# show management radius 2		Show the current configuration of the 2nd RADIUS server.
Examples of Management Radius Command		
Switch(config)# management radius retry-time 2		Set the retry time value to 2. The Managed Switch will try to authenticate twice if the RADIUS server is not reachable.
Switch(config)# management radius timeout 3		If the RADIUS server is not responding, the Managed Switch will wait 3 seconds before determining the authentication as timeout.
Switch(config)# management radius 2		Entering server number 2 will direct you to the configuration of 2nd

	RADIUS server
Switch(config-radius-2)# enable	Enable the 2nd RADIUS server.
Switch(config-radius-2)# port 1812	Set the 2nd RADIUS server port number as 1812.
Switch(config-radius-2)# secret abcxyzabc	Set up “abcxyzabc” as the secret key for validating communications with the 2nd RADIUS server.
Switch(config-radius-2)# server-ip 192.180.3.2	Set the 2nd RADIUS server address to 192.180.3.2.

Configure TACACS+ server authentication method.

Management Tacacs Command	Parameter	Description
Switch(config)# management tacacs secret-key-encryption [aes-128]	[aes-128]	Specify AES-128 as the encryption method to secure the secret key against potential malicious attacks. **aes-128 (advanced encryption method):** An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data.
Switch(config)# management tacacs retry-time [0-3]	[0-3]	Specify the retry time value. This is the number of times that the Managed Switch will try to reauthenticate if the TACACS+ server is not reachable.
Switch(config)# management tacacs timeout [1-3]	[1-3]	Specify the timeout value (second). This is the amount of time that the Managed Switch will wait if the TACACS+ server is not responding.
Switch(config)# management tacacs [1-2]	[1-2]	Specify a TACACS+ server number to configure.
Switch(config-tacacs-NUMBER)# enable		Enable the TACACS+ server.
Switch(config-tacacs-NUMBER)# port [49, 1025-65535]	[49, 1025-65535]	Specify the TACACS+ server’s port number.
Switch(config-tacacs-NUMBER)# secret [secret]	[secret]	Specify a secret, up to 32 alphanumeric characters, for the TACACS+ server. This secret key is used to validate communications with the TACACS+ server.
Switch(config-tacacs-NUMBER)# secret aes-128 [base64]	[base64]	Specify the secret encrypted by aes-128. aes-128 (advanced encryption method): An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data.

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

Configure authentication method management.

Management Command	Parameter	Description

Switch(config)# management authentication continue		Enable “Continue to the Next Method” on the authentication method function. Any user accessing the Managed Switch will be authenticated against the specified method scheme. **Note:** **Once this function is enabled, the Managed Switch will continue to the next method if the first authentication fails, say, due to invalid client credentials. It indeed delivers extra flexibility for an ought-to-be-authenticated user, yet at the expense of network security. To fully protect against malicious users, it’s recommended to set this function disabled.**
Switch(config)# management authentication all [method 1] [method 2] [method 3] [method 4] [method 5]	[disable | local | radius1 | radius2 | tacacs1 | tacacs2]	Configure the authentication method scheme for all interfaces, including Telnet, SSH and Web. **Note:** **Each method can be configured as disable, local, radius1, radius2, tacacs1, or tacacs2. However, local must be set after RADIUS and TACACS+ servers throughout the specified method scheme, and the 1st method cannot be configured as disable.**
No Command		
Switch(config)# no management authentication continue		Disable “Continue to the Next Method” on the authentication method function. **Note:** **Disabling this function means the device will only apply method 1. Access will be denied to those who fail the authentication against the 1st method.**
Switch(config)# no management authentication all		Reset the authencation method scheme back to default (method 1 as local, and the remainder as disable).
Show Command		
Switch(config)# show management authentication		Show the current configuration of the authentication method function.
Examples of Management Command		
Switch(config)# management authentication continue		Enable “Continue to the Next Method” on the authentication method function.

Switch(config)# management authentication all [tacacs2] [radius1] [tacacs1] [radius2] [local]	A user will be first authenticated by the 2nd TACACS+ server which you specified earlier. However, if the authentication fails, the device will move on to the next method (in this case, the 1st RADIUS server), and applies the third method (the 1st TACACS+ server) if the second authentication fails.

2.5.14 Mirror Command

Mirror Command	Parameter	Description
Switch(config)# mirror		Globally enable Port Mirroring function.
Switch(config)# mirror index [1]	[1]	Specify the index of port mirroring you would like to configure. Up to 1 set of port mirroring can be set up.
Switch (config-mirror-index)# enable		Enable the specified port mirroring. **NOTE: This command works only when its mirroring-related settings are completed.**
Switch(config-mirror-index)# destination [port_number]	[port_number]	Specify the preferred destination port for port mirroring.
Switch(config-mirror-index)# source [port_number] direction [tx | rx | both]	[port_number] [tx | rx | both]	Specify the source port number(s) and TX/RX/both direction for port mirroring. **NOTE: The port selected as the destination port cannot be the source port.**
No command		
Switch(config)# no mirror		Globally disable Port Mirroring function.
Switch(config)# no mirror index [1]	[1]	Clear the settings of the specified port mirroring.
Switch (config-mirror-index)# no enable		Disable the specified port mirroring.
Switch(config-mirror-index)# no destination		Reset the mirroring destination port back to the default. (Port 1)
Switch(config-mirror-index)# no source [port_number] direction [tx | rx | both]	[port_number] [tx | rx | both]	Remove the source port number(s) and TX/RX/both direction from the port mirroring list.
Show command		
Switch(config)# show mirror		Show the current port mirroring configuration.
Switch(config-mirror-index)# show		Show the current configuration of the specified port mirroring.
Example of Mirror command		
Switch(config-mirror-1)# destination 3		The selected source ports' data will mirror to Port 3 in the port mirroring of Index No. 1.
Switch(config-mirror-1)# source 1 direction tx		Port 1's transmitting packets will mirror to the destination port in the port mirroring of Index No. 1.
Switch(config-mirror-1)# enable		Enable the specified port mirroring.

2.5.15 NTP Command

NTP Command	Parameter	Description
Switch(config)# ntp		Enable Network Time Protocol to have Managed Switch's system time synchronize with NTP time server.
Switch(config)# ntp daylight-saving [recurring | date]	[recurring]	Enable daylight saving function with recurring mode.
	[date]	Enable daylight saving function with date mode.
Switch(config)# ntp offset [Mm,w,d,hh:mm-Mm,w,d,hh:mm]	[Mm,w,d,hh:mm-Mm,w,d,hh:mm]	Specify the offset of daylight saving in recurring mode. **Mm=1-12, w=1-5, d=0-6(0=Sun, 6=Sat) Hh=0-23, mm=0-59, Days=1-365**
Switch(config)# ntp offset [Days,hh:mm-Days,hh:mm]	[Days,hh:mm-Days,hh:mm]	Specify the offset of daylight saving in date mode. **Mm=1-12, w=1-5, d=0-6(0=Sun, 6=Sat) Hh=0-23, mm=0-59, Days=1-365**
Switch(config)# ntp server1 [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the primary NTP time server's IPv4/IPv6 address.
Switch(config)# ntp server2 [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F:G:H]	Specify the secondary NTP time server's IPv4/IPv6 address.
Switch(config)# ntp syn-interval [1-8]	[1-8]	Specify the time interval to have Managed Switch synchronize with NTP time server. **1=1hour, 2=2hours, 3=3hours, 4=4hours, 5=6hours, 6=8hours, 7=12hours, 8=24hours**
Switch(config)# ntp time-zone [0-135]	[0-135]	Specify the time zone to which the Managed Switch belongs. Use space and a question mark to view the complete code list of 136 time zones. For example, "Switch(config)# ntp time-zone ?"
No command		
Switch(config)# no ntp		Disable Network Time Protocol to stop Managed Switch's system time synchronizing with NTP time server.
Switch(config)# no ntp daylight-saving		Disable the daylight saving function.
Switch(config)# no ntp offset		Reset the offset value back to the default.
Switch(config)# no ntp server1		Delete the primary time server's IPv4/IPv6 address.
Switch(config)# no ntp server2		Delete the secondary time server's IPv4/IPv6 address.
Switch(config)# no ntp syn-interval		Reset the synchronization time interval back to the default.

Switch(config)# no ntp time-zone	Reset the time-zone setting back to the default.
Show command	
Switch# show ntp	Show the current NTP time server configuration.
Switch(config)# show ntp	Show the current NTP time server configuration.
Examples of NTP command	
Switch(config)# ntp	Enable NTP function for the Managed Switch.
Switch(config)# ntp daylight-saving date	Enable the daylight saving function in date mode.
Switch(config)# ntp offset [100,12:00-101,12:00]	Daylight saving time date start from the 100th day of the year to the 101th day of the year.
Switch(config)# ntp server1 192.180.0.12	Set the primary NTP time server's IP address to 192.180.0.12.
Switch(config)# ntp server2 192.180.0.13	Set the secondary NTP time server's IP address to 192.180.0.13.
Switch(config)# ntp syn-interval 4	Set the synchronization interval to 4 hours.
Switch(config)# ntp time-zone 3	Set the time zone to GMT-8:00 Vancouver.

2.5.16 QoS Command

1. Specify the desired QoS mode.

QoS command	Parameter	Description
Switch(config)# qos [port-based | 802.1p | dscp]	[port-based | 802.1p | dscp]	Specify one QoS mode. **port-based:** Use "*interface"* command to assign a queue to the selected interfaces. **802.1p:** Use *"qos 802.1p-map"* command to assign priority bits to a queue. **dscp:** Use "*qos dscp-map"* to assign the DSCP value to a queue.
No command		
Switch(config)# no qos		Disable QoS function.
Show command		
Switch(config)# show qos		Show or verify QoS configurations.
QoS command example		
Switch(config)# qos 802.1p		Enable QoS function and use 802.1p mode.
Switch(config)# qos dscp		Enable QoS function and use DSCP mode.
Switch(config)# qos port-based		Enable QoS function and use port-based mode.

2. Set up the DSCP and queue mapping.

DSCP-map command	Parameter	Description
Switch(config)# qos dscp-map [0-63] [0-7]	[0-63]	Specify the corresponding DSCP value you want to map to a priority queue.
	[0-7]	Specify a queue to which the DSCP value is assigned.
No command		
Switch(config)# no qos dscp-map [0-63]	[0-63]	Set the specific DSCP value's queue mapping back to the default setting.
DSCP-map example		
Switch(config)# qos dscp-map 50 3		Mapping DSCP value 50 to priority queue 3.

3. Set up management traffic priority and port user priority.

Management-priority command	Parameter	Description
Switch(config)# qos management-priority [0-7]	[0-7]	Specify 802.1p priority bit for the management traffic.
Port user priority command		
Switch(config-if-PORT-PORT)# qos user-priority [0-7]	[0-7]	Specify the user priority between 0 and 7 for the ports.
No command		
Switch(config)# no qos management-priority		Set the priority bit setting of the management traffic back to the default.
Switch(config-if-PORT-PORT)# no qos user-priority		Set the selected ports' user priority setting back to the default.
Show command		
Switch(config)# show qos		Show QoS and user priority configuration.
Switch(config)# show qos interface		Show QoS interface overall information.
Switch(config)# show qos interface [port-list]	[port-list]	Show the specific QoS interface information.
Management-priority example		
Switch(config)# qos management-priority 4		Set the priority bit of the management traffic to 4.
Port user priority example		
Switch(config)# interface 1-3		Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen.
Switch(config-if-1-3)# qos user-priority 3		Set the user priority to 3 for the selected ports.

4. Set up QoS queuing mode.

Queuing-mode command	Parameter	Description
Switch(config)# qos queuing-mode [weight | strict]	[weight | strict]	By default, "strict" queuing mode is used. If you want to use "weight" queuing mode, you need to disable "strict" mode.

		Strict mode: Traffic assigned to queue 3 will be transmitted first, and the traffic assigned to queue 2 will not be transmitted until queue 3's traffic is all transmitted, and so forth. **Weight mode**: All queues have fair opportunity of dispatching. Each queue has the specific amount of bandwidth according to its assigned weight.
Switch(config)# qos queue-weighted [1:2:4:8:16:32:64:127]	[1:2:4:8:16:32:64:127]	Specify the queue weighted.
No command		
Switch(config)# no qos queuing-mode		Set the queuing mode to the strict mode.
Switch(config)# no qos queue-weighted		Reset the queue weighted value back to the default.
Show command		
Switch(config)# show qos		Show or verify QoS configurations.
Queuing-mode example		
Switch(config)# qos queuing-mode weight		Set the queuing mode to the weight mode.

5. Set up 802.1p and DSCP remarking

Remarking command	Parameter	Description
Switch(config)# qos remarking dscp		Globally enable DSCP remarking.
Switch(config)# qos remarking dscp-map [1-8]	[1-8]	Specify the DSCP and priority mapping ID.
Switch (config-dscp-map-ID)# new-dscp [0-63]	[0-63]	Specify the new DSCP bit value for the selected priority mapping ID.
Switch (config-dscp-map-ID)# rx-dscp [0-63]	[0-63]	Specify the received DSCP bit value for the selected priority mapping ID.
Switch(config)# qos remarking 802.1p		Globally enable 802.1p remarking.
Switch(config)# qos remarking 802.1p-map [1-8]	[1-8]	Specify the 802.1p and priority mapping ID.
Switch (config-802.1p-map-ID)# priority [0-7]	[0-7]	Specify the new 802.1p bit value for the selected priority mapping ID.
No command		
Switch(config)# no qos remarking dscp		Globally disable DSCP remarking.
Switch(config)# no qos remarking dscp-map [1-8]	[1-8]	Reset the DSCP remaking for the specified priority mapping ID back to the default.
Switch (config-dscp-map-ID)# no new-dscp		Reset the new DSCP bit value for the selected priority mapping ID back to the default.

Switch (config-dscp-map-ID)# no rx-dscp		Reset the received DSCP bit value for the selected priority mapping ID back to the default.
Switch(config)# no qos remarking 802.1p		Globally disable 802.1p bit remarking.
Switch(config)# no qos remarking 802.1p-map [1-8]	[1-8]	Reset the 802.1p remaking for the specified priority mapping ID back to the default.
Switch (config-802.1p-map-ID)# no priority		Reset the new 802.1p bit value for the selected priority mapping ID back to the default.
Show command		
Switch(config)# show qos remarking		Show QoS remarking-mapping information.
Switch (config-dscp-map-ID)# show		Show the DSCP mapping configuration for the selected priority mapping ID.
Switch (config-802.1p-map-ID)# show		Show the 802.1p mapping configuration for the selected priority mapping ID.

6. Assign a tag priority to the specific queue.

802.1p-map command	Parameter	Description
Switch(config)# qos 802.1p-map [0-7] [0-7]	[0-7]	Assign an 802.1p priority bit or several 802.1p priority bits for mapping.
	[0-7]	Assign a queue value for mapping.
No command		
Switch(config)# no qos 802.1p-map [0-7]	[0-7]	Assign an 802.1p priority bit or several 802.1p priority bits that you want to delete or remove.
Show command		
Switch(config)# show qos		Show or verify QoS configurations.
802.1p-map example		
Switch(config)# qos 802.1p-map 6-7 3		Map priority bit 6 and 7 to queue 4.
Switch(config)# no qos 802.1p-map 6-7		Delete or remove 802.1p priority bit 6 and 7's mapping.

7. Use interface command to set up ingress and egress rate limit.

QoS & Interface Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# qos rate-limit ingress		Enable QoS ingress rate limit settings.
Switch(config-if-PORT-PORT)# qos rate-limit ingress rate [500-1000000 | 1-1000] Kbps/Mbps	[500-1000000 | 1-1000] Kbps/Mbps	Specify the ingress rate limit value. (Valid range is from 500-1000000 in unit of Kbps or 1-1000 in unit of Mbps).
Switch(config-if-PORT-PORT)# qos rate-limit ingress unit [Kbps |	[Kbps | Mbps]	Specify the unit of the ingress rate limit between Kbps and Mbps.

Mbps]		
Switch(config-if-PORT-PORT)# qos rate-limit egress		Enable QoS egress rate limit settings.
Switch(config-if-PORT-PORT)# qos rate-limit egress rate [500-1000000 | 1-1000] Kbps/Mbps	[500-1000000 | 1-1000] Kbps/Mbps	Specify the egress rate limit value. (Valid range is from 500-1000000 in unit of Kbps or 1-1000 in unit of Mbps).
Switch(config-if-PORT-PORT)# qos rate-limit egress unit [Kbps | Mbps]	[Kbps | Mbps]	Specify the unit of the egress rate limit between Kbps and Mbps.
Switch(config-if-PORT-PORT)# qos user-priority [0-7]	[0-7]	Specify the default priority bit (P-bit) to the selected interfaces.
No command		
Switch(config-if-PORT-PORT)# no qos rate-limit ingress		Disable QoS ingress rate limit settings.
Switch(config-if-PORT-PORT)# no qos rate-limit ingress rate		Reset the ingress rate limit value back to the default.
Switch(config-if-PORT-PORT)# no qos rate-limit ingress unit		Reset the unit of the ingress rate limit back to the default (Kbps).
Switch(config-if-PORT-PORT)# no qos rate-limit egress		Disable QoS egress rate limit settings.
Switch(config-if-PORT-PORT)# no qos rate-limit egress rate		Reset the egress rate limit value back to the default.
Switch(config-if-PORT-PORT)# no qos rate-limit egress unit		Reset the unit of the egress rate limit back to the default (Kbps).
Switch(config-if-PORT-PORT)# no qos user-priority		Reset the user priority value setting back to the default.(0)

2.5.17 Security Command

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

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

1. Enable or disable storm control and port isolation.

Security Command	Parameter	Description
Switch(config)# security storm-protection		Globally enable the storm control function.
Switch(config)# security port-isolation		Globally enable the port isolation function. If port isolation is set to enabled, the ports cannot communicate with each other. **Note 1: If the port isolation function is enabled, the Port-based VLAN will be invaild automatically.** **Note 2: "Port Isolation" function is not "Private VLAN" function.**
No command		
Switch(config)# no security storm-protection		Globally disable the storm control function.
Switch(config)# no security port-isolation		Globally disable port isolation function.
Show command		
Switch(config)# show security storm-protection		Show the current storm control global configuration.
Switch(config)# show security storm-protection interface		Show each interface's security settings including storm control rates.
Switch(config)# show security storm-protection interface [port_list]	[port_list]	Show the selected interfaces' security settings and storm control rates.
Switch(config)# show security port-isolation		Show the current port isolation configuration.

2. Use "Interface" command to configure storm control and port isolation.

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

		range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# security storm-protection broadcast [1-512k]	[1-512k]	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 NOTE: To view a list of allowable values that can be specified you can press “spacebar” and then followed by “?”. For example, “Switch(config)# security storm-protection broadcast ?”
Switch(config-if-PORT-PORT)# security storm-protection unknown-multicast [1-512k]	[1-512k]	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 ***NOTE:*** *To view a list of allowable values that can be specified you can press “spacebar” and then followed by “?”. For example, “Switch(config)# security storm-protection multicast ?”*
Switch(config-if-PORT-PORT)# security storm-protection unknown-unicast [1-512k]	[1-512k]	Specify the maximum unknown unicast packets per second (pps). Any unknown unicast packets exceeding the specified threshold will then be dropped. The packet rates that can be specified are listed below: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k ***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 ?”*
Switch(config-if-PORT-		Designates the specified port(s) as

PORT)# security port-isolation up-link-port		uplink port(s).
No command		
Switch(config-if-PORT-PORT)# no security storm-protection broadcast		Disable broadcast storm control on the selected ports.
Switch(config-if-PORT-PORT)# no security storm-protection unknown-multicast		Disable unknown-multicast storm control on the selected ports.
Switch(config-if-PORT-PORT)# no security storm-protection unknown-unicast		Disable unknown-unicast storm control on the selected ports.
Switch(config-if-PORT-PORT)# no security port-isolation up-link-port		Removes the specified port(s) from port-isolation (uplink port) status.
Examples of Security command		
Switch(config)# show security storm-protection interface [port_list]		Show the selected interfaces' security settings and storm control rates.
Switch(config)# show security storm-protection interface		Show each interface's security settings including storm control rates.

2.5.18 SFP Command

The **sfp threshold** commands not only displays all SFP' current temperature, voltage, current, TX power and RX power information, but is also capable of detecting whether these SFP port are at normal status or not.

In the display of the above SFP-related information, you can decide one or all items to be shown at a tme by assigning **All/Temperature/Voltage/Current/TX power/RX power** parameter upon your requriements.

Once this function of the specific SFP port is set to "Enabled", the alarm/warning message will be sent via trap and syslog in the event of abnormal situations, including temperature/voltage/current/TX power/RX power is over the **High** value or is under the **Low** value. A normal message can also be sent to notify the user when this SFP port's temperature/voltage/ current/TX power/RX power higher or lower than the threshold returns to the normal status. From these notification, the user can realize the real-time SFP status to prevent the disconnection and packets loss of any fiber ports from being taken place due to the occurrence of abnormal events.

SFP Threshold command	Parameter	Description
Switch(config)# sfp threshold		Globally enable the alarm notification of temperature/voltage/current/TX power/RX power for SFP ports of the Managed Swtich.
Switch(config)# sfp threshold notification continuous-alarm		Enable the continuous alarm message sending function for SFP ports' temperature/voltage/current/TX power/RX power.
Switch(config)# sfp threshold notification continuous-alarm interval [60-86400]	[60-86400]	Specify the continuous alarm interval for SFP ports' temperature/voltage/current/TX power/RX power alarm message in seconds. **Note:** 1. For this to work, the continuous alarm meassage sending function has to be enabled. 2. After each alarm message, the system will follow this specified time interval to continually send the same alarm message **(only for the monitored items of which the values exceed the thresholds)** until the monitored items return to normal status.
Switch(config)# sfp threshold notification interval [120-86400]	[120-86400]	Specify the time interval of sending SFP ports' temperature/voltage/current/TX power/RX power alarm message in seconds.
No command		
Switch(config)# no sfp threshold		Globally disable the alarm notification of temperature/voltage/current/TX power/RX power for SFP ports of the Managed

		Swtich.
Switch(config)# no sfp threshold notification continuous-alarm		Disable the continuous alarm message sending function for SFP ports' temperature/voltage/current/TX power/RX power.
Switch(config)# no sfp threshold notification continuous-alarm interval		Reset to default the continuous alarm interval for SFP ports' temperature/voltage/current/TX power/RX power alarm message (120 seconds).
Switch(config)# no sfp threshold notification interval		Reset the time interval of sending SFP ports' temperature/voltage/current/TX power/RX power alarm message to default (600 seconds).
Show command		
Switch(config)# show sfp information		Show the speed, distance, vendor name, vendor PN and vendor SN of SFP.
Switch(config)# show sfp state		Show the temperature, voltage, TX Bias, TX port and RX power of SFP.
Switch(config)# show sfp threshold		Show SFP threshold configuration, all SFP ports' current temperature/voltage/current (mA) /TX power/RX power and their threshold information of these parameters.
Switch(config)# show sfp threshold [port_list]	[port_list]	Show SFP threshold configuration, the specific SFP ports' current temperature/voltage/current (mA)/TX power/RX power and their threshold information of these parameters.
Switch(config)# show sfp threshold current		Show SFP threshold configuration, all SFP ports' current(mA) and their threshold information of this parameter.
Switch(config)# show sfp threshold current [port_list]	[port_list]	Show SFP threshold configuration, the specific SFP ports' current(mA) and their threshold information of this parameter.
Switch(config)# show sfp threshold rx-power		Show SFP threshold configuration, all SFP ports' current RX power and their threshold information of this parameter.
Switch(config)# show sfp threshold rx-power [port_list]	[port_list]	Show SFP threshold configuration, the specific SFP ports' current RX power and their threshold information of this parameter.
Switch(config)# show sfp threshold temperature		Show SFP threshold configuration, all SFP ports' current temperature and their threshold information of this parameter.
Switch(config)# show sfp threshold temperature [port_list]	[port_list]	Show SFP threshold configuration, the specific SFP ports' current temperature and their threshold information of this parameter.
Switch(config)# show sfp threshold tx-power		Show SFP threshold configuration, all SFP ports' current TX power and their threshold information of this parameter.
Switch(config)# show sfp threshold tx-power [port_list]	[port_list]	Show SFP threshold configuration, the specific SFP ports' current TX power and their threshold information of this

		parameter.
Switch(config)# show sfp threshold voltage		Show SFP threshold configuration, all SFP ports' current voltage and their threshold information of this parameter.
Switch(config)# show sfp threshold voltage [port_list]	[port_list]	Show SFP threshold configuration, the specific SFP ports' current voltage and their threshold information of this parameter.
Example of SFP Threshold		
Switch(config)# sfp threshold notification interval 300		Configure the time interval of sending SFP ports' temperature/voltage/current/TX power/RX power alarm message as 300 seconds. If their SFP threshold is enabled, the alarm message will be sent in 300 seconds when temperature/voltage/TX power/RX power is higher or lower than the threshold.
Switch(config)# sfp threshold notification continuous-alarm interval 60		Configure the continuous alarm interval for SFP ports' temperature/voltage/current/TX power/RX power alarm message as 60 seconds. After each alarm message, the system will repeat sending the same alarm message every 60 seconds **(only for the monitored items of which the values exceed the thresholds)** until the monitored items return to normal status. Please be noted that the function of continuous alarm and SFP threshold must be enabled beforehand for this to work properly.
Switch(config)# show sfp threshold 5		Display SFP Port 5's current temperature/voltage/current/TX power/RX power and their threshold information of these parameters.

Use "Interface" command to configure a group of ports' SFP Port Theshold function.

SFP Threshold & 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)# sfp threshold detect		Enable auto detect alarm and warning threshold for the selected port(s). Default value is enabled.
Switch(config-if-PORT-PORT)# sfp threshold current [high | low]	[high | low]	Enable high/low current threshold for the selected port(s).

Switch(config-if-PORT-PORT)# sfp threshold current [high | low] value [0~1500]	[high | low] [0~1500]	Specify the value for high/low alarm/warning current threshold for the selected port(s). This command can set high/low alarm **and** warning current threshold at the same time and apply the same specified value. The valid value range is 0~1500 (Unit: 1/10mA).
Switch(config-if-PORT-PORT)# sfp threshold current [high | low] value [alarm | warning] [0~1500]	[high | low] [alarm | warning] [0~1500]	Specify the value respectively for high/low alarm/warning current threshold for the selected port. The valid value range is 0~1500 (Unit: 1/10mA).
Switch(config-if-PORT-PORT)# sfp threshold rx-power [high | low]	[high | low]	Enable high/low RX power threshold for the selected port(s).
Switch(config-if-PORT-PORT)# sfp threshold rx-power [high | low] value [-400~100]	[high | low] [-400~100]	Specify the value for high/low alarm/warning RX power threshold for the selected port(s). This command can set high/low alarm **and** warning RX power threshold at the same time and apply the same specified value. The valid value range is -400~100 (Unit: 1/10dBm).
Switch(config-if-PORT-PORT)# sfp threshold rx-power [high | low] value [alarm | warning] [-400~100]	[high | low] [alarm | warning] [-400~100]	Specify the value respectively for high/low alarm/warning RX power threshold for the selected port. The valid value range is -400~100 (Unit: 1/10dBm).
Switch(config-if-PORT-PORT)# sfp threshold temperature [high | low]	[high | low]	Enable high/low temperature threshold for the selected port(s).
Switch(config-if-PORT-PORT)# sfp threshold temperature [high | low] value [-400~1200]	[high | low] [-400~1200]	Specify the value for high/low alarm/warning temperature threshold for the selected port(s). This command can set high/low alarm **and** warning temperature threshold at the same time and apply the same specified value. The valid value range is -400~1200 (Unit: 1/10 degrees Celsius).
Switch(config-if-PORT-PORT)# sfp threshold temperature [high | low] value [alarm | warning] [-400~1200]	[high | low] [alarm | warning] [-400~1200]	Specify the value respectively for high/low alarm/warning temperature threshold for the selected port(s). The valid value range is -400~1200 (Unit: 1/10 degrees Celsius).
Switch(config-if-PORT-PORT)# sfp threshold tx-power [high | low]	[high | low]	Enable high/low TX power threshold for the selected port(s).

Switch(config-if-PORT-PORT)# sfp threshold tx-power [high | low] value [-300~100]	[high | low] [-300~100]	Specify the value for high/low alarm/warning TX power threshold for the selected port. This command can set high/low alarm **and** warning TX power threshold at the same time and apply the same specified value. The valid value range is -300~100 (Unit: 1/10dBm).
Switch(config-if-PORT-PORT)# sfp threshold tx-power [high | low] value [alarm | warning] [-300~100]	[high | low] [alarm | warning] [-300~100]	Specify the value respectively for high/low alarm/warning TX power threshold for the selected port. The valid value range is -300~100 (Unit: 1/10dBm).
Switch(config-if-PORT-PORT)# sfp threshold voltage [high | low]	[high | low]	Enable high/low voltage threshold for the selected port(s).
Switch(config-if-PORT-PORT)# sfp threshold voltage [high | low] value [260~400]	[high | low] [260~400]	Specify the value for high/low alarm/warning voltage threshold for the selected port. This command can set high/low alarm **and** warning voltage threshold at the same time and apply the same specified value. The valid value range is 260~400 (Unit: 1/100V).
Switch(config-if-PORT-PORT)# sfp threshold voltage [high | low] value [alarm | warning] [260~400]	[high | low] [alarm | warning] [260~400]	Specify the value respectively for high/low alarm/warning voltage threshold for the selected port. The valid value range is 260~400 (Unit: 1/100V).
No command		
Switch(config-if-PORT-PORT)# no sfp threshold detect		Disable auto detect alarm and warning threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no sfp threshold current [high | low]	[high | low]	Disable high/low current threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no sfp threshold current [high | low] value	[high | low]	Reset the high/low alarm **and** warning current threshold values to default.
Switch(config-if-PORT-PORT)# no sfp threshold current [high | low] value [alarm | warning]	[high | low] [alarm | warning]	Respectively reset the high/low alarm **or** warning current threshold value to default.
Switch(config-if-PORT-PORT)# no sfp threshold rx-power [high | low]	[high | low]	Disable high/low RX power threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no sfp threshold rx-power [high | low] value	[high | low]	Reset the high/low alarm **and** warning RX power threshold values to default.
Switch(config-if-PORT-	[high | low]	Respectively reset the high/low alarm **or**

PORT)# no sfp threshold rx-power [high | low] value [alarm | warning]	[alarm | warning]	warning RX power threshold value to default.
Switch(config-if-PORT-PORT)# no sfp threshold temperature [high | low]	[high | low]	Disable high/low temperature threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no sfp threshold temperature [high | low] value	[high | low]	Reset the high/low alarm **and** warning temperature threshold values to default.
Switch(config-if-PORT-PORT)# no sfp threshold temperature [high | low] value [alarm | warning]	[high | low] [alarm | warning]	Respectively reset the high/low alarm **or** warning temperature threshold value to default.
Switch(config-if-PORT-PORT)# no sfp threshold tx-power [high | low]	[high | low]	Disable high/low TX power threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no sfp threshold tx-power [high | low] value	[high | low]	Reset the high/low alarm **and** warning TX power threshold values to default.
Switch(config-if-PORT-PORT)# no sfp threshold tx-power [high | low] value [alarm | warning]	[high | low] [alarm | warning]	Respectively reset the high/low alarm **or** warning TX power threshold value to default.
Switch(config-if-PORT-PORT)# no sfp threshold voltage [high | low]	[high | low]	Disable high/low voltage threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no sfp threshold voltage [high | low] value	[high | low]	Reset the high/low alarm **and** warning voltage threshold values to default.
Switch(config-if-PORT-PORT)# no sfp threshold voltage [high | low] value [alarm | warning]	[high | low] [alarm | warning]	Respectively reset the high/low alarm **or** warning voltage threshold value to default.
Example of SFP Threshold & Interface		
Switch(config-if-5)# sfp threshold temperature high		Enable high temperature threshold for Ports 5.
Switch(config-if-5)# sfp threshold temperature high value 800		Configure both high alarm **and** warning temperature thresholds as 80 degrees Celsius for Ports 5.
Switch(config-if-5)# sfp threshold temperature low value warning -100		Configure low warning temperature threshold as -10 degrees Celsius for Ports 5.

2.5.19 SNMP-Server Command

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

Snmp-server command	Parameter	Description
Switch(config)# snmp-server		Enable SNMP server function globally.
Switch(config)# snmp-server community [community]	[community]	Create/modify a SNMP community name. Up to 20 alphanumeric characters can be accepted.
Switch(config-community-NAME)# active		Enable the specified SNMP community account.
Switch(config-community-NAME)# description [Description]	[Description]	Enter the description for the specified SNMP community. Up to 35 alphanumerical characters can be accetpted.
Switch(config-community-NAME)# level [admin | rw | ro]	[admin | rw | ro]	Specify the access privilege level for the specified SNMP account. **admin:** Own the full-access right, including maintaining user account, system information, loading factory settings, etc.. **rw:** Read & Write access privilege. Own the partial-access right, unable to modify user account, system information and load factory settings. **ro:** Allow to view only.
No command		
Switch(config)# no snmp-server		Disable SNMP function.
Switch(config)# no snmp-server community [community]	[community]	Delete the specified community.
Switch(config-community-NAME)# no active		Disable the specified SNMP community account.
Switch(config-community-NAME)# no description		Remove the description of SNMP community.
Switch(config-community-NAME)# no level		Reset the access privilege level back to the default. (Read Only)
Show command		
Switch(config)# show snmp-server		Show SNMP server configuration.
Switch(config)# show snmp-server community		Show SNMP server community configuration.
Switch(config)# show snmp-server community [community]		Show the specified SNMP server community's configuration.
Switch(config-community-NAME)# show		Show the selected community's settings.
Exit command		
Switch(config-community-NAME)# exit		Return to the global configuration mode.

Example of Snmp-server	
Switch(config)# snmp-server community mycomm	Create a new community “mycomm” and edit the details of this community account.
Switch(config-community-mycomm)# active	Activate the SNMP community “mycomm”.
Switch(config-community-mycomm)# description rddeptcomm	Add a description for “mycomm” community.
Switch(config-community-mycomm)# level admin	Set the access privilege level of “mycomm” community to admin (full-access privilege).

2. Set up a SNMP trap destination.

Trap-destination command	Parameter	Description
Switch(config)# snmp-server trap-destination [1-3]	[1-3]	Specify the trap destination you would like to modify.
Switch(config-trap-ID)# active		Enable the specified SNMP trap destination.
Switch(config-trap-ID)# community [community]	[community]	Enter the description for the secified trap destination.
Switch(config-trap-ID)# destination [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F :G:H]	Specify SNMP server IP/IPv6 address for the secified trap destination.
No command		
Switch(config)# no snmp-server trap-destination [1-3]	[1-3]	Reset the specified trap destination configuration back to the default.
Switch(config-trap-ID)# no active		Disable the specified SNMP trap destination.
Switch(config-trap-ID)# no community		Delete the description for the specified trap destination.
Switch(config-trap-ID)# no destination		Delete SNMP server IP/IPv6 address for the specified trap destination.
Show command		
Switch(config)# show snmp-server trap-destination		Show all of SNMP trap destination configurations.
Switch(config)# show snmp-server trap-destination [1-3]	[1-3]	Show the specified SNMP trap destination configuration.
Switch(config-trap-ID)# show		Show the configuration of the selected trap destination.
Exit command		
Switch(config-trap-ID)# exit		Return to the global configuration mode.
Examples of Trap-destination		
Switch(config)# snmp-server trap-destination 1		Specify the trap destination 1 to do the modification.
Switch(config-trap-1)# active		Activate the trap destination ID 1.
Switch(config-trap-1)# community mycomm		Add the description “mycomm” to this trap destination.

Switch(config-trap-1)# destination 192.168.1.254	Set SNMP server IP address as “192.168.1.254” for this trap destination.

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

Trap-type command	Parameter	Description
Switch(config)# snmp-server trap-type [all | auth-fail | auto-backup | cold-start | cpu-load | port-link | power-down | sfp-threshold | warm-start]	[all | auth-fail | auto-backup | cold-start | cpu-load | port-link | power-down | sfp-threshold | warm-start]	Specify a trap type that will be sent when a certain situation occurs. **all:** Enable all traps to be sent when corresponding events are triggered. **auth-fail:** A trap will be sent when any unauthorized user attempts to login. **auto-backup:** A trap will be sent when the auto backup succeeds or fails. **cold-start:** A trap will be sent when the Managed Switch boots up. **cpu-load:** A trap will be sent when the CPU is overloaded. **port-link:** A trap will be sent when the link is up or down. **power-down:** A trap will be sent when the Managed Switch’s power is down. **sfp-threshold:** A trap will be sent when Temperature / Voltage/ Current / TX Power / RX Power of sfp is over the **High** value, under the **Low** value, or returning to the normal status from abnormal status. **warm-start:** A trap will be sent when the Managed Switch restarts.
No command		
Switch(config)# no snmp-server trap-type [all | auth-fail | auto-backup | cold-start | cpu-load | port-link | power-down | sfp-threshold | warm-start]	[all | auth-fail | auto-backup | cold-start | cpu-load | port-link | power-down | sfp-threshold | warm-start]	Specify a trap type that will not be sent when a certain situation occurs.
Show command		
Switch(config)# show snmp-server trap-type		Show the current enabled/disabled status of each type of trap.
Examples of Trap-type		

Switch(config)# snmp-server trap-type all	All types of SNMP traps will be sent.

4. Set up detailed configurations for SNMPv3 USM User

Simple Network Management Protocol Version 3, SNMPv3 in short, features stronger security mechanism, including authentication and encryption that helps ensure that the message is from a valid source and scramble the content of a packet, to prevent from being learned by an unauthorized source.

Snmp-server Command	Parameter	Description
Switch(config)# snmp-server password-encryption [aes-128]	[aes-128]	Enable encryption method AES-128 on the SNMPv3 user password. **aes-128 (advanced encryption method):** An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data.
Switch(config)# snmp-server user [user_name]	[user_name]	Modify an existing username generated in CLI of “User Command” for a SNMPv3 user.
Switch (config-v3-user-user_name)# authentication [md5 | sha]	[md5 | sha]	Specify the authentication method for the specified SNMPv3 user. **md5(message-digest algorithm):** A widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. **sha(Secure Hash Algorithm):** A 160-bit hash function which resembles the said MD5 algorithm.
Switch (config-v3-user-user_name)# authentication password [password]	[password]	Specify the authentication password for the specified SNMPv3 user. The password length must be between 8 and 32 characters, and special characters like ‘ “ % | \ are acceptable.
Switch (config-v3-user-user_name)# authentication password aes-128 [base64]	[base64]	Specify the password encrypted by aes-128. **aes-128 (advanced encryption method):** An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data.
Switch (config-v3-user-user_name)# private [des | aes128]	[des | aes128]	Specify the method to ensure confidentiality of data. **des (data encryption standard):** An algorithm to encrypt critical information such as message text message signatures…etc.

		aes-128 (advanced encryption method): An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data.
Switch (config-v3-user-user_name)# private password [password]	[password]	Specify the private password for the specified SNMPv3 user. The password length must be between 8 and 32 characters, and special characters like ‘ “ % | \ are acceptable.
Switch (config-v3-user-user_name)# private password aes-128 [base64]	[base64]	Specify the password encrypted by aes-128. **aes-128 (advanced encryption method):** An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data.
No Command		
Switch(config)# no snmp-server password-encryption		Disable encryption on the SNMPv3 user password.
Switch (config-v3-user-user_name)# no authentication		Disable the authentication function for the specified SNMPv3 user.
Switch (config-v3-user-user_name)# no authentication password		Delete the configured authentication password.
Switch (config-v3-user-user_name)# no private		Disable data encryption function.
Switch (config-v3-community-user_name)# no private password		Delete the configured private password.
Show Command		
Switch(config)# show snmp-server user		Show SNMPv3 user configuration.
Switch(config)# show snmp-server user [user_name]	[user_name]	Show the specified SNMPv3 user configuration.
Switch(config-v3-user-user_name)# show		Show the specified SNMPv3 user configuration.

A combination of a security event shown as below indicates which security mechanism is used when handling an SNMP packet.

Authentication	Private	Result
None	None	Uses a username match for authentication
Message Digest Algorithm(MD5) or Secure Hash Algorithm(SHA)	None	Enables authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms.

MD5 or SHA	Data Encryption Standard(DES)	Enables authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms. What's more, enables DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES standard.
MD5 or SHA	Advanced Encryption Standard (AES-128)	Enables authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms. What's more, enables 128-bit AES encryption based on the symmetric-key algorithm.

2.5.20 Switch Command

Switch command	Parameter	Description
Switch(config)# switch mtu [1518-16383]	[1518-16383]	Specify the maximum frame size in bytes. The allowable MTU value is between 1518 and 16383 bytes.
No command		
Switch(config)# no switch mtu		Reset MTU size back to the default.
Show command		
Switch(config)# show switch mtu		Show the current the maximum frame size configuration.

2.5.21 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 64 alphanumeric characters, for this Managed Switch.
Switch(config)# switch-info cpu-loading notification		Enable the CPU loading notification.
Switch(config)# switch-info cpu-loading notification threshold [1-99]	[1-99]	Specify CPU loading threshold in percentage for notification.
Switch(config)# switch-info cpu-loading notification restore [1-99]	[1-99]	Specify CPU loading restore threshold in percentage for notification, the value should be lower than the CPU loading threshold.
Switch(config)# switch-info cpu-loading notification observation-interval [5-86400]	[5-86400]	Specify a value for Threshold and Restore Observation Interval time in seconds.
Switch(config)# switch-info dhcp-vendor-id [dhcp_vendor_id]	[dhcp_vendor_id]	Enter the user-defined DHCP vendor ID, and up to 64 alphanumeric characters can be accepted. Please make sure you have an exact DHCP Vendor ID with the value specified in "vendor-classes" in your dhcpd.conf file. For detailed information, see Appendix B.
Switch(config)# switch-info host-name [host_name]	[host_name]	Enter a new hostname, up to 64 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 host-name-sync-to-system-name		Enable synchronization of the host name to the system name.
Switch(config)# switch-info system-contact [sys_contact]	[sys_contact]	Enter the contact information, up to 64 alphanumeric characters, for this Managed switch.
Switch(config)# switch-info system-location [sys_location]	[sys_location]	Enter a brief description of the Managed Switch location, up to 64 alphanumeric characters, for this Managed Switch. Like the name, the location is for reference only, for example, “13th Floor”.
Switch(config)# switch-info system-name [sys_name]	[sys_name]	Enter a unique name, up to 64 alphanumeric characters, for this Managed Switch. Use a descriptive name to identify the Managed Switch in relation to your network, for example, “Backbone 1”. This name is mainly used for reference only.
No command		
Switch(config)# no switch-info company-name		Reset the entered company name back to the default.
Switch(config)# no switch-info cpu-loading notification		Disable the CPU loading notification.
Switch(config)# no switch-info cpu-loading notification threshold		Reset CPU loading threshold back to the default (95 percentage)
Switch(config)# no switch-info cpu-loading notification restore		Reset CPU loading restore threshold back to the default (80 percentage)
Switch(config)# no switch-info cpu-loading notification observation-interval		Reset the Observation interval back to the default. (60 seconds)
Switch(config)# no switch-info dhcp-vendor-id		Reset the entered DHCP vendor ID information back to the default.
Switch(config)# no switch-info host-name		Reset the hostname back to the default.
Switch(config)# no switch-info host-name-sync-to-system-name		Disable synchronization of the host name to the system name.
Switch(config)# no switch-info system-contact		Reset the entered system contact information back to the default.
Switch(config)# no switch-info system-location		Reset the entered system location information back to the default.
Switch(config)# no switch-info system-name		Reset the entered system name information back to the default.
Show command		
Switch(config)# show switch-info		Show the switch-related information including company name, system contact, system location, system name, model name, firmware version and so on.
Switch(config)# show switch-info cpu-loading		Show the current configuration of CPU loading.
Switch(config)# show switch-info cpu-loading statistics		Show the current CPU loading statistics.
Switch(config)# show switch-info cpu-loading		Clear the CPU loading average records.

statistics average clear	
Switch(config)# show switch-info memory statistics	Show the current memory usage rate of the switch.
Examples of Switch-info	
Switch(config)# switch-info company-name telecomxyz	Set the company name to “telecomxyz”.
Switch(config)# switch-info system-contact info@company.com	Set the system contact field to “info@compnay.com”.
Switch(config)# switch-info system-location 13thfloor	Set the system location field to “13thfloor”.
Switch(config)# switch-info system-name backbone1	Set the system name field to “backbone1”.
Switch(config)# switch-info host-name edgeswitch10	Change the Managed Switch’s hostname into “edgeswitch10”.

2.5.22 Syslog Command

Syslog Command	Parameter	Description
Switch(config)# syslog		Enable the system log function.
Switch(config)# syslog facility [0-7]	[0-7]	Specify a facility code (Local 0~Local 7) to a specific device for classifying the syslog message provided by different devices.
Switch(config)# syslog logging-type terminal-history		Enable Terminal-history log function.
Switch(config)# syslog server1 [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F :G:H]	Specify the primary system log server's IPv4/IPv6 address.
Switch(config)# syslog server2 [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F :G:H]	Specify the secondary system log server's IPv4/IPv6 address.
Switch(config)# syslog server3 [A.B.C.D | A:B:C:D:E:F:G:H]	[A.B.C.D | A:B:C:D:E:F :G:H]	Specify the third system log server's IPv4/IPv6 address.
No command		
Switch(config)# no syslog		Disable the system log function.
Switch(config)# no syslog facility		Reset the facility code back to the default. (Local 0)
Switch(config)# no syslog logging-type terminal-history		Disable Terminal-history log function.
Switch(config)# no syslog server1		Delete the primary system log server's IPv4/IPv6 address.
Switch(config)# no syslog server2		Delete the secondary system log server's IPv4/IPv6 address.
Switch(config)# no syslog server3		Delete the third system log server's IPv4/IPv6 address.
Show command		
Switch(config)# show syslog		Show the current system log configuration.
Examples of Syslog command		
Switch(config)# syslog		Enable the system log function.
Switch(config)# syslog server1 192.180.2.1		Set the primary system log server's IP address to 192.168.2.1.
Switch(config)# syslog server2 192.168.2.2		Set the secondary system log server's IP address to 192.168.2.2.
Switch(config)# syslog server3 192.168.2.3		Set the third system log server's IP address to 192.168.2.3.

2.5.23 Terminal Command

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

2.5.24 User Command

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 32 alphanumeric characters. Only 10 login accounts can be registered in this device.
Switch(config)# user password-encryption aes-128		Select **AES-128** (Advanced Encryption Standard) as the password encryption method. ***NOTE:*** *1. The acquired password from backup config file is not applicable for user login on CLI/Web interface.* *2. We strongly recommend not to alter off-line Auth Method setting in backup configure file.* *3. If Auth-Method is enabled and do firmware downgrade, users must reset default config.*
Switch(config-user-USERNAME)# active		Activate this user account.
Switch(config-user-USERNAME)# description [description]	[description]	Enter the brief description for this user account, up to 35 alphanumeric characters are acceptable.
Switch(config-user-USERNAME)# level [admin | rw | ro]	[admin | rw | ro]	Specify user account level. By default, when you create a community, the access privilege for this account is set to “read only”. **Admin:** Full access right, including maintaining user account, system information, loading factory settings, etc.

		rw: Read & Write access privilege. Partial access right, unable to modify system information, user account, load factory settings and upgrade firmware. **Ro:** Read Only access privilege.
Switch(config-user-USERNAME)# password [password]	[password]	Enter the password for this user account up to 64 alphanumeric characters.
Switch (config-user-USERNAME)# password aes-128 [base64]	[base64]	Specify the password encrypted by aes-128. **aes-128 (advanced encryption method):** An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data.
No command		
Switch(config)# no user name [user_name]	[user_name]	Delete the specified user account.
Switch(config)# no user password-encryption		Disable any encryption method on the user passwords. **Note**: When configure the Password Encryption as disabled, all the existing passwords will be cleared. Be sure to reconfigure otherwise the password will be empty (null).
Switch(config-user-USERNAME)# no active		Deactivate the selected user account.
Switch(config-user-USERNAME)# no description		Remove the configured description for the specified user account.
Switch(config-user-USERNAME)# no level		Reset the access privilege level back to the default (Read Only).
Switch(config-user-USERNAME)# no password		Remove the configured password for the specified user account.
Show command		
Switch(config)# show user		Show user account configuration.
Switch(config)# show user name		List all user accounts.
Switch(config)# show user name [user_name]	[user_name]	Show the specific account's configuration.
Switch(config-user-USERNAME)# show		Show the specific account's configuration.
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".

2.5.25 VLAN Command

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

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

2.5.25.1 Port-Based VLAN

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

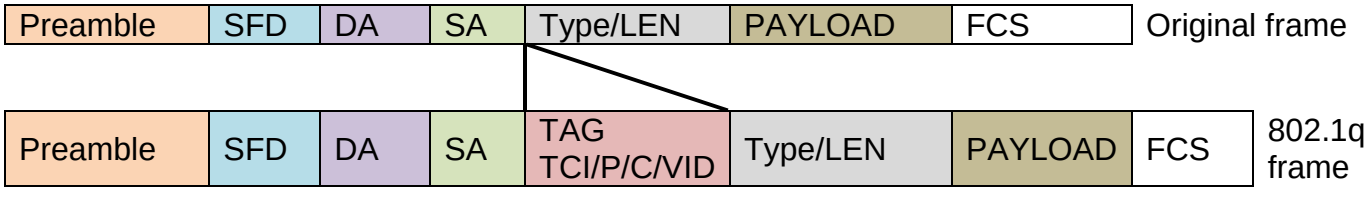
Since source addresses of the packets are listed in MAC address table of specific VLAN (except broadcast/multicast packets), in every VLAN the traffic between two ports will be two-way without restrictions.

2.5.25.2 802.1Q VLAN

802.1Q VLAN Concept

Port-Based VLAN is simple to implement and use, but it cannot be deployed cross switches VLAN. The 802.1Q protocol was developed in order to provide the solution to this problem. By tagging VLAN membership information to Ethernet frames, the IEEE 802.1Q can help network administrators break large switched networks into smaller segments so that broadcast and multicast traffic will not occupy too much available bandwidth as well as provide a higher level security between segments of internal networks.

Introduction to 802.1Q frame format:



PRE Preamble	62 bits	Used to synchronize traffic
SFD Start Frame Delimiter	2 bits	Marks the beginning of the header
DA Destination Address	6 bytes	The MAC address of the destination

SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes set to 8100 for 802.1p and Q tags	
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format - Ethernet set to "0"
VID	VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload < or = 1500 bytes User data			
FCS	Frame Check Sequence	4 bytes	Cyclical Redundancy Check

Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the switch port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

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

- **Access Mode :**
  Access Links (the link to/from access ports) are the most common type of links on any VLAN switch. All **network hosts (such as PCs)** connect to the switch's Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, the **network hosts** will be allowed to access.

  It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal switch. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode :**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between switches. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple switches.

- **Trunk Native Mode :**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.

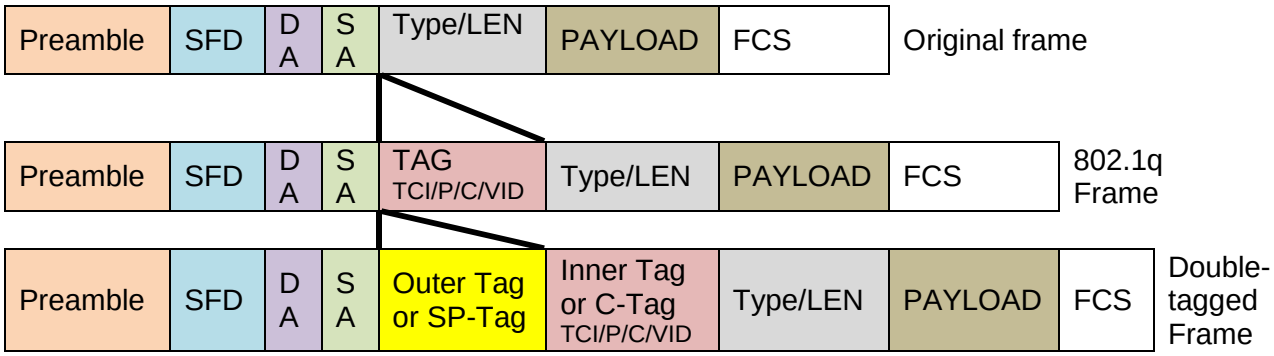
Example : PortX configuration

Configuration	Result
Trunk-VLAN = 10, 11, 12	PortX is an **Access Port**

Access-VLAN = 20 **Mode = Access**	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

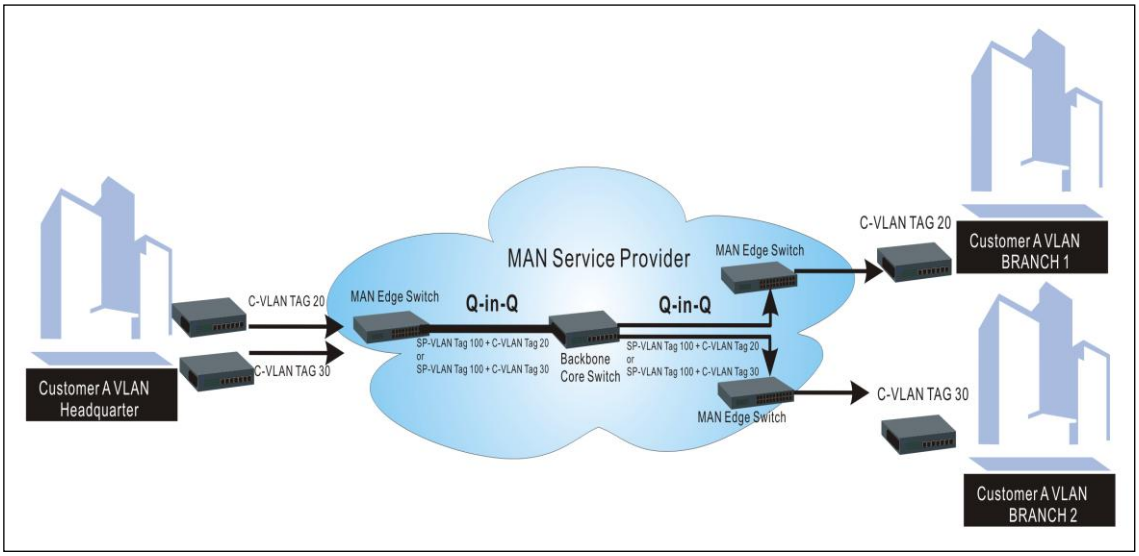
2.5.25.3 Introduction to Q-in-Q (ISP Mode)

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



Double-Tagged Frame Format

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



Q-in-Q Example

1. **Create/modify an 802.1q VLAN and a management VLAN rule, modify a port-based VLAN group or set up ISP mode (IEEE 802.1Q double tagging VLAN).**

VLAN dot1q command	Parameter	Description
Switch(config)# vlan dot1q-vlan		Enable 802.1q VLAN mode globally.
Switch(config)# vlan dot1q-vlan [1-4094]	[1-4094]	Enter a VLAN ID number to create a new 802.1q VLAN or modify an existing 802.1q VLAN.
Switch(config-vlan-ID)# name [vlan_name]	[vlan_name]	Specify a descriptive name for the created VLAN ID, maximun 15 characters.
Switch(config)# vlan management-vlan [1-4094] management-port [port_list] mode [access | trunk | trunk-native]	[1-4094]	Enter the management VLAN ID.
	[port_list]	Specify the management port number.
	[access | trunk | trunk-native]	Specify whether the management port is in trunk or access mode. **"trunk" mode:** Set the selected ports to tagged. **"access" mode:** Set the selected ports to untagged. **"trunk-native" mode:** Set the selected ports to tagged or untagged.
Switch(config)# vlan port-based		Enable port based VLAN mode globally.
Switch(config)# vlan port-based [name]	[name]	Specify a name for the created VLAN ID, maximum 15 characters.
Switch(config)# vlan port-based [name] include-cpu	[name]	Include CPU into any existing Port-Based VLAN.
Switch(config)# vlan port-based [name] rename [new_name]	[new_name]	Specify a new name for the created VLAN ID, maximum 15 characters.
Switch(config)# vlan bypass-ctag		Ignore C-tag checking.
Switch(config)# vlan isp-mode		Enable ISP mode (IEEE 802.1Q double tagging VLAN) globally.
Switch(config)# vlan isp-mode stag-vid [1-4094]	[1-4094]	Specify the service tag VID. Valid values are 1 through 4094.
Switch(config)# vlan isp-mode stag-ethertype [0xWXYZ]	[0xWXYZ]	Specify the service tag's ethertype. (Range: 0000~FFFF)
No command		
Switch(config)# no vlan dot1q-vlan		Disable 802.1q VLAN mode globally.
Switch(config)# no vlan dot1q-vlan [1-4094]	[1-4094]	Remove the specific VLAN ID from the IEEE 802.1q Tag VLAN table.
Switch(config)# no vlan port-based		Disable port based VLAN mode globally.
Switch(config)# no vlan port-based [name]	[name]	Delete the specified port based VLAN by its name.
Switch(config)# no vlan port-based [name] include-cpu	[name]	Exclude CPU from the specified any existing port based VLAN.
Switch(config)# no vlan bypass-ctag		Active C-tag checking.
Switch(config)# no vlan isp-		Diable ISP mode (IEEE 802.1Q double

mode		tagging VLAN) globally.
Switch(config)# no vlan isp-mode stag-vid		Reset the service tag VID back to the default.
Switch(config)# no vlan isp-mode stag-ethertype		Reset the service tag's ethertype to the default.
Show command		
Switch(config)# show vlan		Show VLAN table.
Switch(config)# show vlan interface		Show all ports' VLAN assignment and VLAN mode.
Switch(config)#show vlan interface [port_list]	[port_list]	Show the selected ports' VLAN assignment and VLAN mode.
Switch(config)# show vlan port-based		Show port-based VLAN table.
Switch(config)# show vlan isp-mode		Show ISP mode (IEEE 802.1Q double tagging VLAN) configuration.
Example of VLAN dot1q & interface		
Switch(config)# vlan dot1q-vlan 100		Create a new VLAN 100.
Switch(config)# vlan port-based MKT_Office		Create a port-based VLAN "MKT_Office".
Switch(config)# vlan management-vlan 1 management-port 1-3 mode access		Set VLAN 1 to management VLAN (untagged) and Port 1~3 as management ports.

2. Use "Interface" command to configure a group of ports' 802.1q/Port-based/ISP mode (IEEE 802.1Q double tagging VLAN) settings.

VLAN & Interface 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)# vlan dot1q-vlan pvid [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode access		Set the selected ports to the access mode (untagged).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk		Set the selected ports to the trunk mode (tagged).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk native		Enable native VLAN for untagged traffic on the selected ports. (Tagged and untagged) **Note: When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.**
Switch(config-if-PORT-PORT)# vlan isp-mode isp-port		Specify the selected ports to be the ISP ports (IEEE 802.1Q double tagging port).
Switch(config-if-PORT-PORT)# vlan port-based [name]	[name]	Set the selected ports to a specified port-based VLAN.

		Note : **Need to create a port-based VLAN group under the VLAN global configuration mode before joining it.**
No command		
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan pvid		Reset the selected ports' PVID back to the default setting.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan mode		Reset the selected ports' 802.1q VLAN mode back to the default setting (Access Mode).
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the specified trunk VLAN ID from the selected ports.
Switch(config-if-PORT-PORT)# no vlan port-based [name]	[name]	Remove the selected port(s) from the specified port-based VLAN.
Switch(config-if-PORT-PORT)# no vlan isp-mode isp-port		Reset the selected ports to non-ISP ports (the default setting).
Example of VLAN dot1q & interface		
Switch(config)# interface 1-3		Enter port 1 to port 3's interface mode.
Switch(config-if-1-3)# vlan dot1q-vlan trunk-vlan 100		Assign the selected ports to VLAN 100.
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 pvid 100		Set the selected ports' PVID to 100.

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

Example 1,

We will configure a 6-port Managed Switch via CLI as the Table 2-3 listed.

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

Table 2-3

1. Create 802.1q VLAN IDs.

Switch(config)# interface 1-2	Enter port 1 to port 2's interface mode.
Switch(config-if-1,2)# vlan dot1q-vlan trunk-vlan 10, 20	Set port 1 to port 2's Trunk-VLAN ID (VID) to 10 and 20.
Switch(config-if-1,2)# vlan dot1q-vlan mode trunk	Set the selected ports to Trunk Mode (tagged).
Switch(config-if-1,2)# exit	Exit current ports interface mode.
Switch(config)# interface 3-4	Enter port 3 to 4's interface mode.
Switch(config-if-3,4)# vlan dot1q-vlan pvid 50	Set port 3 to port 4's Access-VLAN ID (PVID) to 50.
Switch(config-if-3,4)# vlan dot1q-vlan trunk-	Set port 3 to port 4's Trunk-VLAN ID

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

2. Modify 802.1q VLAN IDs' names.

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

2.5.26 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 the commands below.

2. Enable port auto-negotiation.

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

3. Set up port description.

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

4. Set up port duplex mode.

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

5. Enable flow control operation.

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

6. Shutdown interface.

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

7. Set up port speed.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# speed [10000 | 5000 | 2500 | 1000 | 100 | auto-sense | auto-speed]	[10000 | 5000 | 2500 | 1000 | 100 | auto-sense | auto-speed]	Configure the port speed as 10Gbps, 5Gbps, 2.5Gbps, 1000Mbps, 100Mbp, auto-sense or auto-speed. **Note 1: Speed can only be configured when auto-negotiation is disabled.** **Note 2: The specified speed can only be configured when it's supported on the selected interface.** **Note 3: Only port 4 supports 5000 and auto-sense, only port 5 support auto-speed.**
No command		
Switch(config-if-PORT-PORT)# no speed		Reset the port speed setting back to the default.

Use show interface command to display configurations, statistics or informations of several discontinuous ports or a range of ports.

1. "**Show interface status" command** displays the current link status of ports and can be executed in either Privileged mode or Global Configuration mode. This command is useful for network administrators to monitor and analyze the real-time status of each port.

Command	Parameters	Description
Switch(config)# show interface		Display the overall interface configuration.
Switch(config)# show interface [port_list]	[port_list]	Display interface configuration of the selected port(s).

Switch(config)# show interface status		Display the overall interface status.
Switch(config)# show interface status [port_list]	[port_list]	Display the interface status of the selected port(s).

2. Show interface description

Command	Parameters	Description
Switch(config)# show interface description		Display the description of all interfaces.
Switch(config)# show interface description [port_list]	[port_list]	Display the description of the selected port(s).

3. Show interface detailed

Command	Parameters	Description
Switch(config)# show interface detailed		Display the details of all interfaces, including configurations, SFP diagnostics and statistics.
Switch(config)# show interface detailed [port_list]	[port_list]	Display the details of the selected port(s), including configurations, SFP diagnostics and statistics.

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

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

Switch(config)# show interface statistics error rate [port_list]	[port_list]	Display error packets statistics (rates) for the selected ports.
Switch(config)# show interface statistics traffic		Display traffic statistics (events) for each port.
Switch(config)# show interface statistics traffic [port_list]	[port_list]	Display traffic statistics (events) for the selected ports.
Switch(config)# show interface statistics traffic rate		Display traffic statistics (rates) for each port.
Switch(config)# show interface statistics traffic rate [port_list]	[port_list]	Display traffic statistics (rates) for the selected ports.

2.5.27 Diagnostics Command

The following section provides an overview of the diagnostics commands used to configure and execute diagnostic functions on the device. It covers commands for detailed configuration of diagnostics and instructions for initiating, scheduling, and managing diagnostic processes. These commands are essential for monitoring network performance and troubleshooting issues effectively.

2.5.27.1 Configure Diagnostics Details

This section focuses on commands used to configure diagnostic parameters for various features, such as Cable, DHCP Client, DNS, IPTV, ping, and throughput testing. It includes details on setting diagnostic modes, input parameters, and specific configurations tailored to each diagnostic type.

2.5.27.1.1 Cable Diagnostics

Diagnostics Command	Parameter	Description
Switch(config)# diagnostics cable interface [port_number]	[port_number]	Configure the port for cable diagnostics (diagnostics must be started separately).
No Command	**Parameter**	**Description**
Switch(config)# no diagnostics cable		Reset the configured port for cable diagnostics to the default (port 1).
Show Command	**Parameter**	**Description**
Switch(config)# show diagnostics cable		Show the current configuration of cable diagnostics.

2.5.27.1.2 DHCP client Diagnostics.

Diagnostics Command	Parameter	Description
Switch(config)# diagnostics dhcp-client ip-version ipv4		Configure the device to use IPv4 for the DHCP client to obtain an IP address.
Switch(config)# diagnostics dhcp-client ip-version ipv6		Configure the device to use IPv6 for the DHCP client to obtain an IP address.
Switch(config)# diagnostics dhcp-client ip-version ipv6 auto-configuration [stateless | stateful]	[stateless | stateful]	Set the DHCPv6 auto-configuration type for DHCP Client diagnostics to either stateless or stateful. **Stateless:** The device generates its own IP address based on the network prefix, with the DHCPv6 server only providing additional configuration information (like DNS). **Stateful**: The DHCPv6 server assigns the device a full IP address and manages its lease.
Switch(config)# diagnostics dhcp-client keep-ip-interval [0-30]	[0-30]	Set the interval (in minutes) for keeping the IP address before it is released.

		When set to 0, the IP address will be released immediately
Switch(config)# diagnostics dhcp-client option [15 | 16 | 60] [identifier]	[15 | 16 | 60] [identifier]	Configure the DHCP option and the corresponding value for the selected option. **NOTE:** **1.** Before configuring Option 15 or Option 16, ensure that the device is set to DHCPv6 mode. **2.** Before configuring Option 60, ensure that the device is set to DHCPv4 mode.
Switch(config)# diagnostics dhcp-client source-mac [xx:xx:xx:xx:xx:xx]	[xx:xx:xx:xx:xx:xx]	Configure the source MAC address for the DHCP client.
Switch(config)# diagnostics dhcp-client vlan [1-4094]	[1-4094]	Configure the VLAN ID for the DHCP client. Valid range is from 1 to 4094.
No Command	**Parameter**	**Description**
Switch(config)# no diagnostics dhcp-client		Reset all DHCP client configurations for diagnostics to default values.
Switch(config)# no diagnostics dhcp-client ip-version ipv6 auto-configuration		Reset the DHCPv6 auto-configuration type to the default value (Stateless).
Switch(config)# no diagnostics dhcp-client keep-ip-interval		Reset the DHCP client keep IP interval to the default value (0, which means immediate release).
Switch(config)# no diagnostics dhcp-client option		Reset all DHCP client options to their default values and clear the fields.
Switch(config)# no diagnostics dhcp-client option [15 | 16 | 60]	[15 | 16 | 60]	Reset the specified DHCP option (15, 16, or 60) to its default value and clear the corresponding field.
Switch(config)# no diagnostics dhcp-client source-mac		Reset the DHCP client source MAC address to the default value of all 0.
Switch(config)# no diagnostics dhcp-client vlan		Reset the DHCP client VLAN to the default value of VLAN ID 1.
Show Command	**Parameter**	**Description**
Switch(config)# show diagnostics dhcp-client		Show the current configuration of DHCP client diagnostics.

2.5.27.1.3 DNS Diagnostics.

Diagnostics Command	Parameter	Description
Switch(config)# diagnostics dns ip-version ipv4 mode dhcpv4		Configure the DNS diagnostics mode to use DHCPv4 for IPv4 addresses.
Switch(config)# diagnostics dns ip-version ipv4 mode static		Configure the DNS diagnostics mode to use static IPv4.

Switch(config)# diagnostics dns ip-version ipv4 mode static ip [A.B.C.D] [255.X.X.X] [A.B.C.D]	[A.B.C.D] [255.X.X.X] [A.B.C.D]	Set the following parameters for IPv4 static mode: **1. [A.B.C.D]:** Source IPv4 address **2. [255.X.X.X]:** Source subnet mask **3. [A.B.C.D]:** Source default gateway
Switch(config)# diagnostics dns ip-version ipv6 mode dhcpv6		Configure the DNS diagnostics mode to use DHCPv6 for IPv6 addresses.
Switch(config)# diagnostics dns ip-version ipv6 mode dhcpv6 auto-configuration [stateless | stateful]	[stateless | stateful]	Set the DHCPv6 auto-configuration type for DNS diagnostics to either stateless or stateful. **Stateless:** The device generates its own IP address based on the network prefix, with the DHCPv6 server only providing additional configuration information (like DNS). **Stateful**: The DHCPv6 server assigns the device a full IP address and manages its lease.
Switch(config)# diagnostics dns ip-version ipv6 mode static		Configure the DNS diagnostics mode to use static IPv6.
Switch(config)# diagnostics dns ip-version ipv6 mode static ipv6 [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] [A:B:C:D:E:F:G:H]	Set the following parameters for IPv6 static mode: **1. [A:B:C:D:E:F:G:H]:** Source IPv6 address **2. [10-128]:** Source prefix length **3. [A:B:C:D:E:F:G:H]:** Source default IPv6 gateway
Switch(config)# diagnostics dns dns-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]	Configure the DNS server with an IPv4 or IPv6 address. **NOTE:** Set the IP version mode before configuring the DNS server IP address.
Switch(config)# diagnostics dns option [15 | 16 | 60] [identifier]	[15 | 16 | 60] [identifier]	Configure the DHCP option and the corresponding value for the selected option. **NOTE:** **1.** Before configuring Option 15 or Option 16, ensure that the device is set to DHCPv6 mode. **2.** Before configuring Option 60, ensure that the device is set to DHCPv4 mode.
Switch(config)# diagnostics dns source-mac [xx:xx:xx:xx:xx:xx]	[xx:xx:xx:xx:xx:xx]	Configure the source MAC address for DNS diagnostics.
Switch(config)# diagnostics dns domain-name [domain name]	[domain name]	Configure the destination domain name for DNS diagnostics.

Switch(config)# diagnostics dns vlan [1-4094]	[1-4094]	Configure the VLAN ID for DNS diagnostics. Valid range is from 1 to 4094.
No Command	**Parameter**	**Description**
Switch(config)# no diagnostics dns		Reset all DNS configurations for diagnostics to default values.
Switch(config)# no diagnostics dns dns-server		Reset the DNS server IP address to the default value of 0.0.0.0.
Switch(config)# no diagnostics dns ip-version ipv4 mode dhcpv4		Configure the DNS diagnostics mode to use static IPv4.
Switch(config)# no diagnostics dns ip-version ipv4 mode static		Configure the DNS diagnostics mode to use DHCPv4 for IPv4 addresses.
Switch(config)# no diagnostics dns ip-version ipv4 mode static ip		Reset the configured source IP address, subnet mask and gateway to default for IPv4 static mode.
Switch(config)# no diagnostics dns ip-version ipv6 mode dhcpv6		Configure the DNS diagnostics mode to use static IPv6.
Switch(config)# no diagnostics dns ip-version ipv6 mode dhcpv6 auto-configuration		Reset the DHCPv6 auto-configuration type to the default value (Stateless)
Switch(config)# no diagnostics dns ip-version ipv6 mode static		Configure the DNS diagnostics mode to use DHCPv6 for IPv6 addresses.
Switch(config)# no diagnostics dns ip-version ipv6 mode static ipv6		Reset the configured source IP address, prefix length and gateway to default for IPv6 static mode.
Switch(config)# no diagnostics dns option		Reset all DHCP options to their default values and clear the fields.
Switch(config)# no diagnostics dns option [15 | 16 | 60]	[15 | 16 | 60]	Reset the specified DHCP option (15, 16, or 60) to its default value and clear the corresponding field.
Switch(config)# no diagnostics dns source-mac		Reset the source MAC address of DNS diagnositcs to the default value of all 0.
Switch(config)# no diagnostics dns domain-name		Reset the domain name of DNS diagnositcs to the default value.
Switch(config)# no diagnostics dns vlan		Reset the VLAN of DNS diagnostics to the default value of VLAN ID 1.
Show Command	**Parameter**	**Description**
Switch(config)# show diagnostics dns		Show the current configuration of DNS diagnostics.

2.5.27.1.4 IPTV Diagnostics.

1. IPTV general query interval Diagnostics.

Diagnostics Command	Parameter	Description

Switch(config)# diagnostics iptv gen-query-interval maximum query-interval-waiting-time [1-10]	[1-10]	Configure the maximum waiting time for IPTV general query interval diagnostics, ranging from 1 to 10 minutes.
Switch(config)# diagnostics iptv gen-query-interval maximum record-times [1-60]	[1-60]	Configure the maximum record times for IPTV general query interval diagnostics, ranging from 1 to 60.
Switch(config)# diagnostics iptv gen-query-interval mcast-router interface [port_list]	[port_list]	Specify the multicast router port for IPTV general query interval diagnostics.
Switch(config)# diagnostics iptv gen-query-interval mcast-router interface existing-igmp-router-port		Use the existing IGMP router port as the multicast router port for IPTV general query interval diagnostics.
Switch(config)# diagnostics iptv gen-query-interval threshold alarm [100-110]	[100-110]	Configure the alarm threshold for IPTV general query interval diagnostics, with a range of 100 to 110 seconds.
Switch(config)# diagnostics iptv gen-query-interval threshold warning [70-80]	[70-80]	Configure the warning threshold for IPTV general query interval diagnostics, with a range of 70 to 80 seconds.
Switch(config)# diagnostics iptv gen-query-interval vlan [1-4094]	[1-4094]	Configure the VLAN ID for IPTV general query interval diagnostics. Valid range is from 1 to 4094.
No Command	**Parameter**	**Description**
Switch(config)# no diagnostics iptv gen-query-interval		Reset all IPTV general query interval configurations for diagnostics to default values.
Switch(config)# no diagnostics iptv gen-query-interval maximum query-interval-waiting-time		Reset the maximum waiting time for IPTV general query interval diagnostics to the default value of 10 minutes.
Switch(config)# no diagnostics iptv gen-query-interval maximum record-times		Reset the maximum record times for IPTV general query interval diagnostics to the default value of 60.
Switch(config)# no diagnostics iptv gen-query-interval mcast-router		Reset the IPTV general query interval multicast router port to the default value of port 6.
Switch(config)# no diagnostics iptv gen-query-interval mcast-router existing-igmp-router-port		Remove the configuration that uses the existing IGMP router port as the multicast router port for IPTV general query interval diagnostics.
Switch(config)# no diagnostics iptv gen-query-interval threshold		Reset all threshold settings for IPTV general query interval diagnostics to the default values: alarm = 100, warning = 70.
Switch(config)# no diagnostics iptv gen-query-interval threshold alarm		Reset the threshold alarm for IPTV general query interval diagnostics to the default value of 100 seconds.
Switch(config)# no diagnostics iptv gen-query-interval threshold warning		Reset the threshold warning for IPTV general query interval diagnostics to the default value of 70 seconds.

Switch(config)# diagnostics iptv gen-query-interval vlan		Reset the VLAN of IPTV general query interval diagnostics to the default value of VLAN ID 1.
Show Command	**Parameter**	**Description**
Switch(config)# show diagnostics iptv gen-query-interval		Show the current configuration of IPTV general query interval diagnostics.

2. IPTV general query response Diagnostics.

Diagnostics Command	Parameter	Description
Switch(config)# diagnostics iptv gen-query-response maximum query-interval-waiting-time [1-10]	[1-10]	Configure the maximum query interval waiting time for IPTV general query response, ranging from 1 to 10 minutes.
Switch(config)# diagnostics iptv gen-query-response maximum record-times [1-60]	[1-60]	Configure the maximum record times for IPTV general query response diagnostics, ranging from 1 to 60.
Switch(config)# diagnostics iptv gen-query-response mcast-client interface [port_list]	[port_list]	Specify the multicast client port for IPTV general query response diagnostics.
Switch(config)# diagnostics iptv gen-query-response mcast-router interface [port_list]	[port_list]	Specify the multicast router port for IPTV general query response diagnostics.
Switch(config)# diagnostics iptv gen-query-response mcast-router interface existing-igmp-router-port		Use the existing IGMP router port as the multicast router interface for IPTV general query response diagnostics.
Switch(config)# diagnostics iptv gen-query-response threshold alarm [10-12]	[10-12]	Configure the alarm threshold for IPTV general query response diagnostics, with a range of 10 to 12 seconds.
Switch(config)# diagnostics iptv gen-query-response threshold warning [7-9]	[7-9]	Configure the warning threshold for IPTV general query response diagnostics, with a range of 7 to 9 seconds.
Switch(config)# diagnostics iptv gen-query-response vlan [1-4094]	[1-4094]	Configure the VLAN ID for IPTV general query response diagnostics. Valid range is from 1 to 4094.
No Command	**Parameter**	**Description**
Switch(config)# no diagnostics iptv gen-query-response		Reset all IPTV general query response configurations for diagnostics to default values.
Switch(config)# no diagnostics iptv gen-query-response maximum query-interval-waiting-time		Reset the maximum waiting time for IPTV general query response diagnostics to the default value of 10 minutes.
Switch(config)# no diagnostics iptv gen-query-response maximum record-times		Reset the maximum record times for IPTV general query interval diagnostics to the default value of 60.

Switch(config)# no diagnostics iptv gen-query-response mcast-client		Reset the IPTV general query response multicast client port to the default value of port 1.
Switch(config)# diagnostics iptv gen-query-response mcast-router		Reset the IPTV general query response multicast router port to the default value of port 6.
Switch(config)# diagnostics iptv gen-query-response mcast-router existing-igmp-router-port		Remove the configuration that uses the existing IGMP router port as the multicast router port for IPTV general query response diagnostics.
Switch(config)# no diagnostics iptv gen-query-response threshold		Reset all threshold settings for IPTV general query response diagnostics to the default values: alarm = 10, warning = 7.
Switch(config)# no diagnostics iptv gen-query-response threshold alarm		Reset the threshold alarm for IPTV general query response diagnostics to the default value of 10 seconds.
Switch(config)# no diagnostics iptv gen-query-response threshold warning		Reset the threshold warning for IPTV general query response diagnostics to the default value of 7 seconds.
Switch(config)# diagnostics iptv gen-query-response vlan		Reset the VLAN of IPTV general query response diagnostics to the default value of VLAN ID 1.
Show Command	**Parameter**	**Description**
Switch(config)# show diagnostics iptv gen-query-response		Show the current configuration of IPTV general query response diagnostics.

3. IPTV MPEG-loss Diagnostics.

Diagnostics Command	**Parameter**	**Description**
Switch(config)# diagnostics iptv mpeg-loss dhcp		Enabled DHCP mode for IPTV MPEG Loss diagnostics.
Switch(config)# diagnostics iptv mpeg-loss destination-l4-port [1 | 2 | 3] [any | 1024-65535]	[1 | 2 | 3] [any | 1024-65535]	Configure the Layer 4 port number for IPTV MPEG Loss diagnostics. 1. **[1 | 2 | 3]:** Specify the index, ranging from 1 to 3. 2. **[any | 1024-65535]:** Set the Layer 4 port number, either "any" for any port or a value between 1024 and 65535.
Switch(config)# diagnostics iptv mpeg-loss diagnostic-mode [normal | pid | per-second]	[normal | pid | per-second]	Configure the iptv MPEG Loss diagnostic mode. **normal:** Supports up to 3 streams simultaneously with a diagnostic period of up to 1440 minutes (1 day). **pid:** Supports 1 stream at a time with a diagnostic period of up to 60 minutes (1 hour). **NOTE:** Each stream PID corresponds to

		a different service (e.g., video, audio, logo, subtitle), making it easier to identify which service is experiencing packet loss. **per-second:** Supports up to 3 streams simultaneously with a diagnostic period of up to 60 minutes (1 hour).
Switch(config)# diagnostics iptv mpeg-loss diagnostic-period [1-1440]	[1-1440]	Configure the diagnostic period for IPTV MPEG Loss testing, with a range of 1 to 1440 minutes.
Switch(config)# diagnostics iptv mpeg-loss mcast-router interface [port_list]	[port_list]	Specify the multicast router port for IPTV MPEG Loss diagnostics.
Switch(config)# diagnostics iptv mpeg-loss mcast-router interface existing-igmp-router-port		Use the existing IGMP router port as the multicast router interface for IPTV MPEG Loss diagnostics.
Switch(config)# diagnostics iptv mpeg-loss option [60] [identifier]	[60] [identifier]	Configure the DHCP option and the corresponding value for the selected option.
Switch(config)# diagnostics iptv mpeg-loss search-stream-time [5-30]	[5-30]	Configure the stream search time for IPTV MPEG loss diagnostics, ranging from 5 to 30 seconds.
Switch(config)# diagnostics iptv mpeg-loss source-mac [xx:xx:xx:xx:xx:xx]	[xx:xx:xx:xx:xx:xx]	Configure the source MAC address for IPTV MPEG Loss diagnostics.
Switch(config)# diagnostics iptv mpeg-loss stream-ip-address [1 | 2 | 3]	[1 | 2 | 3]	Enable the specifid stream index for IPTV MPEG Loss diagnostics.
Switch(config)# diagnostics iptv mpeg-loss stream-ip-address [1 | 2 | 3] [A.B.C.D]	[1 | 2 | 3] [A.B.C.D]	Assign IP address to the specified stream index for IPTV MPEG Loss diagnostics
Switch(config)# diagnostics iptv mpeg-loss stream-ip-address auto		Activate the auto search mode to automatically detect the stream IP address.
Switch(config)# diagnostics iptv mpeg-loss stream-ip-address manual		Activate the manual search mode, where the stream IP address must be configured manually
Switch(config)# diagnostics iptv mpeg-loss vlan [1-4094]	[1-4094]	Configure the VLAN ID for IPTV MPEG Loss diagnostics. Valid range is from 1 to 4094.
No Command	**Parameter**	**Description**
Switch(config)# no diagnostics iptv mpeg-loss		Reset all IPTV MPEG Loss configurations for diagnostics to default values.
Switch(config)# no diagnostics iptv mpeg-loss dhcp		Disable DHCP mode for IPTV MPEG Loss diagnostics.
Switch(config)# no diagnostics iptv mpeg-loss destination-l4-port		Reset the Layer 4 port configuration for IPTV MPEG Loss diagnostics to the default value.
Switch(config)# no	[1 | 2 | 3]	Reset the specified index (1 to 3) of the

diagnostics iptv mpeg-loss destination-l4-port [1 | 2 | 3]		Layer 4 port configuration for IPTV MPEG Loss diagnostics to the default value.
Switch(config)# no diagnostics iptv mpeg-loss diagnostic-mode		Reset the diagnostics mode for IPTV MPEG Loss diagnostics to the default value (Normal mode).
Switch(config)# no diagnostics iptv mpeg-loss diagnostic-period		Reset the IPTV MPEG Loss diagnostic period to the default value of 1 minute.
Switch(config)# no diagnostics iptv mpeg-loss mcast-router		Reset the IPTV MPEG Loss multicast router port to the default value of port 6.
Switch(config)# diagnostics iptv mpeg-loss mcast-router existing-igmp-router-port		Remove the configuration that uses the existing IGMP router port as the multicast router interface for IPTV MPEG Loss diagnostics.
Switch(config)# no diagnostics iptv mpeg-loss option		Reset all DHCP options to their default values and clear the fields.
Switch(config)# no diagnostics iptv mpeg-loss option [60]		Reset the specified DHCP option to its default value and clear the corresponding field.
Switch(config)# no diagnostics iptv mpeg-loss search-stream-time		Reset the stream search time for IPTV MPEG loss diagnostics to the default value of 5 seconds.
Switch(config)# no diagnostics iptv mpeg-loss source-mac		Reset the source MAC address of IPTV MPEG loss diagnositcs to the default value of all 0.
Switch(config)# no diagnostics iptv mpeg-loss stream-ip-address		Reset all stream IP address configurations to the default values of IP address 0.0.0.0 and stream mode auto.
Switch(config)# no diagnostics iptv mpeg-loss stream-ip-address [1 | 2 | 3]	[1 | 2 | 3]	Disable the specifid stream index for IPTV throughput diagnostics.
Switch(config)# no diagnostics iptv mpeg-loss stream-ip-address manual		Reset the stream mode from manual to auto.
Switch(config)# no diagnostics iptv mpeg-loss vlan		Reset the VLAN of IPTV MPEG loss diagnostics to the default value of VLAN ID 1.
Show Command	**Parameter**	**Description**
Switch(config)# show diagnostics iptv mpeg-loss		Show the current configuration of IPTV MPEG Loss diagnostics.

4. IPTV PCR-jitter Diagnostics.

Diagnostics Command	Parameter	Description
Switch(config)# diagnostics iptv pcr-jitter dhcp		Enabled DHCP mode for IPTV PCR jitter diagnostics.
Switch(config)# diagnostics iptv pcr-jitter destination-l4-port [1 | 2 | 3] [any | 1024-65535]	[1 | 2 | 3] [any | 1024-65535]	Configure the Layer 4 port number for IPTV PCR jitter diagnostics. 1. **[1 | 2 | 3]:** Specify the index, ranging

		from 1 to 3. 2. **[any | 1024-65535]:** Set the Layer 4 port number, either "any" for any port or a value between 1024 and 65535.
Switch(config)# diagnostics iptv pcr-jitter mcast-router interface [port_list]	[port_list]	Specify the multicast router port for IPTV PCR Jitter diagnostics.
Switch(config)# diagnostics iptv pcr-jitter mcast-router interface existing-igmp-router-port		Use the existing IGMP router port as the multicast router interface for IPTV PCR Jitter diagnostics.
Switch(config)# diagnostics iptv pcr-jitter option [60] [identifier]	[60] [identifier]	Configure the DHCP option and the corresponding value for the selected option.
Switch(config)# diagnostics iptv pcr-jitter source-mac [xx:xx:xx:xx:xx:xx]	[xx:xx:xx:xx:xx:xx]	Configure the source MAC address for IPTV PCR Jitter diagnostics.
Switch(config)# diagnostics iptv pcr-jitter stream-ip-address [1 | 2 | 3]	[1 | 2 | 3]	Enable the specifid stream index for IPTV PCR Jitter diagnostics.
Switch(config)# diagnostics iptv pcr-jitter stream-ip-address [1 | 2 | 3] [A.B.C.D]	[1 | 2 | 3] [A.B.C.D]	Assign IP address to the specified stream index for IPTV PCR Jitter diagnostics
Switch(config)# diagnostics iptv pcr-jitter stream-ip-address auto		Activate the auto search mode to automatically detect the stream IP address.
Switch(config)# diagnostics iptv pcr-jitter stream-ip-address manual		Activate the manual search mode, where the stream IP address must be configured manually
Switch(config)# diagnostics iptv pcr-jitter vlan [1-4094]	[1-4094]	Configure the VLAN ID for IPTV PCR Jitter diagnostics. Valid range is from 1 to 4094.
No Command	**Parameter**	**Description**
Switch(config)# no diagnostics iptv pcr-jitter		Reset all IPTV PCR Jitter configurations for diagnostics to default values.
Switch(config)# no diagnostics iptv pcr-jitter dhcp		Disable DHCP mode for IPTV PCR Jitter diagnostics.
Switch(config)# no diagnostics iptv pcr-jitter destination-l4-port		Reset the Layer 4 port configuration for IPTV PCR Jitter diagnostics to the default value.
Switch(config)# no diagnostics iptv pcr-jitter destination-l4-port [1 | 2 | 3]		Reset the specified index (1 to 3) of the Layer 4 port configuration for IPTV PCR Jitter diagnostics to the default value.
Switch(config)# no diagnostics iptv pcr-jitter mcast-router		Reset the IPTV PCR Jitter multicast router port to the default value of port 6.
Switch(config)# no diagnostics iptv pcr-jitter mcast-router existing-igmp-router-port		Remove the configuration that uses the existing IGMP router port as the multicast router interface for IPTV PCR Jitter diagnostics.
Switch(config)# no		Reset all DHCP options to their default

diagnostics iptv pcr-jitter option		values and clear the fields.
Switch(config)# no diagnostics iptv pcr-jitter option [60]	[60]	Reset the specified DHCP option to its default value and clear the corresponding field.
Switch(config)# no diagnostics iptv pcr-jitter source-mac		Reset the source MAC address of IPTV PCR Jitter diagnositcs to the default value of all 0.
Switch(config)# no diagnostics iptv pcr-jitter stream-ip-address		Reset all stream IP address configurations to the default values of IP address 0.0.0.0 and stream mode auto.
Switch(config)# no diagnostics iptv pcr-jitter stream-ip-address [1 | 2 | 3]	[1 | 2 | 3]	Disable the specifid stream index for IPTV PCR Jitter diagnostics.
Switch(config)# no diagnostics iptv pcr-jitter stream-ip-address manual		Reset the stream mode from manual to auto.
Switch(config)# no diagnostics iptv pcr-jitter vlan		Reset the VLAN of IPTV PCR Jitter diagnostics to the default value of VLAN ID 1.
Show Command	**Parameter**	**Description**
Switch(config)# show diagnostics iptv pcr-jitter		Show the current configuration of IPTV PCR Jitter diagnostics.

5. IPTV throughput Diagnostics.

Diagnostics Command	Parameter	Description
Switch(config)# diagnostics iptv throughput dhcp		Enabled DHCP mode for IPTV throughput diagnostics.
Switch(config)# diagnostics iptv throughput destination-l4-port [1 | 2 | 3] [any | 1024-65535]	[1 | 2 | 3] [any | 1024-65535]	Configure the Layer 4 port number for IPTV throughput diagnostics. 1. **[1 | 2 | 3]:** Specify the index, ranging from 1 to 3. 2. **[any | 1024-65535]:** Set the Layer 4 port number, either "any" for any port or a value between 1024 and 65535.
Switch(config)# diagnostics iptv throughput diagnostic-period [1-1440]	[1-1440]	Configure the diagnostic period for IPTV throughput testing, with a range of 1 to 1440 minutes.
Switch(config)# diagnostics iptv throughput mcast-router interface [port_list]	[port_list]	Specify the multicast router port for IPTV throughput diagnostics.
Switch(config)# diagnostics iptv throughput mcast-router interface existing-igmp-router-port		Use the existing IGMP router port as the multicast router port for IPTV throughput diagnostics.
Switch(config)# diagnostics iptv throughput option [60] [identifier]	[60] [identifier]	Configure the DHCP option and the corresponding value for the selected option.
Switch(config)# diagnostics iptv throughput source-mac [xx:xx:xx:xx:xx:xx]	[xx:xx:xx:xx:xx:xx]	Configure the source MAC address for IPTV throughput diagnostics.

Switch(config)# diagnostics iptv throughput stream-ip-address [1 | 2 | 3]	[1 | 2 | 3]	Enable the specifid stream index for IPTV throughput diagnostics.
Switch(config)# diagnostics iptv throughput stream-ip-address [1 | 2 | 3] [A.B.C.D]	[1 | 2 | 3] [A.B.C.D]	Assign IP address to the specified stream index for IPTV throughput diagnostics
Switch(config)# diagnostics iptv throughput stream-ip-address auto		Activate the auto search mode to automatically detect the stream IP address.
Switch(config)# diagnostics iptv throughput stream-ip-address manual		Activate the manual search mode, where the stream IP address must be configured manually
Switch(config)# diagnostics iptv throughput vlan [1-4094]	[1-4094]	Configure the VLAN ID for IPTV throughput diagnostics. Valid range is from 1 to 4094.
No Command	**Parameter**	**Description**
Switch(config)# no diagnostics iptv throughput		Reset all IPTV throughput configurations for diagnostics to default values.
Switch(config)# no diagnostics iptv throughput dhcp		Disabled DHCP mode for IPTV throughput diagnostics.
Switch(config)# no diagnostics iptv throughput destination-l4-port		Reset the Layer 4 port configuration for IPTV throughput diagnostics to the default value.
Switch(config)# no diagnostics iptv throughput destination-l4-port [1 | 2 | 3]	[1 | 2 | 3]	Reset the specified index (1 to 3) of the Layer 4 port configuration for IPTV throughput diagnostics to the default value.
Switch(config)# no diagnostics iptv throughput diagnostic-period		Reset the IPTV throughput diagnostic period to the default value of 1 minute.
Switch(config)# no diagnostics iptv throughput mcast-router		Reset the IPTV throughput multicast router port to the default value of port 6.
Switch(config)# no diagnostics iptv throughput mcast-router existing-igmp-router-port		Remove the configuration that uses the existing IGMP router port as the multicast router interface for IPTV throughput diagnostics.
Switch(config)# no diagnostics iptv throughput option		Reset all DHCP options to their default values and clear the fields.
Switch(config)# no diagnostics iptv throughput option [60]	[60]	Reset the specified DHCP option to its default value and clear the corresponding field.
Switch(config)# no diagnostics iptv throughput source-mac		Reset the source MAC address of IPTV throughput diagnositcs to the default value of all 0.
Switch(config)# no diagnostics iptv throughput stream-ip-address		Reset all stream IP address configurations to the default values of IP address 0.0.0.0 and stream mode auto.
Switch(config)# no diagnostics iptv throughput stream-ip-address [1 | 2 | 3]	[1 | 2 | 3]	Disable the specifid stream index for IPTV throughput diagnostics.

Switch(config)# no diagnostics iptv throughput stream-ip-address manual		Reset the stream mode from manual to auto.
Switch(config)# no diagnostics iptv throughput vlan		Reset the VLAN of IPTV throughput diagnostics to the default value of VLAN ID 1.
Show Command	**Parameter**	**Description**
Switch(config)# show diagnostics iptv throughput		Show the current configuration of IPTV throughput diagnostics.

6. IPTV zapping time Diagnostics.

Diagnostics Command	**Parameter**	**Description**
Switch(config)# diagnostics iptv zapping-time maximum join-waiting-time [1-300]	[1-300]	Configure the maximum join waiting time for IPTV zapping time diagnostics, ranging from 1 to 300 seconds.
Switch(config)# diagnostics iptv zapping-time maximum record-times [1-60]	[1-60]	Configure the maximum record times for IPTV Zapping time diagnostics, ranging from 1 to 60.
Switch(config)# diagnostics iptv zapping-time mcast-client interface [port_list]	[port_list]	Specify the multicast client port for IPTV Zapping time diagnostics.
Switch(config)# diagnostics iptv zapping-time mcast-router interface [port_list]	[port_list]	Specify the multicast router port for IPTV Zapping time diagnostics.
Switch(config)# diagnostics iptv zapping-time mcast-router interface existing-igmp-router-port		Use the existing IGMP router port as the multicast router interface for IPTV Zapping time diagnostics.
Switch(config)# diagnostics iptv zapping-time threshold alarm [30-40]	[30-40]	Configure the alarm threshold for IPTV Zapping time diagnostics, with a range of 30 to 40 seconds.
Switch(config)# diagnostics iptv zapping-time threshold warning [10-20]	[10-20]	Configure the warning threshold for IPTV general query response diagnostics, with a range of 10 to 20 seconds.
Switch(config)# diagnostics iptv zapping-time vlan [1-4094]	[1-4094]	Configure the VLAN ID for IPTV general query response diagnostics. Valid range is from 1 to 4094.
No Command	**Parameter**	**Description**
Switch(config)# no diagnostics iptv zapping-time		Reset all IPTV Zapping time configurations for diagnostics to default values.
Switch(config)# no diagnostics iptv zapping-time maximum join-waiting-time		Reset the maximum join waiting time for IPTV Zapping time diagnostics to the default value of 60 seconds.
Switch(config)# no diagnostics iptv zapping-time maximum record-times		Reset the maximum record times for IPTV Zapping time diagnostics to the default value of 60.
Switch(config)# no diagnostics iptv zapping-		Reset the IPTV Zapping time multicast client port to the default value of port 1.

time mcast-client		
Switch(config)# no diagnostics iptv zapping-time mcast-router		Reset the IPTV Zapping time multicast router port to the default value of port 6.
Switch(config)# no diagnostics iptv zapping-time mcast-router existing-igmp-router-port		Remove the configuration that uses the existing IGMP router port as the multicast router port for IPTV Zapping time diagnostics.
Switch(config)# no diagnostics iptv zapping-time threshold		Reset all threshold settings for IPTV Zapping time diagnostics to the default values: alarm = 30, warning = 10.
Switch(config)# no diagnostics iptv zapping-time threshold alarm		Reset the threshold alarm for IPTV Zapping time diagnostics to the default value of 30 seconds.
Switch(config)# no diagnostics iptv zapping-time threshold warning		Reset the threshold warning for IPTV Zapping time diagnostics to the default value of 10 seconds.
Switch(config)# no diagnostics iptv zapping-time vlan		Reset the VLAN of IPTV Zapping time diagnostics to the default value of VLAN ID 1.
Show Command	**Parameter**	**Description**
Switch(config)# show diagnostics iptv zapping-time		Show the current configuration of IPTV Zapping time diagnostics.

2.5.27.1.5 Ping Diagnostics.

Diagnostics Command	Parameter	Description
Switch(config)# diagnostics ping count [1-99]	[1-99]	Specify the number of ping requests to send for diagnostics, ranging from 1 to 99.
Switch(config)# diagnostics ping destination [A.B.C.D | A:B:C:D:E:F:G:H | domain name]	[A.B.C.D | A:B:C:D:E:F:G:H | domain name]	Specify the target IPv4 or IPv6 address, or domain name, for the ping diagnostics.
Switch(config)# diagnostics ping dns-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 IPv4 or IPv6 address of the DNS server for the ping diagnostics.
Switch(config)# diagnostics ping ip-version ipv4 mode dhcpv4		Set the ping diagnostics mode to use DHCPv4 for IPv4 address assignment.
Switch(config)# diagnostics ping ip-version ipv4 mode static		Set the ping diagnostics mode to use a static IPv4 address.
Switch(config)# diagnostics ping ip-version ipv4 mode static ip [A.B.C.D] [255.X.X.X] [A.B.C.D]	[A.B.C.D] [255.X.X.X] [A.B.C.D]	Set the following parameters for IPv4 static mode: 1. **[A.B.C.D]:** Source IPv4 address 2. **[255.X.X.X]:** Source subnet mask 3. **[A.B.C.D]:** Source default gateway
Switch(config)# diagnostics ping ip-version ipv6 mode dhcpv6		Set the ping diagnostics mode to use DHCPv6 for IPv6 address assignment.

Switch(config)# diagnostics ping ip-version ipv6 mode dhcpv6 auto-configuration [stateless | stateful]	[stateless | stateful]	Set the DHCPv6 auto-configuration type for ping diagnostics to either stateless or stateful. **Stateless:** The device generates its own IP address based on the network prefix, with the DHCPv6 server only providing additional configuration information (like DNS). **Stateful**: The DHCPv6 server assigns the device a full IP address and manages its lease.
Switch(config)# diagnostics ping ip-version ipv6 mode static		Set the ping diagnostics mode to use a static IPv6 address.
Switch(config)# diagnostics ping ip-version ipv6 mode static ipv6 [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] [A:B:C:D:E:F:G:H]	Set the following parameters for IPv6 static mode: 1. **[A:B:C:D:E:F:G:H]:** Source IPv6 address 2. **[10-128]:** Source prefix length 3. **[A:B:C:D:E:F:G:H]:** Source default IPv6 gateway Source prefix length Gateway
Switch(config)# diagnostics ping option [15 | 16 | 60] [identifier]	[15 | 16 | 60] [identifier]	Configure the DHCP option and the corresponding value for the selected option.
Switch(config)# diagnostics ping size [1-65500]	[1-65500]	Set the ICMP data size for the ping diagnostics, ranging from 1 to 65500 bytes.
Switch(config)# diagnostics ping source-mac [xx:xx:xx:xx:xx:xx]	[xx:xx:xx:xx:xx:xx]	Configure the source MAC address for Ping diagnostics.
Switch(config)# diagnostics ping timeout [1-99]	[1-99]	Set the timeout duration for the ping diagnostics, ranging from 1 to 99 seconds.
Switch(config)# diagnostics ping vlan [1-4094]	[1-4094]	Configure the VLAN ID for Ping diagnostics. Valid range is from 1 to 4094.
No Command	**Parameter**	**Description**
Switch(config)# no diagnostics ping		Reset all Ping configurations for diagnostics to default values.
Switch(config)# no diagnostics ping count		Reset the number of ping requests to the default value of 1.
Switch(config)# no diagnostics ping destination		Reset the ping destination to the default value of empty.
Switch(config)# no diagnostics ping dns-server		Reset the DNS server address to the default value of 0.0.0.0.
Switch(config)# no diagnostics ping ip-version ipv4 mode dhcpv4		Configure the Ping diagnostics mode to use static IPv4.

Switch(config)# no diagnostics ping ip-version ipv4 mode static		Configure the Ping diagnostics mode to use DHCPv4 for IPv4 addresses.
Switch(config)# no diagnostics ping ip-version ipv4 mode static ip		Reset the configured source IP address, subnet mask and gateway to default for IPv4 static mode.
Switch(config)# no diagnostics ping ip-version ipv6 mode dhcpv6		Configure the Ping diagnostics mode to use static IPv6.
Switch(config)# no diagnostics ping ip-version ipv6 mode dhcpv6 auto-configuration		Reset the DHCPv6 auto-configuration type to the default value (Stateless)
Switch(config)# no diagnostics ping ip-version ipv6 mode static		Configure the Ping diagnostics mode to use DHCPv6 for IPv6 addresses.
Switch(config)# no diagnostics ping ip-version ipv6 mode static ipv6		Reset the configured source IP address, prefix length and gateway to default for IPv6 static mode.
Switch(config)# no diagnostics ping option		Reset all DHCP options to their default values and clear the fields.
Switch(config)# no diagnostics ping option [15 | 16 | 60]	[15 | 16 | 60]	Reset the specified DHCP option (15, 16, or 60) to its default value and clear the corresponding field.
Switch(config)# no diagnostics ping size		Reset the ICMP data size to the default value of 64 Bytes.
Switch(config)# no diagnostics ping source-mac		Reset the source MAC address of Ping diagnositcs to the default value of all 0.
Switch(config)# no diagnostics ping timeout		Reset the ping timeout duration to the default value of 1 second.
Switch(config)# no diagnostics ping vlan		Reset the VLAN of Ping diagnostics to the default value of VLAN ID 1.
Show Command	**Parameter**	**Description**
Switch(config)# show diagnostics ping		Show the current configuration of Ping diagnostics.

2.5.27.1.6 Throughput Diagnostics.

Diagnostics Command	Parameter	Description
Switch(config)# diagnostics throughput application iperf3		Configure iperf3 for throughput diagnostics.
Switch(config)# diagnostics throughput application nuttcp		Configure nuttcp for throughput diagnostics.
Switch(config)# diagnostics throughput 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]	Configure the destination IPv4 or IPv6 address for throughput diagnostics.
Switch(config)# diagnostics throughput diagnostic-period [10-120]	[10-120]	Configure the diagnostic period for throughput testing, ranging from 10 to 120 seconds

Switch(config)# diagnostics throughput ip-version ipv4 mode dhcpv4		Configure the throughput diagnostics mode to use DHCPv4 for IPv4 addresses.
Switch(config)# diagnostics throughput ip-version ipv4 mode static		Configure the throughput diagnostics mode to use static IPv4.
Switch(config)# diagnostics throughput ip-version ipv4 mode static ip [A.B.C.D] [255.X.X.X] [A.B.C.D]	[A.B.C.D] [255.X.X.X] [A.B.C.D]	Set the following parameters for IPv4 static mode: 1. **[A.B.C.D]:** Source IPv4 address 2. **[255.X.X.X]:** Source subnet mask 3. **[A.B.C.D]:** Source default gateway
Switch(config)# diagnostics throughput ip-version ipv6 mode dhcpv6		Configure the throughput diagnostics mode to use DHCPv6 for IPv6 addresses.
Switch(config)# diagnostics throughput ip-version ipv6 mode dhcpv6 auto-configuration [stateless | stateful]	[stateless | stateful]	Set the DHCPv6 auto-configuration type for throughput diagnostics to either stateless or stateful. **Stateless:** The device generates its own IP address based on the network prefix, with the DHCPv6 server only providing additional configuration information (like DNS). **Stateful**: The DHCPv6 server assigns the device a full IP address and manages its lease.
Switch(config)# diagnostics throughput ip-version ipv6 mode static		Configure the throughput diagnostics mode to use static IPv6.
Switch(config)# diagnostics throughput ip-version ipv6 mode static ipv6 [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] [A:B:C:D:E:F:G:H]	Set the following parameters for IPv6 static mode: 1. **[A:B:C:D:E:F:G:H]:** Source IPv6 address 2. **[10-128]:** Source prefix length 3. **[A:B:C:D:E:F:G:H]:** Source default IPv6 gateway
Switch(config)# diagnostics throughput option [15 | 16 | 60] [identifier]	[15 | 16 | 60] [identifier]	Configure the DHCP option and the corresponding value for the selected option. **NOTE:** 1. Before configuring Option 15 or Option 16, ensure that the device is set to DHCPv6 mode. 2. Before configuring Option 60, ensure that the device is set to DHCPv4 mode.
Switch(config)# diagnostics throughput packet-type tcp		Configure the throughput diagnostic to use TCP packet type.
Switch(config)# diagnostics throughput packet-type udp		Configure the throughput diagnostic to use UDP packet type.

Switch(config)# diagnostics throughput port_number [5001-60000]	[5001-60000]	Specify the application TCP/UDP port number, ranging from 5001 to 60000.
Switch(config)# diagnostics throughput server-lifetime [10-1440]	[10-1440]	Specify the duration for the throughput server, ranging from 10 to 1440 minutes.
Switch(config)# diagnostics throughput source-mac [xx:xx:xx:xx:xx:xx]	[xx:xx:xx:xx:xx:xx]	Configure the source MAC address for throughput diagnostics.
Switch(config)# diagnostics throughput role client-rx		Configure the throughput role as client-receive
Switch(config)# diagnostics throughput role client-tx		Configure the throughput role as client-transmit.
Switch(config)# diagnostics throughput role server		Configure the throughput role as server.
Switch(config)# diagnostics throughput vlan [1-4094]	[1-4094]	Configure the VLAN ID for throughput diagnostics. Valid range is from 1 to 4094.
No Command	**Parameter**	**Description**
Switch(config)# no diagnostics throughput		Reset all throughput configurations for diagnostics to default values.
Switch(config)# no diagnostics throughput application		Reset the throughput application to the default value, which is iperf3.
Switch(config)# no diagnostics throughput destination		Reset the throughput destination to the default value, which is empty.
Switch(config)# no diagnostics throughput diagnostic-period		Reset the diagnostic period to the default value of 10 seconds
Switch(config)# no diagnostics throughput ip-version ipv4 mode dhcpv4		Configure the throughput diagnostics mode to use static IPv4.
Switch(config)# no diagnostics throughput ip-version ipv4 mode static		Configure the throughput diagnostics mode to use DHCPv4 for IPv4 addresses.
Switch(config)# no diagnostics throughput ip-version ipv4 mode static ip		Reset the configured source IP address, subnet mask and gateway to default for IPv4 static mode.
Switch(config)# no diagnostics throughput ip-version ipv6 mode dhcpv6		Configure the throughput diagnostics mode to use static IPv6.
Switch(config)# no diagnostics throughput ip-version ipv6 mode dhcpv6 auto-configuration		Reset the DHCPv6 auto-configuration type to the default value (Stateless)
Switch(config)# no diagnostics throughput ip-version ipv6 mode static		Configure the DNS diagnostics mode to use DHCPv6 for IPv6 addresses.
Switch(config)# no diagnostics throughput ip-version ipv6 mode static ipv6		Reset the configured source IP address, prefix length and gateway to default for IPv6 static mode.
Switch(config)# no		Reset all DHCP options to their default

diagnostics throughput option		values and clear the fields.
Switch(config)# no diagnostics throughput option [15 | 16 | 60]	[15 | 16 | 60]	Reset the specified DHCP option (15, 16, or 60) to its default value and clear the corresponding field.
Switch(config)# no diagnostics throughput packet-type		Reset the packet type to the default value of TCP.
Switch(config)# no diagnostics throughput port-number		Reset the port number to the default value of 5001.
Switch(config)# no diagnostics throughput server-lifetime		Reset the server lifetime to the default value of 10 minutes.
Switch(config)# no diagnostics throughput source-mac		Reset the source MAC address of throughput diagnositcs to the default value of all 0.
Switch(config)# no diagnostics throughput role		Reset the role to the default value of client-tx.
Switch(config)# no diagnostics throughput vlan		Reset the VLAN of throughput diagnostics to the default value of VLAN ID 1.
Show Command	**Parameter**	**Description**
Switch(config)# show diagnostics throughput		Show the current configuration of throughput diagnostics.

2.5.27.2 Perform Diagnostics

This section includes commands for executing diagnostics, whether as one-time or periodic operations. It also includes commands for stopping diagnostics, viewing results, and configuring result display settings, ensuring flexible and efficient diagnostic workflows.

Perform one-time diagnostics

Diagnostics Command	Parameter	Description
Switch(config)# diagnostics start cable		Start the cable diagnostics session.
Switch(config)# diagnostics start dhcp-client		Start the DHCP client diagnostics session.
Switch(config)# diagnostics start dns		Start the DNS diagnostics session.
Switch(config)# diagnostics start iptv throughput		Start the IPTV throughput diagnostics session.
Switch(config)# diagnostics start iptv gen-query-interval		Start the IPTV general query interval session.
Switch(config)# diagnostics start iptv gen-query-response		Start the IPTV general query response diagnostics session.
Switch(config)# diagnostics start iptv mpeg-loss		Start the IPTV MPEG Loss diagnostics session.
Switch(config)# diagnostics start iptv pcr-jitter		Start the IPTV PCR Jitter diagnostics session.
Switch(config)# diagnostics start iptv zapping-time		Start the IPTV zapping time diagnostics session.
Switch(config)# diagnostics start ping		Start the PING diagnostics session.
Switch(config)# diagnostics start throughput		Start the throughput diagnostics session.

Stop the ongoing diagnostics process.

Diagnostics Command	Parameter	Description
Switch(config)# diagnostics stop		Stop the currently running diagnostics.

Show diagnostics result

Diagnostics Command	Parameter	Description
Switch(config)# show diagnostics result		Display the most recent results of one-time diagnostics.
Switch(config)# show diagnostics result terminal-length [0-512]	[0-512]	Set the number of lines per page displayed on the screen for diagnostic results, with 0 disabling pausing.

Perform diagnostics periodically.

Diagnostics Command	Parameter	Description
Switch(config)# diagnostics schedule [1-3]	[1-3]	Enter the corresponding diagnostics schedule index configuration mode.

Switch(config-schedule-index)# active		Enable the selected diagnostic schedule index.
Switch(config-schedule-index)# diagnostics configuration cable		Set up cable diagnostics details for scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.1 Cable Diagnostics for further commands.
Switch(config-schedule-index)# diagnostics configuration dhcp-client		Set up DHCP Client diagnostics details for scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.2 DHCP client Diagnostics for further commands.
Switch(config-schedule-index)# diagnostics configuration dns		Set up DNS diagnostics details for scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.3 DNS Diagnostics for further commands.
Switch(config-schedule-index)# diagnostics configuration iptv gen-query-interval		Set up IPTV general query interval diagnostics details for scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.4 IPTV Diagnostics for further commands.
Switch(config-schedule-index)# diagnostics configuration iptv gen-query-response		Set up IPTV general query response diagnostics details for scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.4 IPTV Diagnostics for further commands.
Switch(config-schedule-index)# diagnostics configuration iptv mpeg-loss		Set up IPTV MPEG Loss diagnostics details for scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.4 IPTV Diagnostics for further commands.
Switch(config-schedule-index)# diagnostics configuration iptv pcr-jitter		Set up IPTV PCR Jitter diagnostics details for scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.4 IPTV Diagnostics for further commands.
Switch(config-schedule-index)# diagnostics configuration iptv throughput		Set up IPTV throughput diagnostics details for scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.4 IPTV Diagnostics for further commands.
Switch(config-schedule-index)# diagnostics configuration iptv zapping-time		Set up IPTV Zapping time diagnostics details for scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.4 IPTV Diagnostics for further

		commands.
Switch(config-schedule-index)# diagnostics configuration ping		Set up Ping diagnostics details for scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.5 Ping Diagnostics for further commands.
Switch(config-schedule-index)# diagnostics configuration throughput		Set up Throughput diagnostics details for scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.6 Throughput Diagnostics for further commands.
Switch(config-schedule-index)# diagnostics item cable		Configure the scheduled diagnostics to perform cable diagnostics for the selected schedule index.
Switch(config-schedule-index)# diagnostics item dhcp-client		Configure the scheduled diagnostics to perform DHCP client diagnostics for the selected schedule index.
Switch(config-schedule-index)# diagnostics item dns		Configure the scheduled diagnostics to perform DNS diagnostics for the selected schedule index.
Switch(config-schedule-index)# diagnostics item iptv gen-query-interval		Configure the scheduled diagnostics to perform IPTV General Query Interval diagnostics for the selected schedule index.
Switch(config-schedule-index)# diagnostics item iptv gen-query-response		Configure the scheduled diagnostics to perform IPTV General Query Response diagnostics for the selected schedule index.
Switch(config-schedule-index)# diagnostics item iptv mpeg-loss		Configure the scheduled diagnostics to perform IPTV MPEG Loss diagnostics for the selected schedule index.
Switch(config-schedule-index)# diagnostics item iptv pcr-jitter		Configure the scheduled diagnostics to perform IPTV PCR Jitter diagnostics for the selected schedule index.
Switch(config-schedule-index)# diagnostics item iptv throughput		Configure the scheduled diagnostics to perform IPTV Throughput diagnostics for the selected schedule index.
Switch(config-schedule-index)# diagnostics item iptv zapping-time		Configure the scheduled diagnostics to perform IPTV Zapping time diagnostics for the selected schedule index.
Switch(config-schedule-index)# diagnostics item ping		Configure the scheduled diagnostics to perform Ping diagnostics for the selected schedule index.
Switch(config-schedule-index)# diagnostics item throughput		Configure the scheduled diagnostics to perform Throughput diagnostics for the selected schedule index.
Switch(config-schedule-index)# periodic-mode one-time [hh:mm date month year]	[hh:mm date month year]	Configure the schedule to run the diagnostic once at the specified time on the given date, month, and year. hh:0-23, mm: 0-59, date: 1-31, month: 1-12, year: 2023-2037

		NOTE: The NTP function must be globally enabled and synchronized with the server before operating scheduled diagnostics. Please refer to the NTP Command Section for more details.
Switch(config-schedule-index)# periodic-mode daily [hh:mm]	[hh:mm]	Configure the schedule to run the diagnostic daily at the specified time. hh: 0-23, mm: 0-59 **NOTE:** The NTP function must be globally enabled and synchronized with the server before operating scheduled diagnostics. Please refer to the NTP Command Section for more details.
Switch(config-schedule-index)# periodic-mode weekly [hh:mm day]	[hh:mm day]	Configure the schedule to run the diagnostic weekly at the specified time on the selected day. hh: 0-23, mm: 0-59, day: sun, mon, tue, wed, thu, fri, sat **NOTE:** The NTP function must be globally enabled and synchronized with the server before operating scheduled diagnostics. Please refer to the NTP Command Section for more details.
Switch(config-schedule-index)# periodic-mode monthly [hh:mm date]	[hh:mm date]	Configure the schedule to run the diagnostic monthly at the specified time on the selected date. hh:0-23, mm: 0-59, date: 1-31 **NOTE:** The NTP function must be globally enabled and synchronized with the server before operating scheduled diagnostics. Please refer to the NTP Command Section for more details.
No Command	**Parameter**	**Description**
Switch(config-schedule-index)# no active		Disable the selected diagnostic schedule index.
Switch(config-schedule-index)# no diagnostics configuration cable		Reset the configured port for cable diagnostics to the default port (port 1) in the scheduled diagnostics.
Switch(config-schedule-index)# no diagnostics configuration dhcp-client		Reset DHCP Client diagnostics details in the scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.2 DHCP client Diagnostics for further commands.
Switch(config-schedule-index)# no diagnostics configuration dns		Reset DNS diagnostics details in the scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section

		2.5.27.1.3 DNS Diagnostics for further commands.
Switch(config-schedule-index)# no diagnostics configuration iptv gen-query-interval		Reset IPTV general query interval diagnostics details in scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.4 IPTV Diagnostics for further commands.
Switch(config-schedule-index)# no diagnostics configuration iptv gen-query-response		Reset IPTV general query response diagnostics details in scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.4 IPTV Diagnostics for further commands.
Switch(config-schedule-index)# no diagnostics configuration iptv mpeg-loss		Reset IPTV MPEG Loss diagnostics details in scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.4 IPTV Diagnostics for further commands.
Switch(config-schedule-index)# no diagnostics configuration iptv pcr-jitter		Reset IPTV PCR Jitter diagnostics details in scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.4 IPTV Diagnostics for further commands.
Switch(config-schedule-index)# no diagnostics configuration iptv throughput		Reset IPTV throughput diagnostics details in scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.4 IPTV Diagnostics for further commands.
Switch(config-schedule-index)# no diagnostics configuration iptv zapping-time		Reset IPTV Zapping time diagnostics details in scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.4 IPTV Diagnostics for further commands.
Switch(config-schedule-index)# no diagnostics configuration ping		Reset Ping diagnostics details in scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.5 Ping Diagnostics for further commands.
Switch(config-schedule-index)# no diagnostics configuration throughput		Reset Throughput diagnostics details in scheduled diagnostics. The configuration process is identical to one-time diagnostics. Please refer to Section 2.5.27.1.6 Throughput Diagnostics for further commands.
Switch(config-schedule-index)# no periodic-mode		Clear the configured diagnostics schedule for the selected schedule index.
Show Command	**Parameter**	**Description**

Switch(config-schedule-index)# show		Display the current settings of the selected schedule index.
Switch(config)# show diagnostics schedule		Display the current settings of all schedule index.
Switch(config)# show diagnostics schedule [1-3]	[1-3]	Display the current settings of the specified schedule index.
Switch(config)# show diagnostics schedule [1-3] result	[1-3]	Display diagnostics results of the specified schedule index.
Switch(config)# show diagnostics schedule [1-3] result terminal-Length [0-512]	[0-512]	Set the number of lines per page displayed on the screen for diagnostic results, with 0 disabling pausing.

3. SNMP NETWORK MANAGEMENT

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

SNMP consists of following key components.

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

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

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

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

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

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

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

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

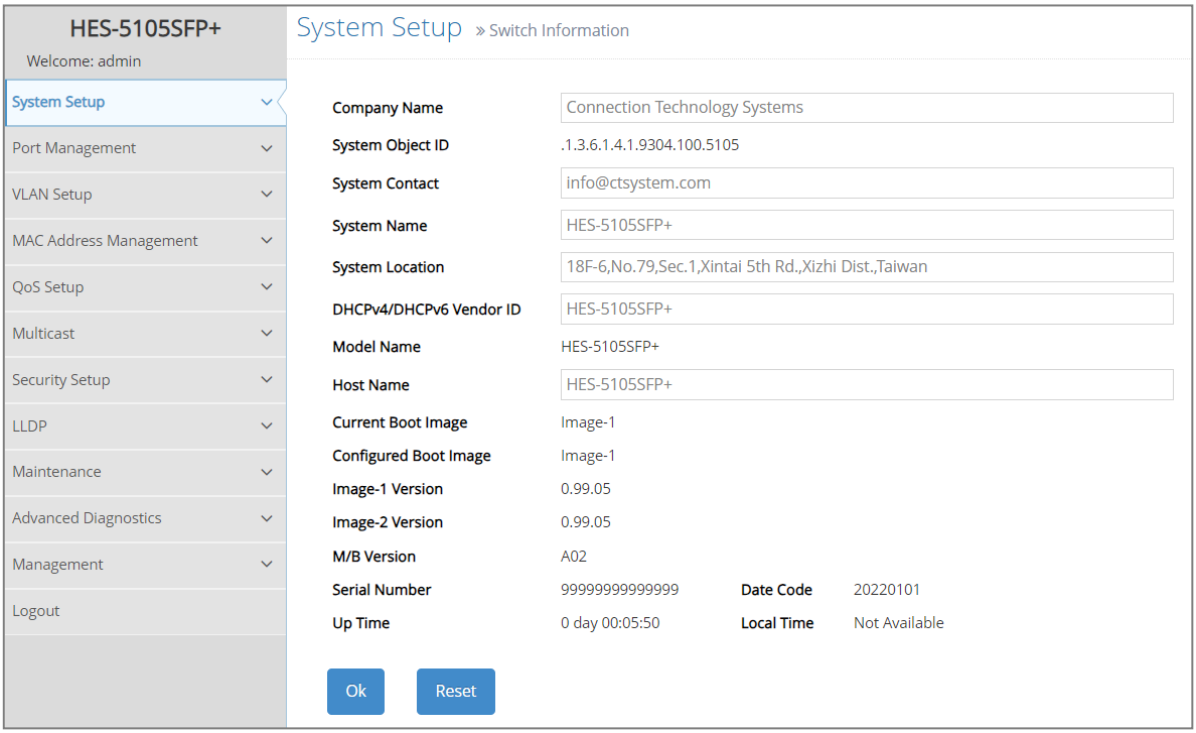
Please refer to the appropriate documentation for the instructions of installing the system private MIB.

4. WEB MANAGEMENT

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

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

After you login successfully, the screen with the Main Menu will show up.

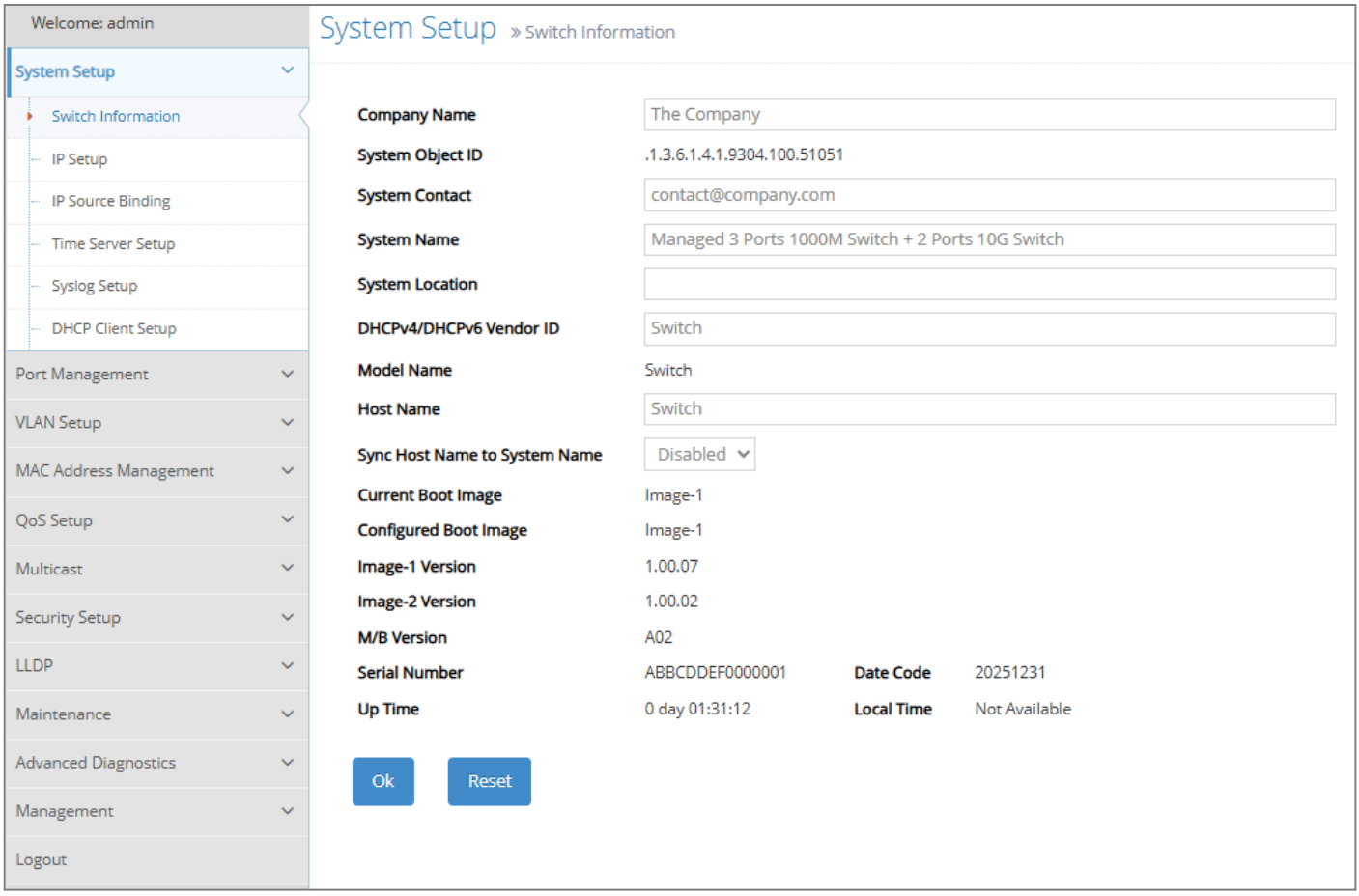


There are 12 main functions in the main menu. We will respectively describe their sub-functions in the following sections of this chapter.

- **System Setup:** Set up or view the Managed Switch's system information, IP address and related information required for network management applications, etc.
- **Port Management:** Set up each port's configuration and monitor the port's status.
- **VLAN Setup:** Set up VLAN mode as well as VLAN configuration, and view the IEEE802.1q VLAN Table of the Managed Switch.
- **MAC Address Management:** Set up MAC address, enable or disable MAC address learning, etc.
- **QoS Setup:** Set up the priority queuing, remarking, rate limit, and so on.
- **Multicast:** Configure IGMP/MLD Snooping and view the IGMP/MLD status and Groups table.
- **Security Setup:** Set up DHCP Snooping, DHCP Option 82 / DHCPv6 Option 37 relay agent, port isolation, storm control, and so on.
- **LLDP:** Enable or disable LLDP on ports, set up LLDP-related attributes, and view the TLV information sent by the connected device with LLDP-enabled.
- **Maintenance:** View the operation status and event logs of the system, ping, lookback test, etc.
- **Advanced Diagnositics:** Perform advanced diagnostics.
- **Management:** Enable or disable the specified network services, view user account management, do the firmware upgrade, load the factory default settings, etc.
- **Logout:** Log out the management interface.

4.1 System Setup

In order to enable network management of the Managed Switch, proper network configuration is required. To do this, click the folder **System Setup** from the **Main Menu** and then 6 options within this folder will be displayed as follows.



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

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

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

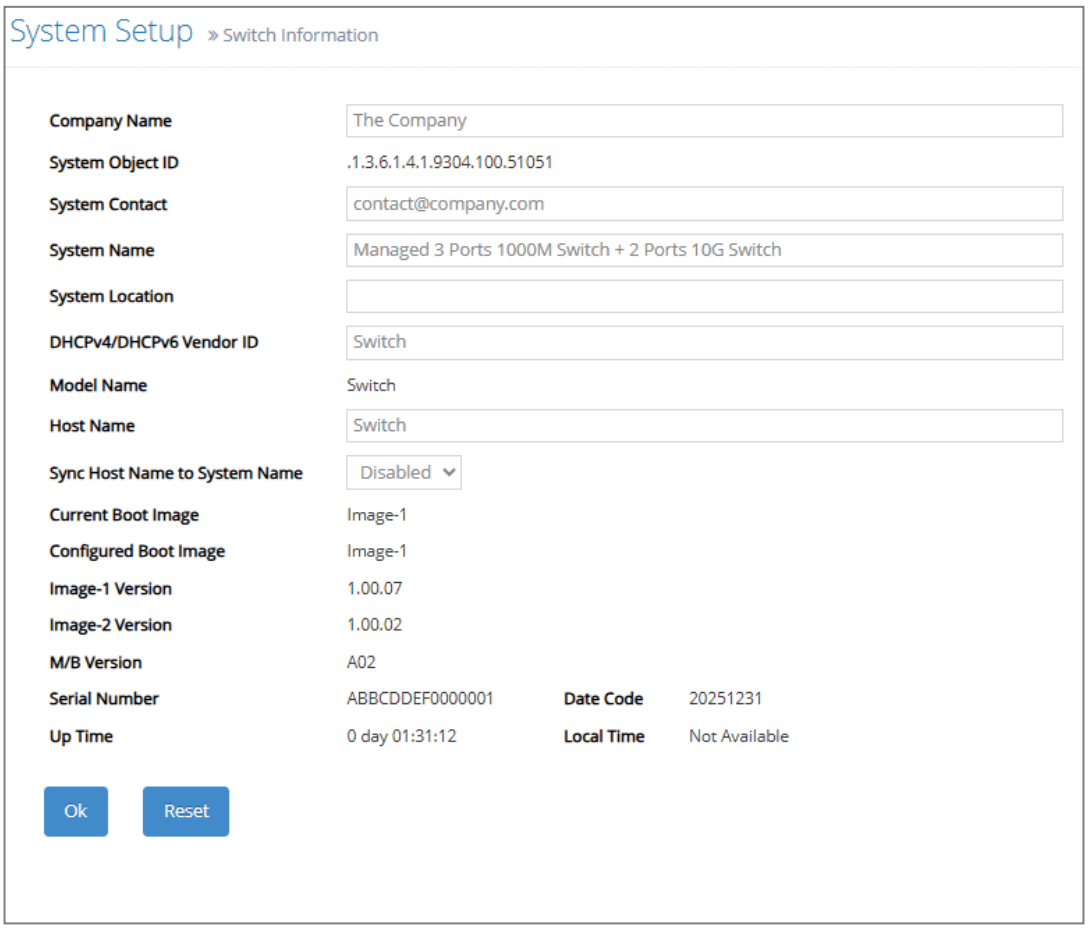
4. **Time Server Setup:** Set up the time server's configuration.

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

6. **DHCP Client Setup:** Enable or disable the DHCP client settings for the Managed Switch to automatically obtain the host name from a DHCP server.

4.1.1 System Information

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



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

System Object ID: Display the predefined System OID.

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

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

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

DHCPv4/DHCPv6 Vendor ID: Vendor Class Identifier. Enter the user-defined DHCP vendor ID, up to 64 alphanumeric characters. Please make sure you have an exact DHCP Vendor ID with the value specified in “vendor-classes” in your dhcpd.conf file. For detailed information, see Appendix B.

Model Name: Display the product’s model name.

Host Name: Enter the product’s host name.

Sync Host Name to System Name: Enable or disable the synchronization of the host name to the system name.

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

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

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

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

M/B Version: Display the main board version.

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

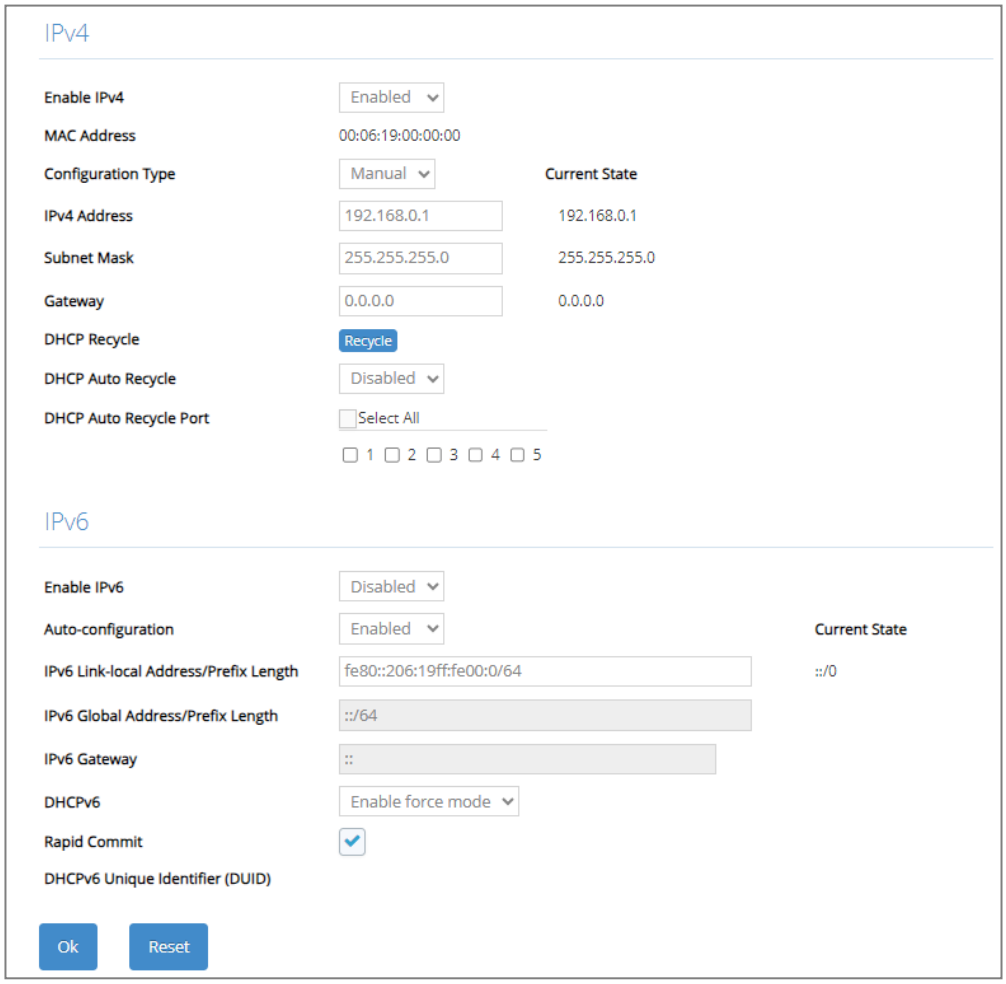
Date Code: Display the date code of the Managed Switch firmware.

Up Time: Display the up time since last restarting.

Local Time: Display the local time of the system.

4.1.2 IP Setup

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



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

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

Configuration Type: There are two configuration types that users can select from the pull-down menu, "**DHCP**" and "**Manual**". When "**DHCP"** is selected and a DHCP server is also available on the network, the Managed Switch will automatically get the IP address from the DHCP server. If "**Manual"** is selected, users need to specify the IP address, Subnet Mask and Gateway.

IPv4 Address: Enter the unique IP address of this Managed Switch. You can use the default IP address or specify a new one when the situation of address duplication occurs or the address does not match up with your network. (The default factory setting is 192.168.0.1.)

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

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

Gateway: Specify the IP address of a gateway or a router, which is responsible for the delivery of the IP packets sent by the Managed Switch. This address is required when the Managed Switch and the network management station are on different networks or subnets. The default value of this parameter is 0.0.0.0, which means no gateway exists and the network management station and Managed Switch are on the same network.

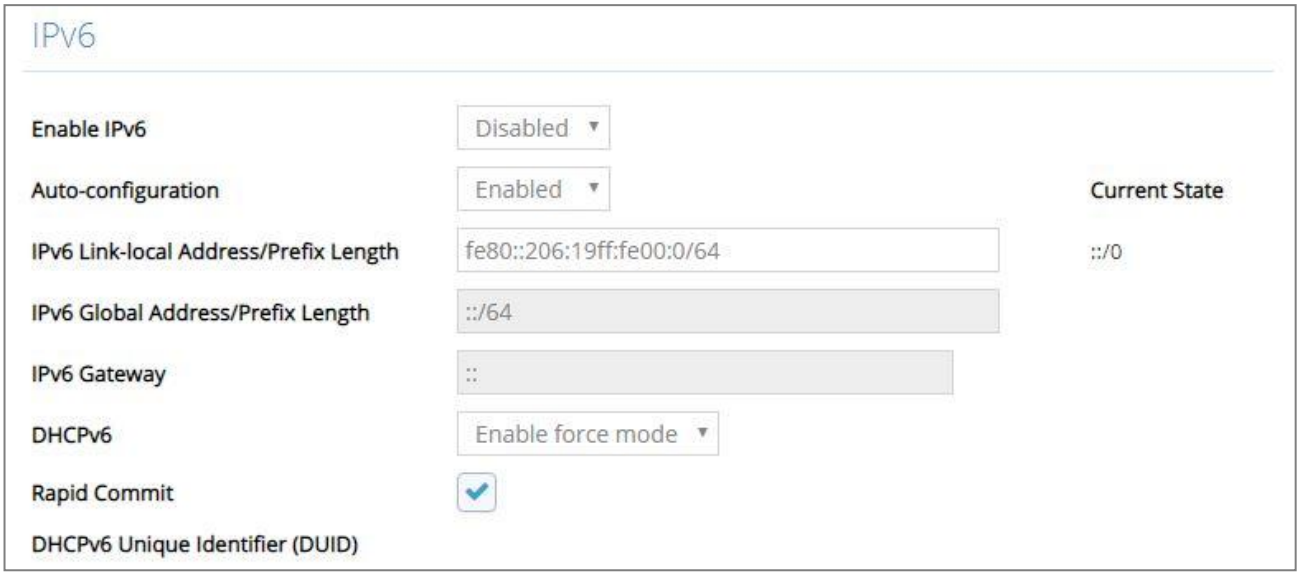
Current State: This view-only field shows currently assigned IP address (by DHCP or manual), Subnet Mask and Gateway of the Managed Switch.

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

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

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

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



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

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

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

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

IPv6 Gateway: Specify the IP address of a gateway or a router, which is responsible for the delivery of the IP packets sent by the Managed Switch. This address is required when the Managed Switch and the network management station are on different networks or subnets.

DHCPv6: Enable or disable DHCPv6 function

Disabled: Disable DHCPv6.

Enable auto mode: Configure DHCPv6 function in auto mode.

Enable force mode: Configure DHCPv6 function in force mode.

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

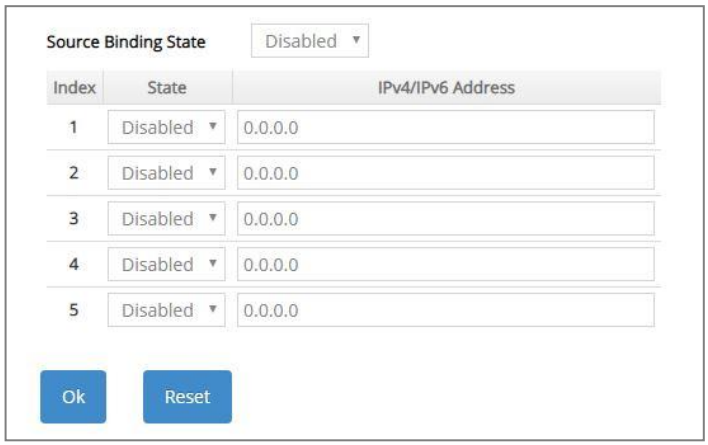
DHCPv6 Unique Identifier (DUID): View-only field that shows the DHCP Unique Identifier (DUID).

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

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

4.1.3 IP Source Binding

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



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

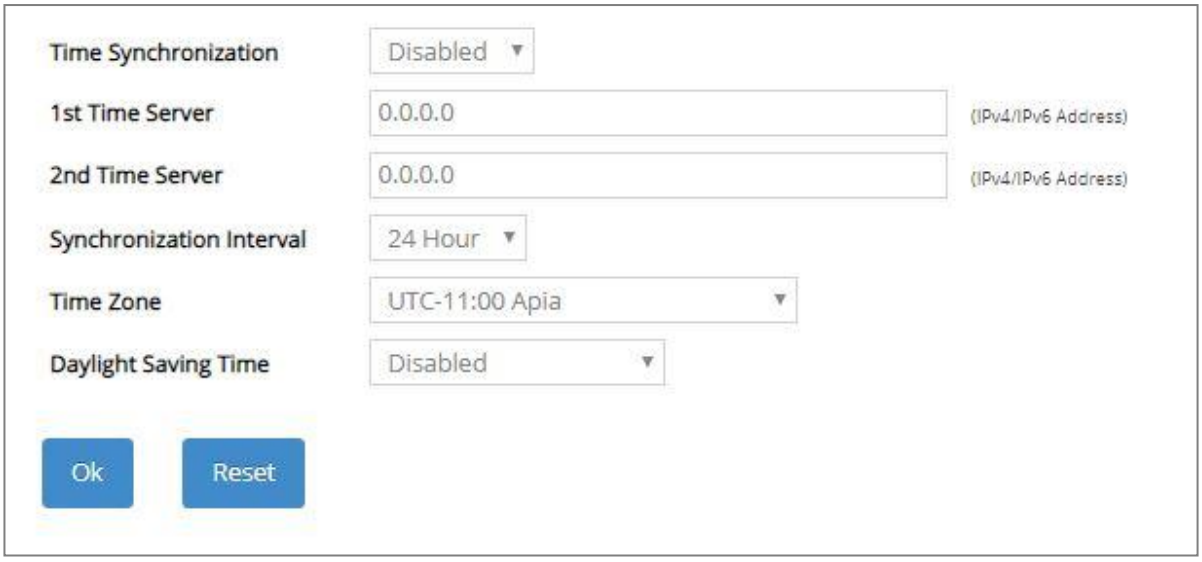
State: Disable or enable the assigned IP address to reach the management.

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

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

4.1.4 Time Server Setup

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



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

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

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

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

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

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

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

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

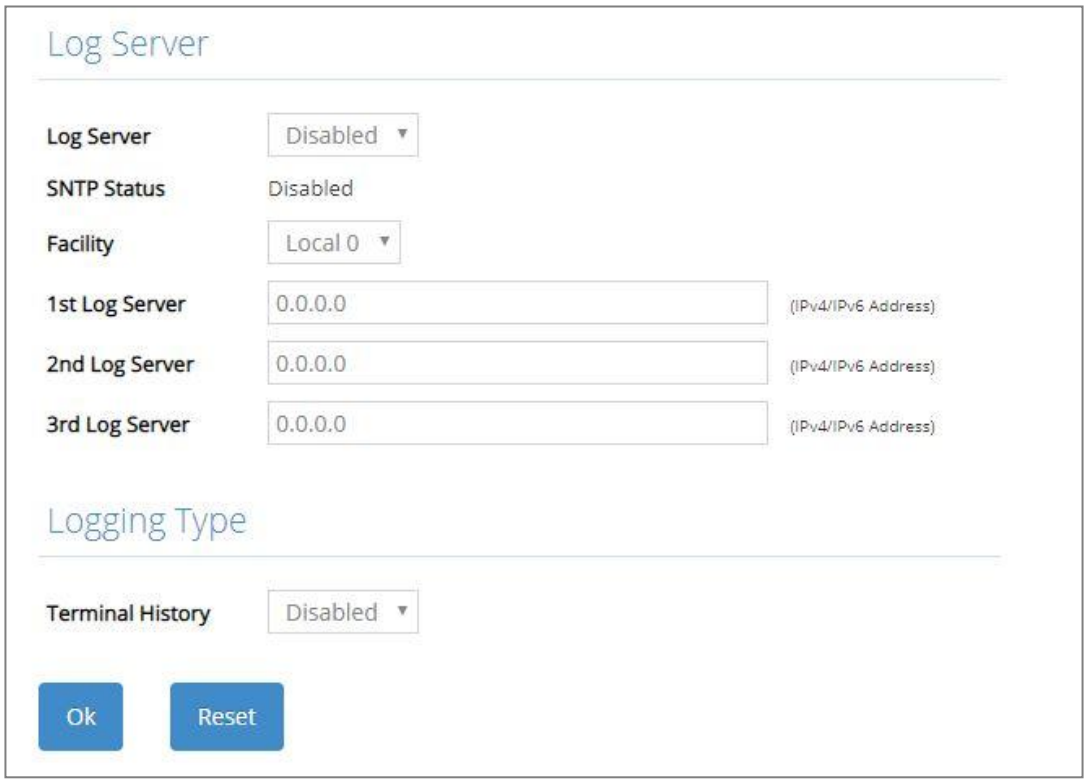
Daylight Saving Time Recurring Start: If the "recurring / Weekday" option is selected in Daylight Saving Time, click the pull-down menu to select the recurring start date of daylight saving time.

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

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

4.1.5 Syslog Setup

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



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

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

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

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

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

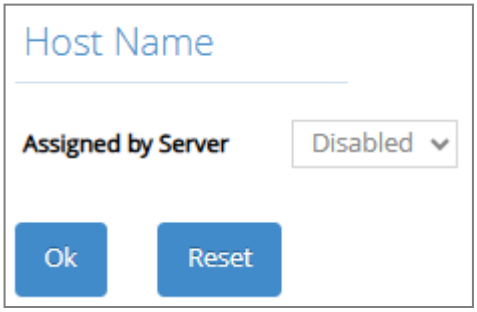
2nd Log Server: Specify the secondary log server's IPv4/IPv6 address. When the first log server is down, the Managed Switch will automatically contact the second or third Log server.

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

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

4.1.6 DHCP Client Setup

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



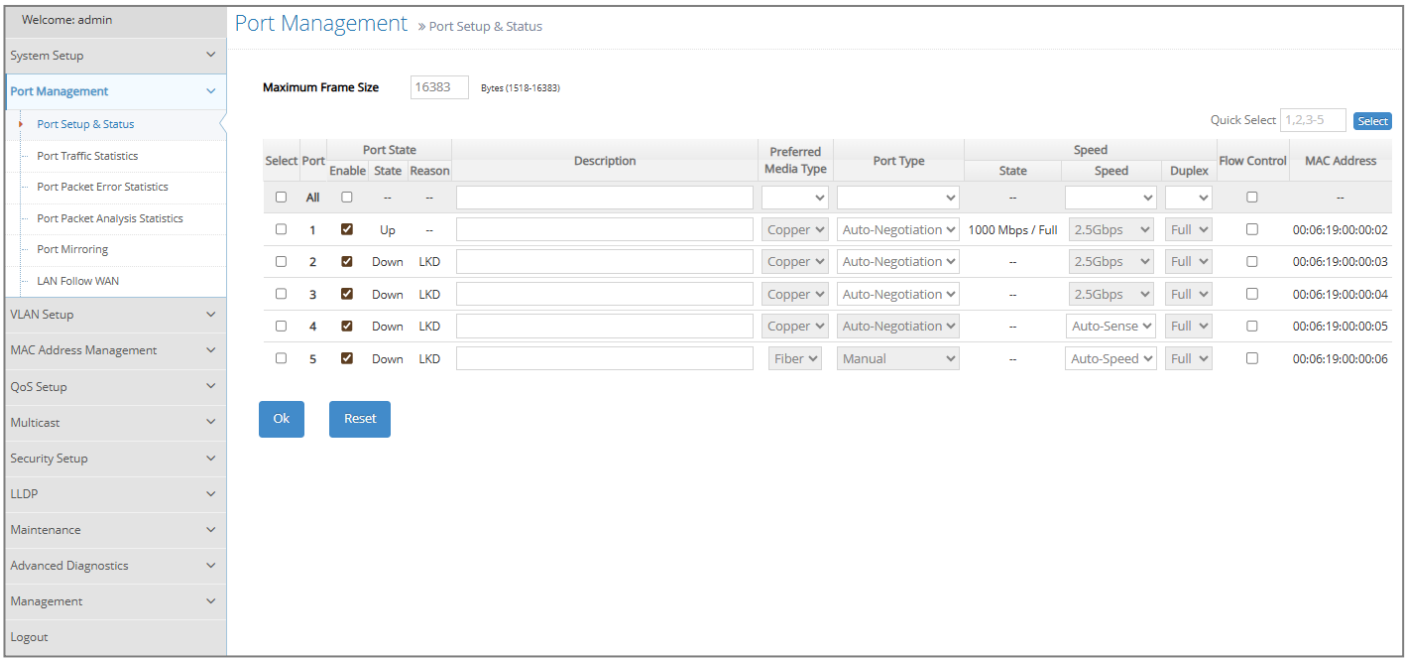
Assigned by Server: Enable or disable the option to automatically obtain the host name assigned by the DHCP server.

Disabled: The host name will not be updated by the DHCP server.

Enabled: If the DHCP Option 12 value received from the server differs from the current host name, the system will automatically update the host name in the running configuration based on the received value. To retain the updated host name after a reboot, you must manually save the configuration.

4.2 Port Management

In order to configure each port of the Managed Switch and monitor the real-time ports' link-up status or traffic counters for maintenance or diagnostic purposes. Select the folder **Port Management** from the **Main Menu** and then 6 options within this folder will be displayed for your selection.



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

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

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

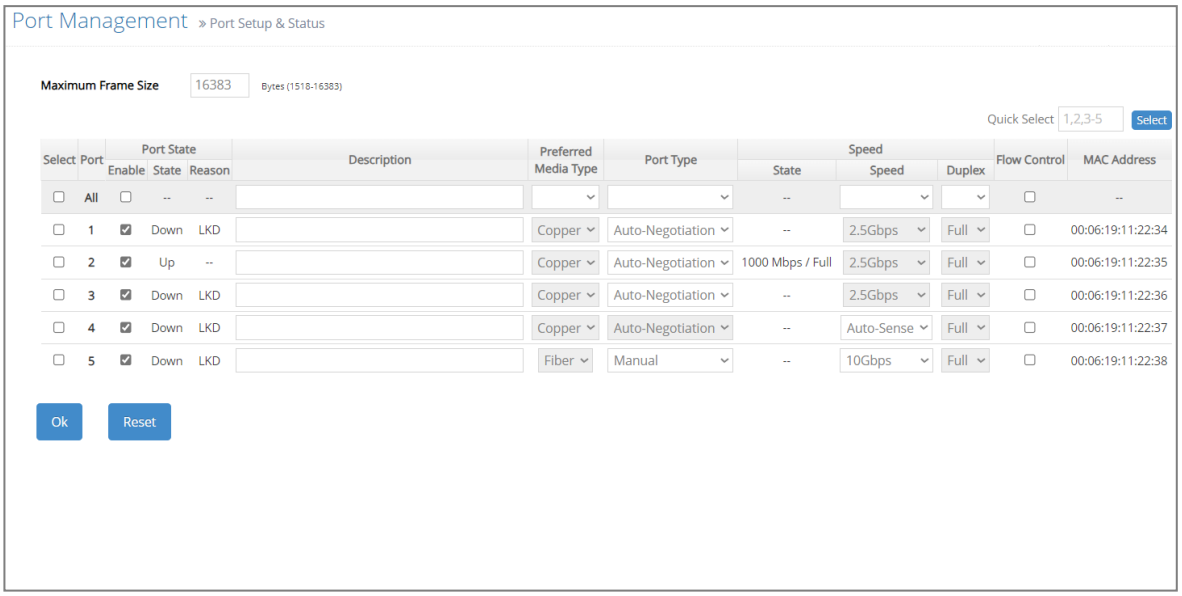
4. **Port Packet Analysis Statistics:** View each port's traffic analysis of packets, e.g. RX/TX frames of Multicast and Broadcast, etc.

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

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

4.2.1 Port Setup & Status

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



Maximum Frame Size: Specify the maximum frame size between 1518 and 16383 bytes. The default maximum frame size is 16383 bytes.

Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-5) in the **Quick Select** field located at the top-right corner of the Port Setup & Status table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Port: The number of the port.

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

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

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

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

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

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

State of Port in Speed field**:** View-only field that shows the current operation speed of ports, which can be 100Mbps/1000Mbps/2.5Gbps in copper port(s) 1-3, 100Mbps/1000Mbps/Auto-

Sense/2.5Gbps/5Gbps/10Gbps in the copper port 4, and 1000Mbps/10Gbps/Auto-Speed in the fiber port 5 and the current operation duplex mode of the port, either Full or Half.

Speed of Port in Speed field**:** When you select “Manual” as port type, you can further specify the transmission speed (100Mbps/1000Mbps/2.5Gbps) of copper port(s) 1-3, (100Mbps/1000Mbps/Auto-Sense/2.5Gbps/5Gbps/10Gbps) of coppert port 4 and (1000Mbps/10Gbps/Auto-Speed) of the fiber port 5. When you select “Auto-Negotiation” as port type for fiber port(s), the transmission speed is 1000Mbps.

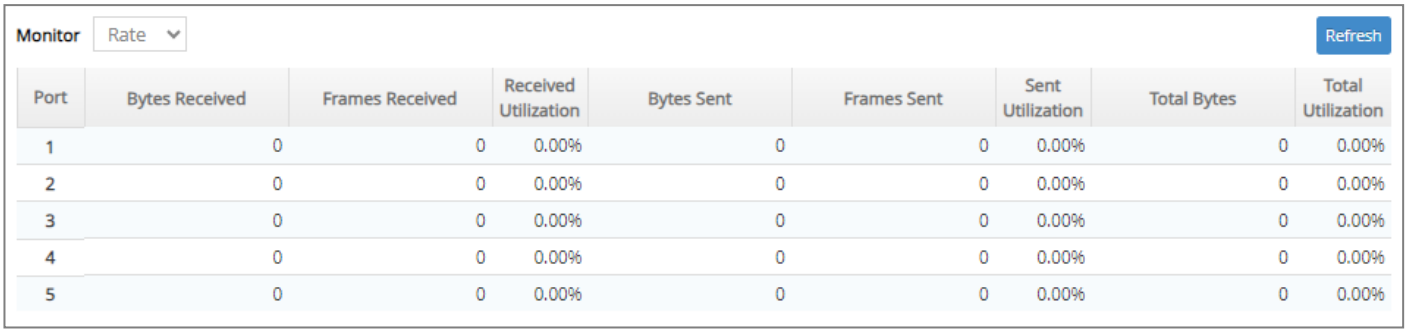
Duplex of Port in Speed field**:** In fiber ports, only the full-duplex operation mode is allowed.

Flow Control: Enable or disable the flow control.

MAC Address: The unique MAC address for each interface.

4.2.2 Port Traffic Statistics

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



Port	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%

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

Bytes Received: Total bytes received from each port.

Frames Received: Total frames received from each port.

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

Bytes Sent: The total bytes sent from current port.

Frames Sent: The total frames sent from current port.

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

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

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

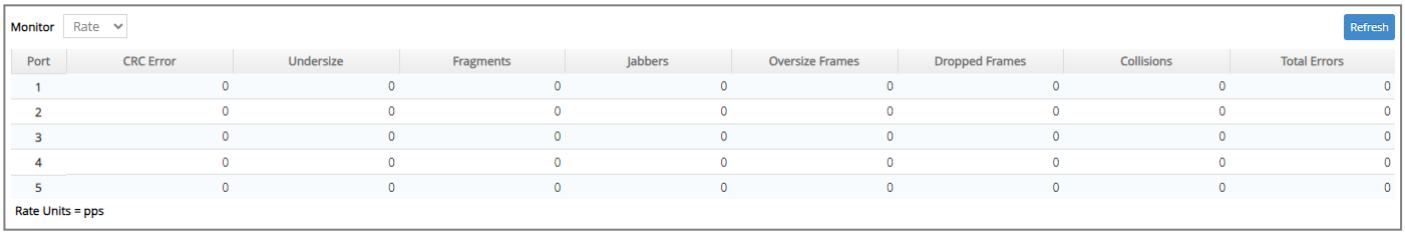
Refresh: Click **Refresh** to update the latest port traffic statistics.

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

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

4.2.3 Port Packet Error Statistics

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



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

CRC Error: CRC Error frames received.

Undersize: Undersize frames received.

Fragments: Fragments frames received.

Jabbers: Jabber frames received.

Oversize Frames: Oversize frames received.

Dropped Frames: Drop frames received.

Collisions: Each port’s Collision frames.

Total Errors: Total error frames received.

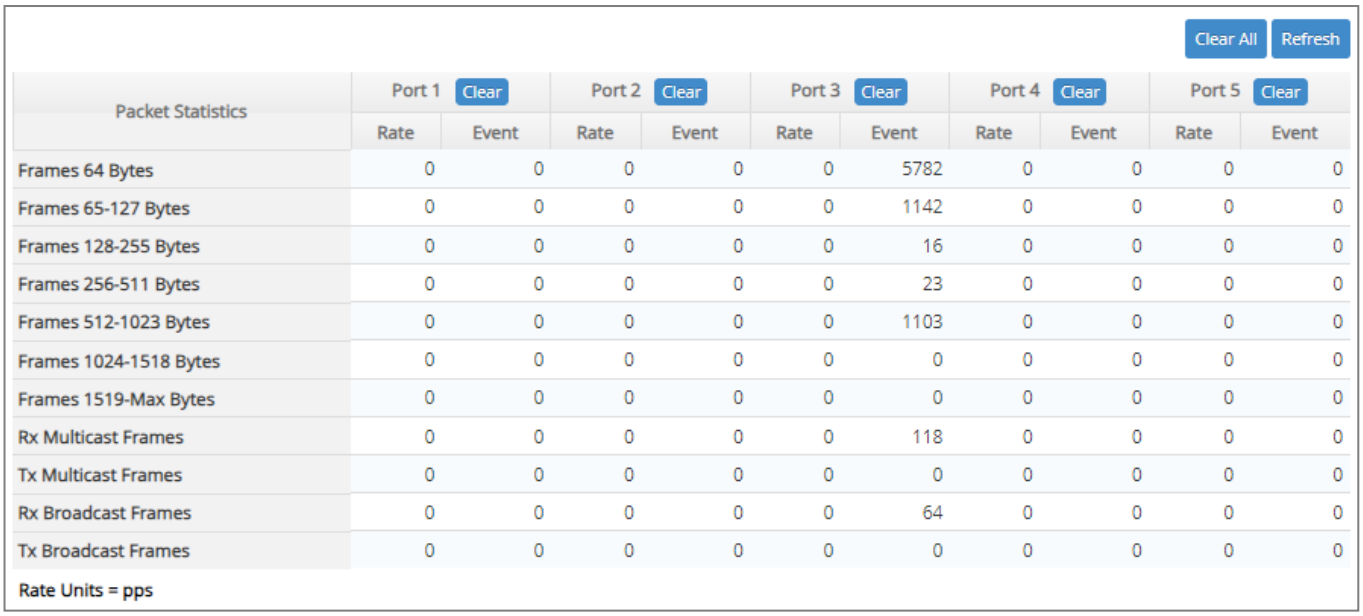
Refresh: Click **Refresh** to update the latest port packet error statistics.

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

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

4.2.4 Port Packet Analysis Statistics

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



Packet Statistics	Port 1 Clear		Port 2 Clear		Port 3 Clear		Port 4 Clear		Port 5 Clear	
	Rate	Event	Rate	Event	Rate	Event	Rate	Event	Rate	Event
Frames 64 Bytes	0	0	0	0	0	5782	0	0	0	0
Frames 65-127 Bytes	0	0	0	0	0	1142	0	0	0	0
Frames 128-255 Bytes	0	0	0	0	0	16	0	0	0	0
Frames 256-511 Bytes	0	0	0	0	0	23	0	0	0	0
Frames 512-1023 Bytes	0	0	0	0	0	1103	0	0	0	0
Frames 1024-1518 Bytes	0	0	0	0	0	0	0	0	0	0
Frames 1519-Max Bytes	0	0	0	0	0	0	0	0	0	0
Rx Multicast Frames	0	0	0	0	0	118	0	0	0	0
Tx Multicast Frames	0	0	0	0	0	0	0	0	0	0
Rx Broadcast Frames	0	0	0	0	0	64	0	0	0	0
Tx Broadcast Frames	0	0	0	0	0	0	0	0	0	0

Rate Units = pps

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.

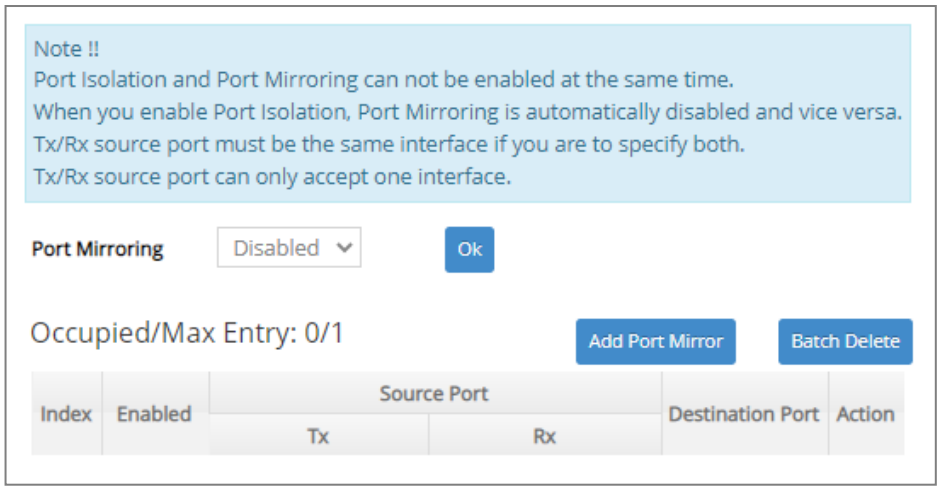
Refresh: Click **Refresh** to update the latest port packet analysis statistics.

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

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

4.2.5 Port Mirroring

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



This table will display the overview of each configured port mirroring. Up to 1 set of port mirroring can be set up.

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

Occupied/Max Entry: View-only field.

> **Occupied:** This shows the amount of total port mirroring(s) that have already been created.
>
> **Max:** This shows the maximum number available for the port mirroring. The maximum number is 1.

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

Enabled: Enable or disable the specific port mirroring.

TX Source Port: Input the port number (e.g.1, 2, 5) to specify the transmitting packets of preferred source port for mirroring. Please note that the port selected as the destination port cannot be the source port.

RX Source Port: Input the port number (e.g.1, 2, 5) to specify the receiving packets of preferred source port for mirroring. Please note that the port selected as the destination port cannot be the source port.

Destination Port: Choose from port 1 to port 5 from the pull-down menu to designate the destination port.

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

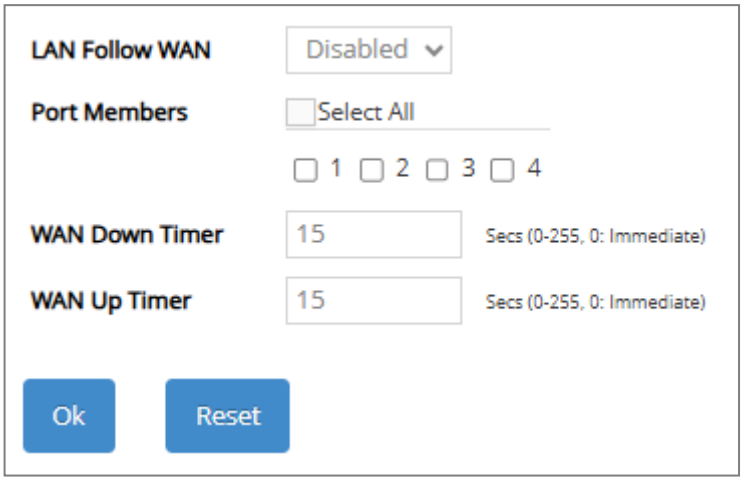
Click the icon to modify the settings of a specified port mirroring.

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

4.2.6 LAN Follow WAN

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

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



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

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

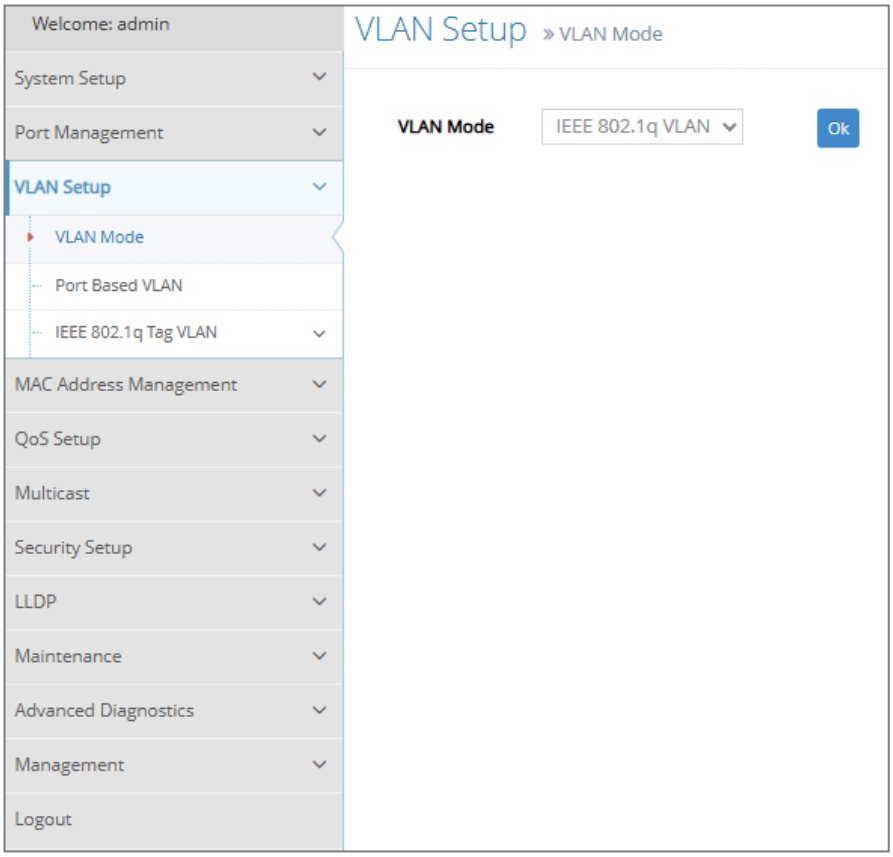
WAN Down Timer: Specify the timer to count down in order to trigger the specific LAN port(s) to do the link down when WAN port's link is down. Vaild range: 0~255 (seconds). "0" stands for "immediate".

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

4.3 VLAN Setup

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

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



Click **VLAN Setup** folder from the **Main Menu** and then three options within this folder will be displayed.

1. VLAN Mode: Configure VLAN mode as Port-Based VLAN or IEEE 802.1q Tag VLAN.

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

3. IEEE 802.1q Tag VLAN: Configure Trunk VLAN Setup, VLAN Interface, and view the VLAN Table.

4.3.1 VLAN Mode

To set up and specify the VLAN mode on which the Managed Switch runs, click the option **VLAN Mode** from the **VLAN Setup** menu and then the following screen page appears.

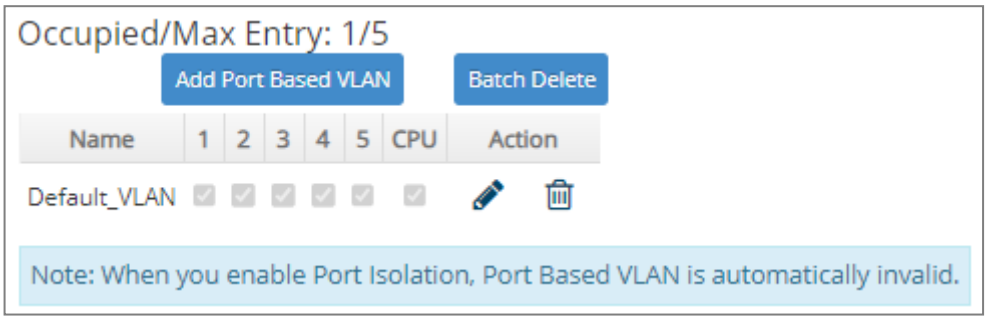
VLAN Mode: Specify **Port Based VLAN**, **IEEE 802.1q Tag VLAN** or **Bypass ctag** from the pull-down menu. The Managed Switch will run VLAN accordingly to the mode that which you decide on. You can then go to Port Based VLAN or IEEE 802.1q VLAN web pages to configure in depth.

Click **OK** after you complete the configuration, and the new setting will be taken effect immediately.

4.3.2 Port Based VLAN

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

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

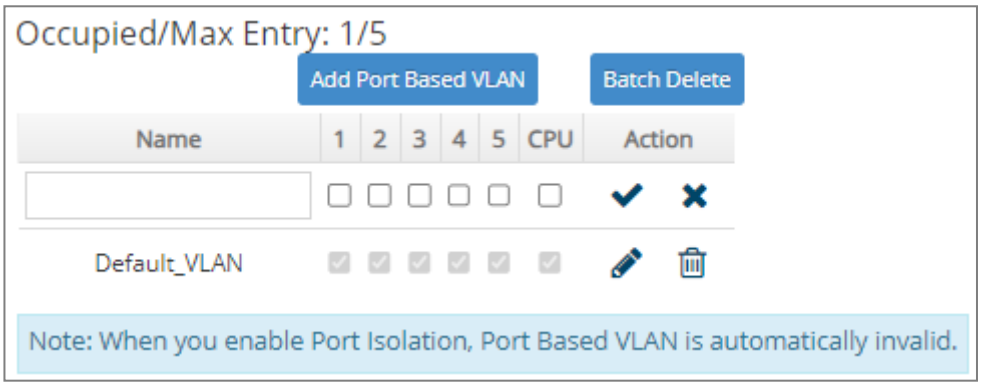


Since source addresses of the packets are listed in MAC address table of specific VLAN (except broadcast/multicast packets), in every VLAN the traffic between two ports will be two-way without restrictions.

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

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

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



Occupied/Max Entry: View-only field.

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

Max: This shows the maximum number of Port-Based VLANs that can be created. The maximum number is 5.

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

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

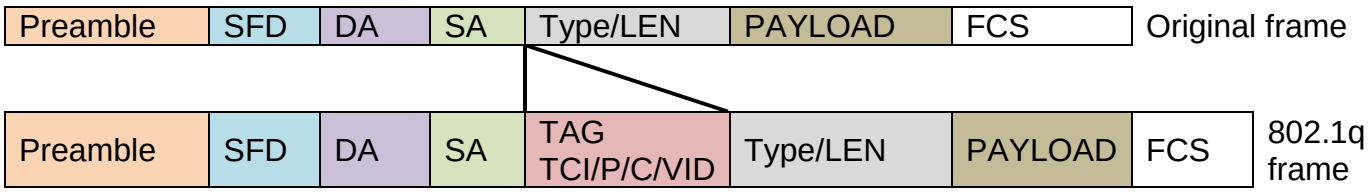
Click ✔ when the settings are completed, this new Port-Based VLAN will be listed on the Port-Based VLAN table, or click ✖ to cancel the settings.

4.3.3 IEEE 802.1q Tag VLAN

802.1Q VLAN Concept

Port-Based VLAN is simple to implement and use, but it cannot be deployed cross switches VLAN. The 802.1Q protocol was developed in order to provide the solution to this problem. By tagging VLAN membership information to Ethernet frames, the IEEE 802.1Q can help network administrators break large switched networks into smaller segments so that broadcast and multicast traffic will not occupy too much available bandwidth as well as provide a higher level security between segments of internal networks.

Introduction to 802.1Q Frame Format:



PRE Preamble	62 bits	Used to synchronize traffic
SFD Start Frame Delimiter	2 bits	Marks the beginning of the header
DA Destination Address	6 bytes	The MAC address of the destination
SA Source Address	6 bytes	The MAC address of the source
TCI Tag Control Info	2 bytes set to 8100 for 802.1p and Q tags	
P Priority	3 bits	Indicates 802.1p priority level 0-7
C Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format - Ethernet set to "0"
VID VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload < or = 1500 bytes User data		
FCS Frame Check Sequence	4 bytes	Cyclical Redundancy Check

Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the switch port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

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

- **Access Mode :**
  Access Links (the link to/from access ports) are the most common type of links on any VLAN switch. All **network hosts (such as PCs)** connect to the switch's Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, **the network hosts** will be allowed to access.

It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal switch. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

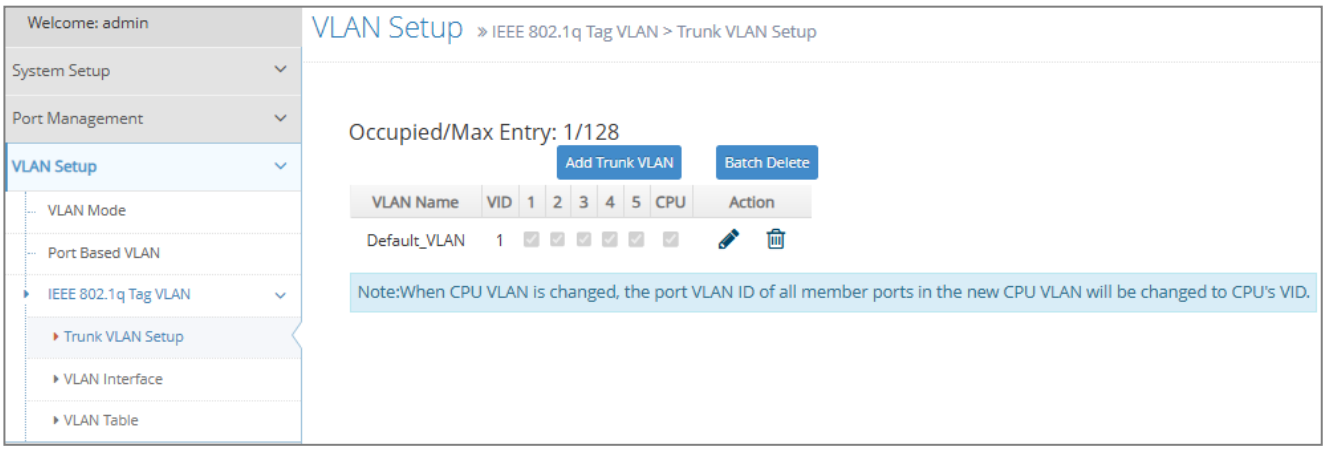
- **Trunk Mode :**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between switches. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple switches.

- **Trunk Native Mode :**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.

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

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



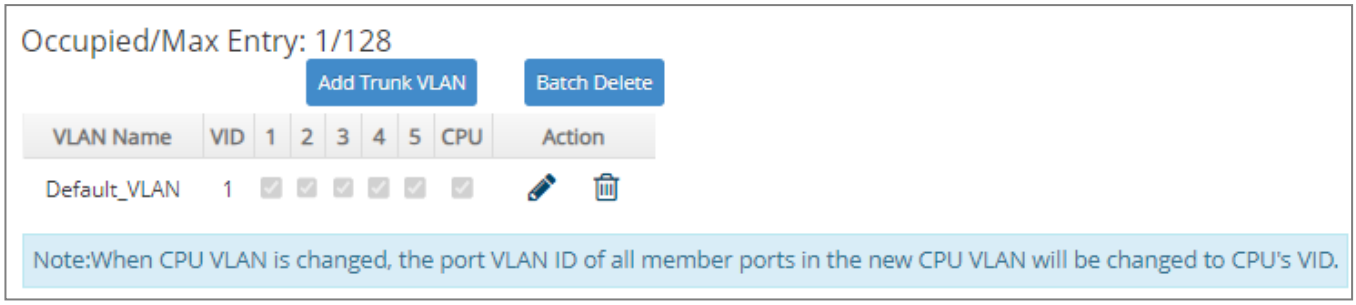
1. **Trunk VLAN Setup:** To create, modify or remove IEEE 802.1q Tag VLAN settings.

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

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

4.3.3.1 Trunk VLAN Setup

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



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

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

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

Occupied/Max Entry: View-only field.

> **Occupied:** This shows the amount of total 802.1q VLANs that have already been created.
>
> **Max:** This shows the maximum number of 802.1q VLANs that can be created. The maximum number is 128.

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

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

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

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

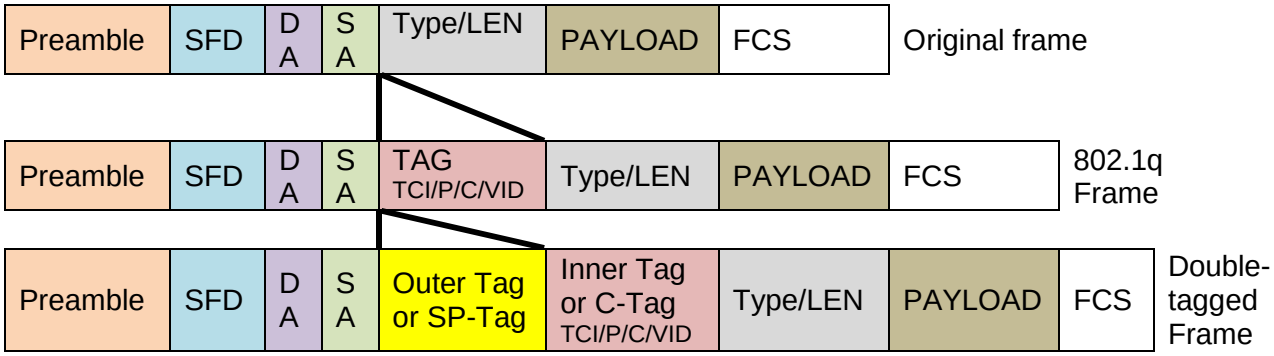
4.3.3.2 VLAN Interface

VLAN Interface function includes IEEE 802.1Q double tagging VLAN configuration. Before you dive into setting it up, take a look at the concepts down below.

Introduction to Q-in-Q (ISP Mode)

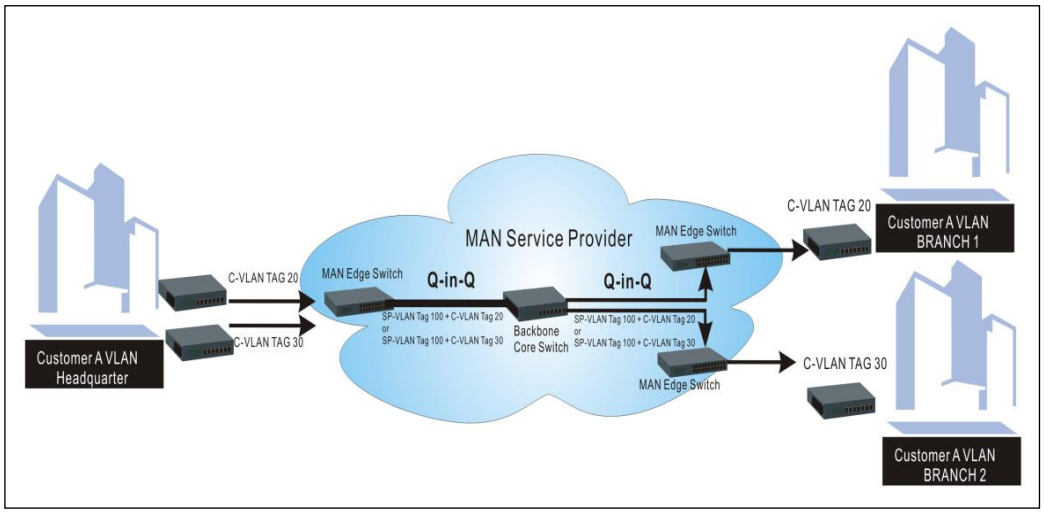
The IEEE 802.1Q double tagging VLAN is also referred to as Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1q VLAN space by tagging the inner tagged packets. In this way, a “double-tagged” frame is created so as to separate customer traffic within a service

provider network. As shown below in “Double-Tagged Frame” illustration, an outer tag is added between source destination and inner tag at the provider network’s edge. This can support C-VLAN (Customer VLAN) over Metro Area Networks and ensure complete separation between traffic from different user groups. Moreover, the addition of double-tagged space increases the number of available VLAN tags which allow service providers to use a single SP-VLAN (Service Provider VLAN) tag per customer over the Metro Ethernet network.



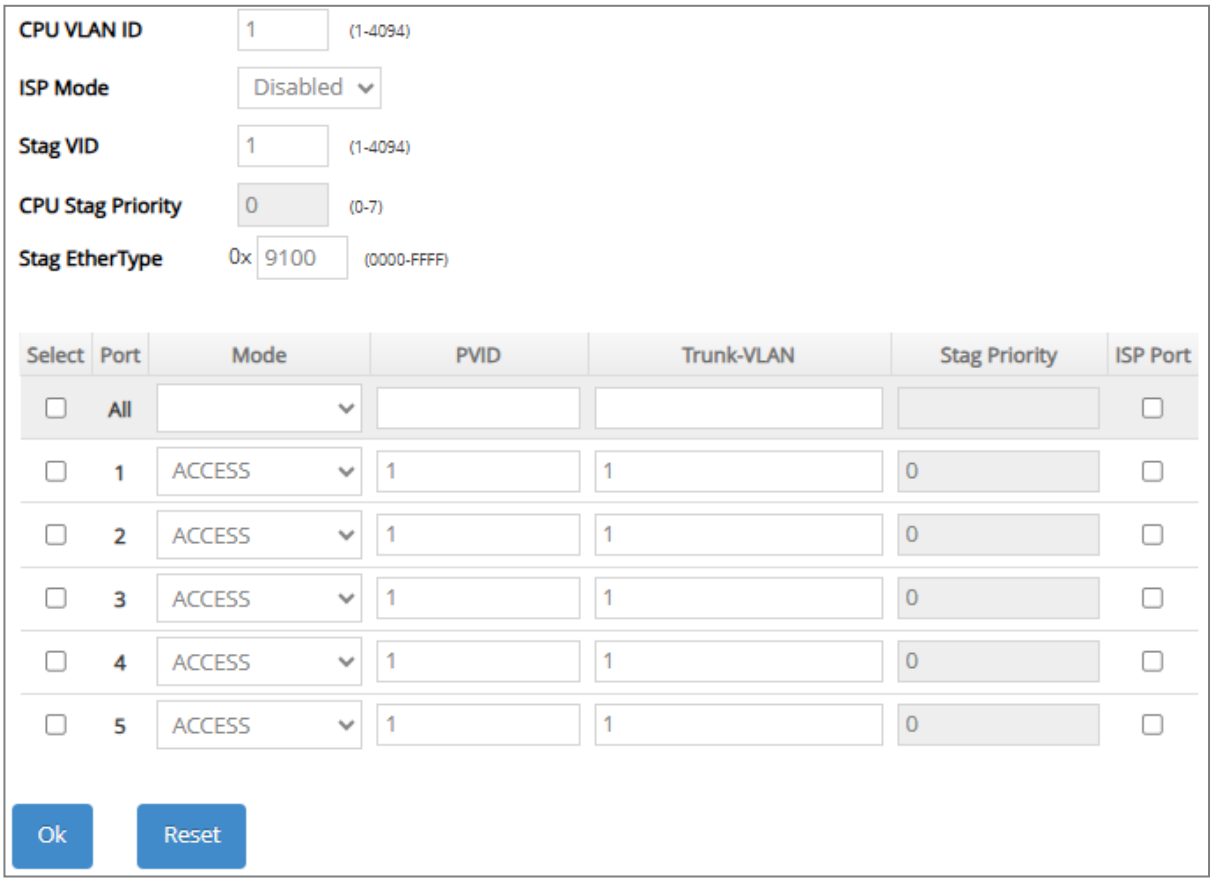
Double-Tagged Frame Format

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



Q-in-Q Example

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



CPU VLAN ID: Specify an existing VLAN ID.

ISP Mode: Enable or disable ISP mode (IEEE 802.1Q double tagging VLAN) globally.

Stag VID: Specify the service tag VID. Valid values are 1 through 4094.

CPU Stag Priority: Displays the 802.1p bit value assigned to the service tag VID of the CPU, used to prioritize different classes of traffic. The value is determined by QoS user priority settings. Please refer to Section 4.5.1 QoS Priority for more details.

Stag EtherType: Configure the service tag ethertype. (Range: 0000-FFFF, Default: 9100).

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

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

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

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

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.

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

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

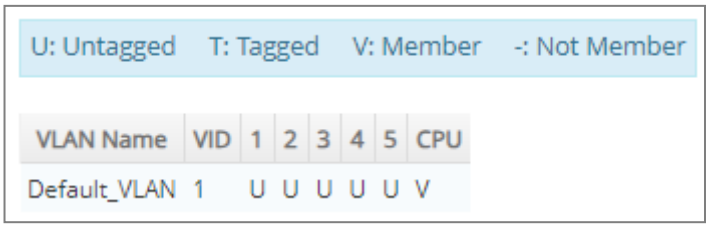
Stag Priority: Displays the 802.1p bit value assigned to the service tag VID of the specific port, used to prioritize different classes of traffic. The value is determined by the QoS user priority settings. Please refer to Section 4.5.1 QoS Priority for more details.

ISP Port: Specify interfaces as ISP ports by clicking on the checkbox of the corresponding port number.

Select: You can apply all the configurations specified in the first row of the table to each interface by clicking on the first checkbox. Or, select multiple ports to reset them to prior settings by clicking the intended ports' checkboxes and then the **Reset** button. After you are done configurating, click on the **Ok** button to have the setup in effect.

4.3.3.3 VLAN Table

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

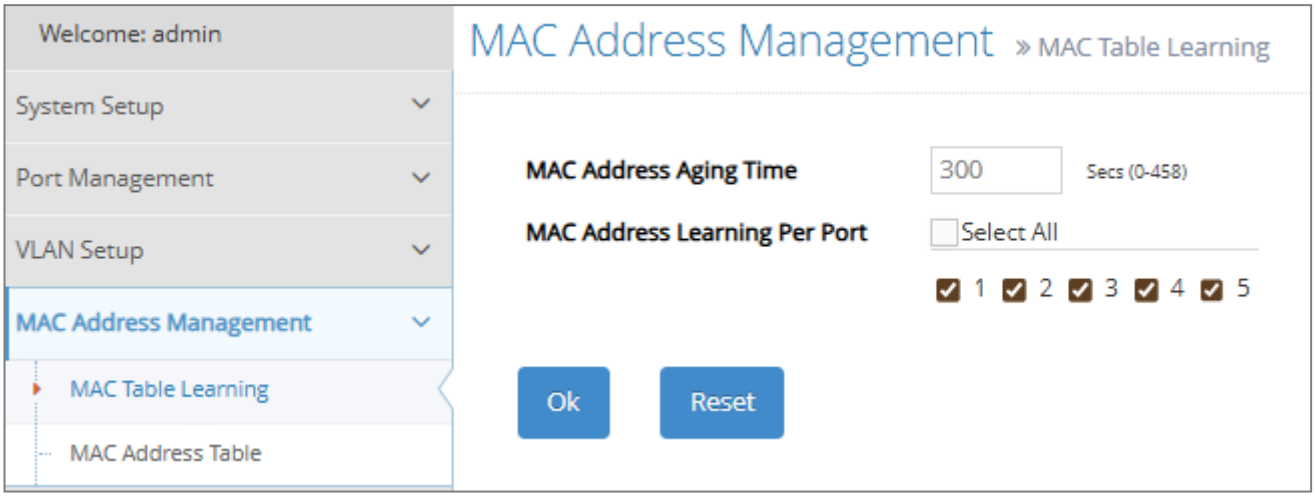


VLAN Name: View-only field that shows the VLAN name.

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

4.4 MAC Address Management

Select the folder **MAC Address Management** from the **Main Menu** and then 2 options will be displayed for your selection.

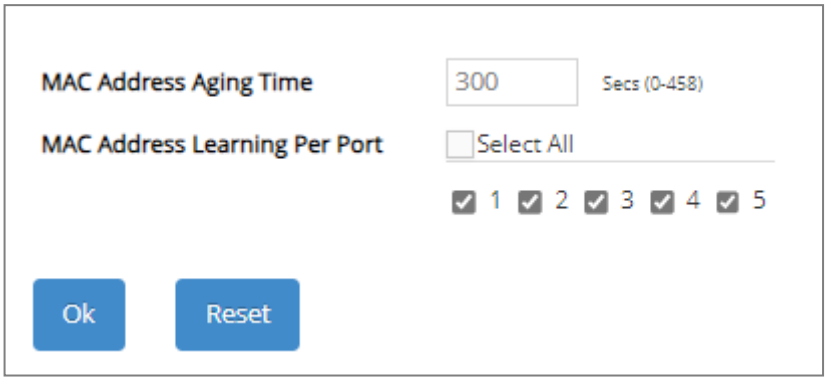


1. **MAC Table Learning:** Set up MAC address table aging time, and enable/disable MAC address learning function.

2. **MAC Address Table:** List the current MAC addresses automatically learned by the Managed Switch and the created static MAC addresses.

4.4.1 MAC Table Learning

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

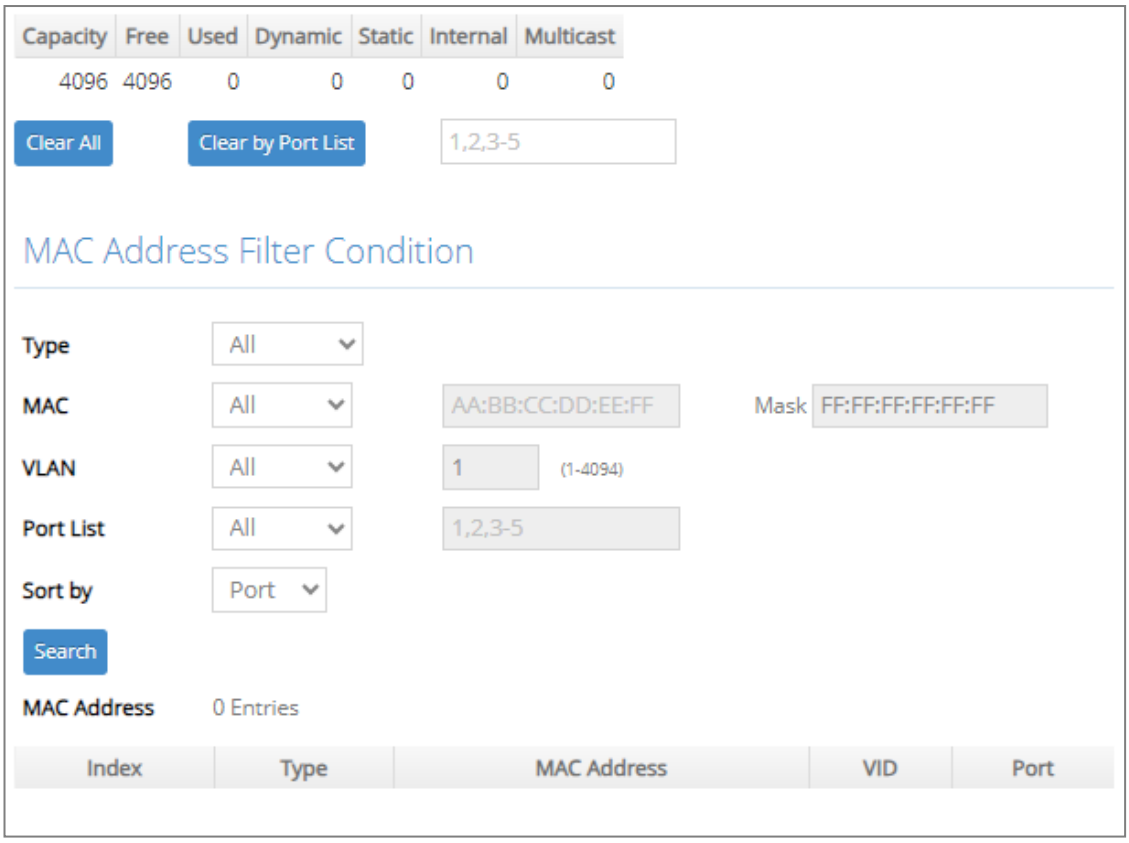


MAC Address Aging Time: Specify MAC address table aging time between 0 and 458 seconds. “0” means that MAC addresses will never age out.

MAC Address Learning Per Port: Enable port MAC address learning function on the specified ports by clicking on the checkbox of the corresponding port number. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

4.4.2 MAC Address Table

MAC Address Table displays MAC addresses learned when MAC Address Learning is enabled. Select the option **MAC Address Table** from the **MAC Address Management** menu and then the following screen page appears.



The table that sits at the very top of the webpage displays an up-to-date summary of the MAC address table down below.

1. **Capacity:** The maximum number of the MAC address entries allowed to be kept on the Managed Switch.

2. **Free:** The available number of the MAC address entries still allowed to be kept on the Managed Switch.

3. **Used:** The number of the MAC address entries already kept on the Managed Switch.

4. **Dynamic:** The number of the dynamic MAC addresses entries already kept on the Managed Switch.

5. **Static:** The number of the static MAC addresses entries already kept on the Managed Switch.

6. **Internal:** The MAC address of the Managed Switch.

7. **Multicast**: The number of the known multicast addresses entries already kept on the Managed Switch.

The table that sits at the very bottom of the page is composed of the MAC addresses that are automatically learned from each port of Managed Switch or manually created by the users. Click

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

MAC Address Filter Condition section delivers a flexible approach to investigating the MAC address table in accordance with the specified filter options, which are respectively described below to guide you through the filter setup. When you have done determining the filtering behavior, click **Search** to update the MAC address table.

1. **Type:** Select **All**, **Dynamic**, or **Static**, to specify which MAC address type to be displayed in the table.

2. **MAC:** Select **All**, **Include**, or **Exclude** to determine the filtering behavior for the MAC address comparison. It indicates how many bits, from left to right, the filter checks against the MAC address. To require an exact comparison to the full MAC address (to check all 48 bits), enter FF:FF:FF:FF:FF:FF; to check only the first 32 bits, enter FF:FF:FF:FF:00:00.

   AA:BB:CC:DD:EE:FF: Specify a MAC address to allow the filter to compare it against the specified MAC address mask.

   Mask: Specify a MAC address mask to allow the filter to compare it against the specified MAC address.

3. **VLAN:** Select **All**, **Include**, or **Exclude** to determine the filtering behavior, and specify the VLAN ID to be filtered with.

4. **Port List:** Select **All, Include**, or **Exclude** to determine the filtering behavior, and specify the port to be filtered with.

5. **Sort by:** Select **Port**, **MAC**, or **VLAN** to determine the arrangement of the MAC address entries displayed in the table. Each option is described below:

   Port: MAC addresses that are learned from the same port will be grouped together and displayed in ascending order.

   MAC: MAC addresses will be displayed in ascending order according to their digit sizes.

   VLAN: MAC addresses that belong to the same VLAN ID will be grouped together and displayed in ascending order.

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

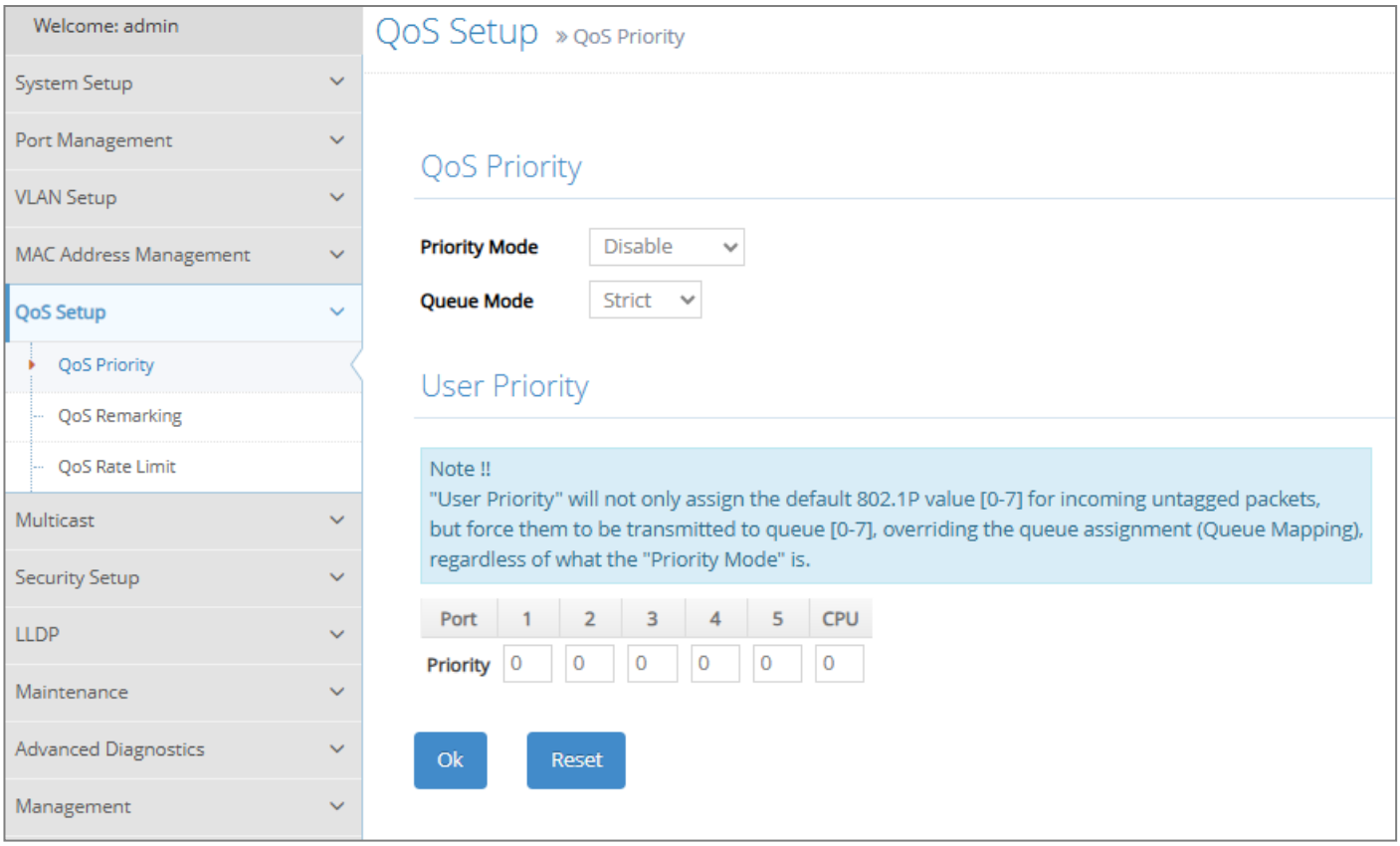
MAC Address: The total number of the MAC address entries displayed in the MAC address table according to the specified filtering options.

To view the MAC addresses that are searched, you may pull down the page list to directly go to the desired page. Or click **>**, **<**, **>>**, **<<** to move to the next/previous/last/first page of MAC address table.

4.5 QoS Setup

Network traffic is always unpredictable and the only basic assurance that can be offered is the best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria and receives preferential treatments.

QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic. To set up the priority of packets in the Managed Switch, click the folder **QoS Setup** from the **Main Menu** and then 3 options will be displayed for your selection.



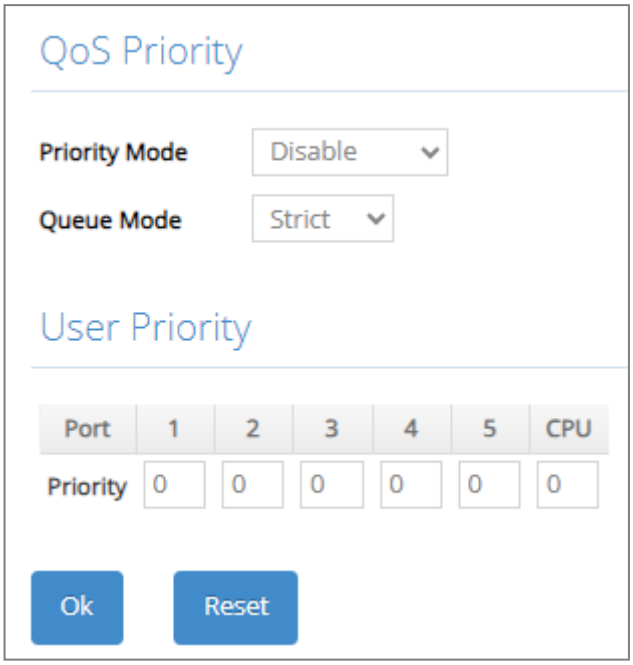
1. **QoS Priority:** To set up Priority Mode, Queuing Mode, User Priority, and so on.

2. **QoS Remarking:** To set up QoS 802.1p Remarking and DSCP Remarking.

3. **QoS Rate Limit:** To configure each port's Ingress and Egress Rate.

4.5.1 QoS Priority

Select the option **QoS Priority** from the **QoS Setup** menu and then the following screen page appears.



Priority Mode: Select the QoS priority mode of the Managed Switch.

Port Based: Port Based mode will prioritize traffic accordingly to interface priority level.

IEEE 802.1p: IEEE 802.1p mode utilizes p-bits in VLAN tag for differential service.

DSCP: DSCP mode utilizes TOS field in IPv4 header for differential service.

Disable: Disable QoS.

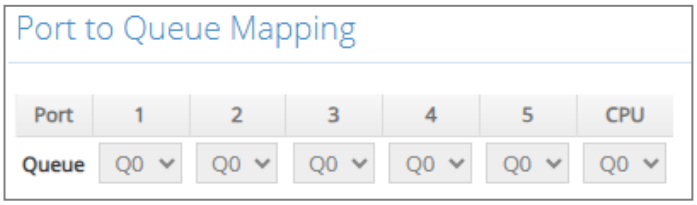
Queue Mode: Specify the queue mode as Strict or Weight.

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

Weight: Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 8, 16, 32, 64, 127 for queues 1 through 8 respectively. The following parameter will appear when Queue Mode is selected as “Weight”.

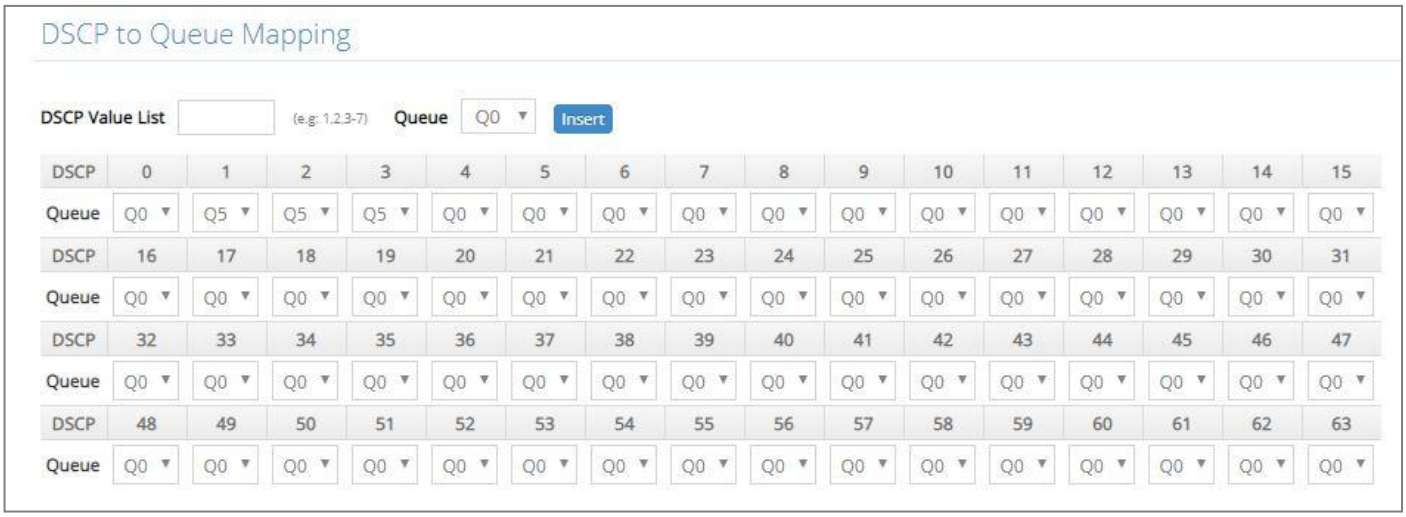
Queue Weight: Specify the Queue weight for each Queue. Valid value ranges from 1 to 127.

Port to Queue Mapping: Display the priority level for interfaces and CPU to prioritize network traffic. The value is determined by the QoS user priority settings.

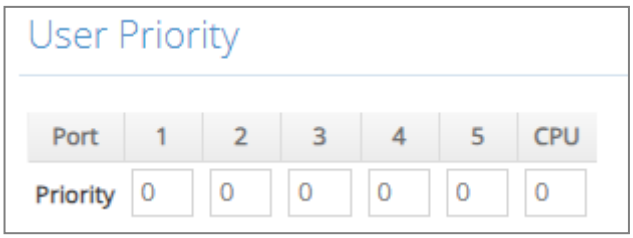


802.1p to Queue Mapping: Assign an 802.1p value (0~7) of 8 different levels to the specific queue.

DSCP to Queue Mapping: Assign a DSCP value (0~63) of 64 different levels to the specific queue by pulling down the **Queue** menu. Or directly input a range of the DSCP value (e.g.1, 2, 3-7) in the **DSCP Value List** field and specify them to the preferred queue from the **Queue** pull-down menu at a time. Then, press the **Insert** button, the specified DSCP value(s) will be assigned to this queue immediately.



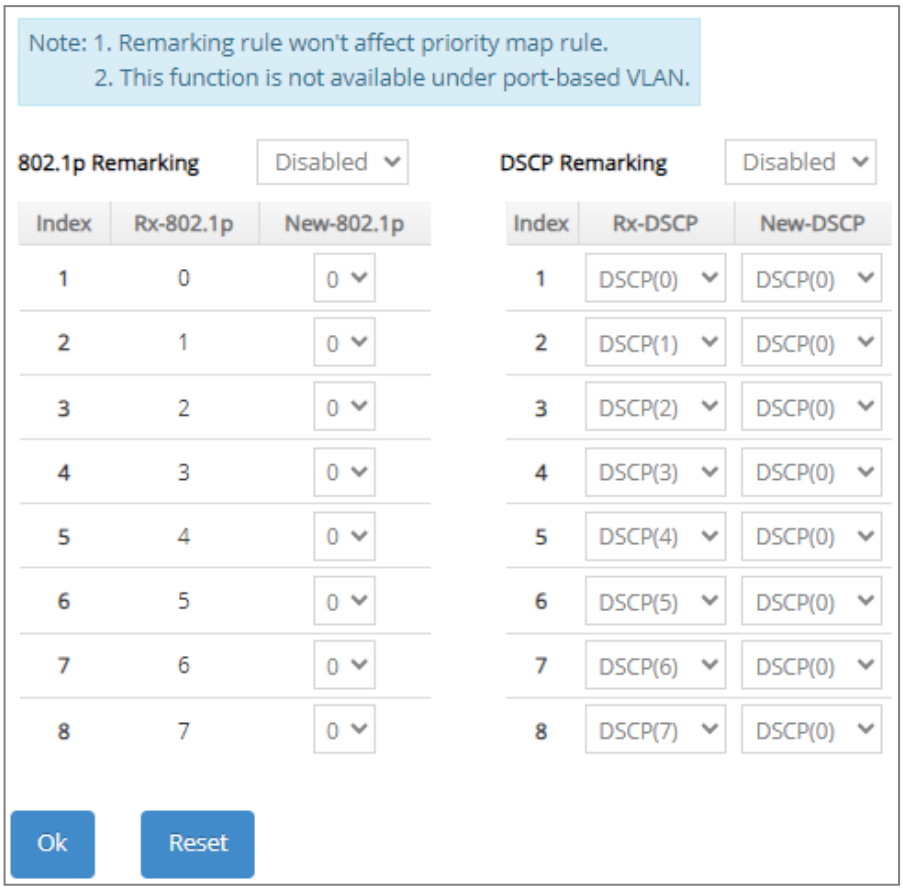
User Priority:



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

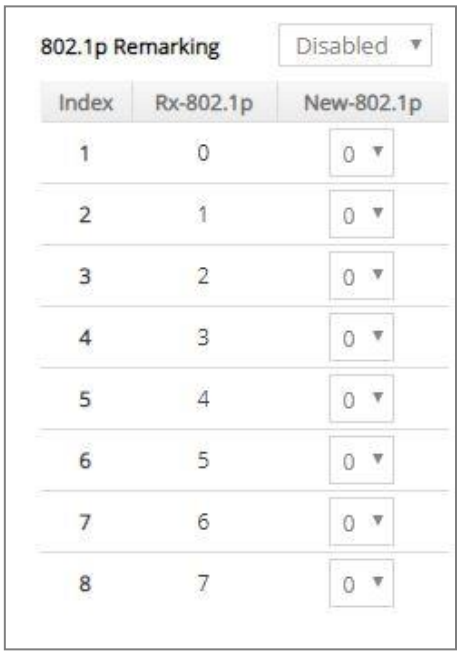
4.5.2 QoS Remarking

QoS Remarking includes 802.1p Remarking and DSCP Remarking. To configure it, select the option **QoS Remarking** from the **QoS Setup** menu and then the following screen page appears Please note that 802.1p / DSCP remarking rule will not affect the priority mapping rule.



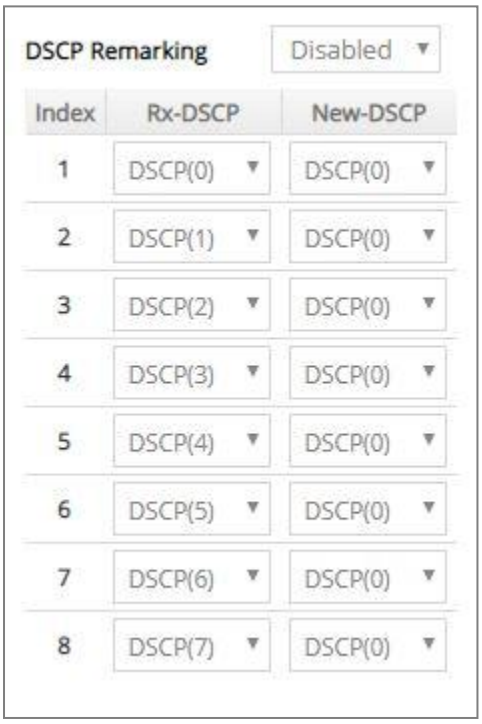
Configure 802.1p Remarking:

This allows you to enable or disable 802.1p remarking for each priority by pulling down the **802.1p Remarking** menu. The default setting is disabled.



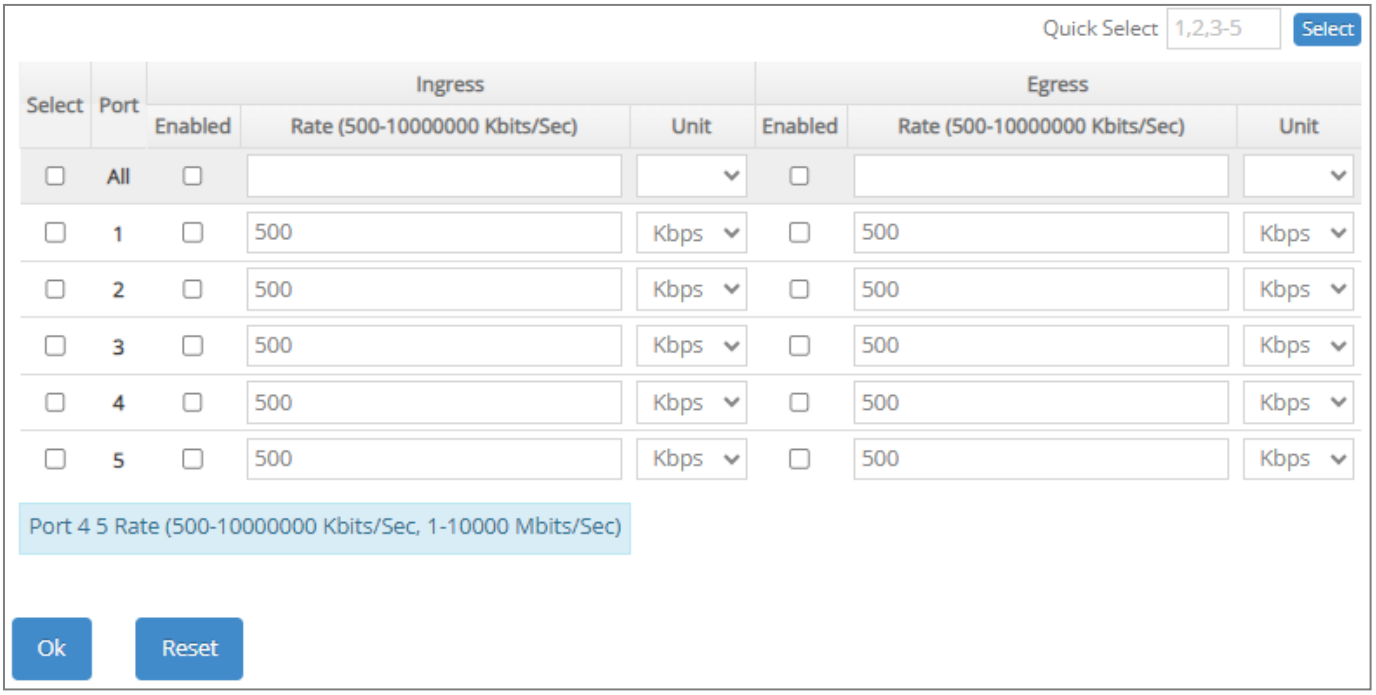
Configure DSCP Remarking:

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



4.5.3 QoS Rate Limit

Select the option **QoS Rate Limit** from the **QoS Setup** menu and then the following screen page appears. This allows users to specify each port's both inbound and outbound bandwidth. The excess traffic will be dropped.



Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. Or quickly configure the desired ports at a time, you can also directly input the port number (e.g.1, 2, 3-5) in the **Quick Select** field located at the top-right corner of the QoS Rate Limit table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Port: The number of each port.

Enabled in Ingress/Egress field**:** Enable or disable each port's QoS Rate Limit of inbound and outbound bandwidth. To enable it, just click on the checkbox of the corresponding port(s). The default setting is "unchecked", which is disabled.

Rate in Ingress/Egress field**:** Specify the transmitting rate limit of the inbound and outbound bandwidth. Valid range is from 500 ~10000000 in unit of Kbps or 1~10000 in unit of Mbps.

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

4.6 Multicast

Select the folder **Multicast** from the **Main Menu**, the **IGMP/MLD Snooping** subfolder will be displayed.

4.6.1 IGMP/MLD Snooping

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

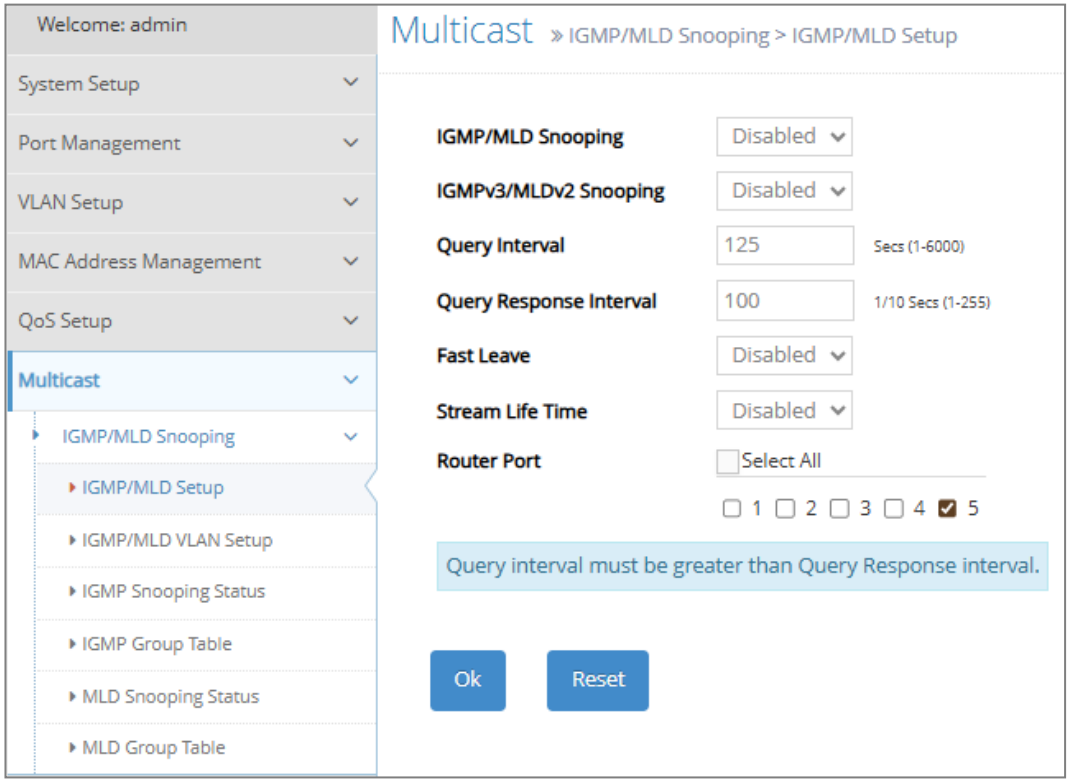
IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers by processing the layer 3 packets that IGMP packets sent in a multicast network.

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

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

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

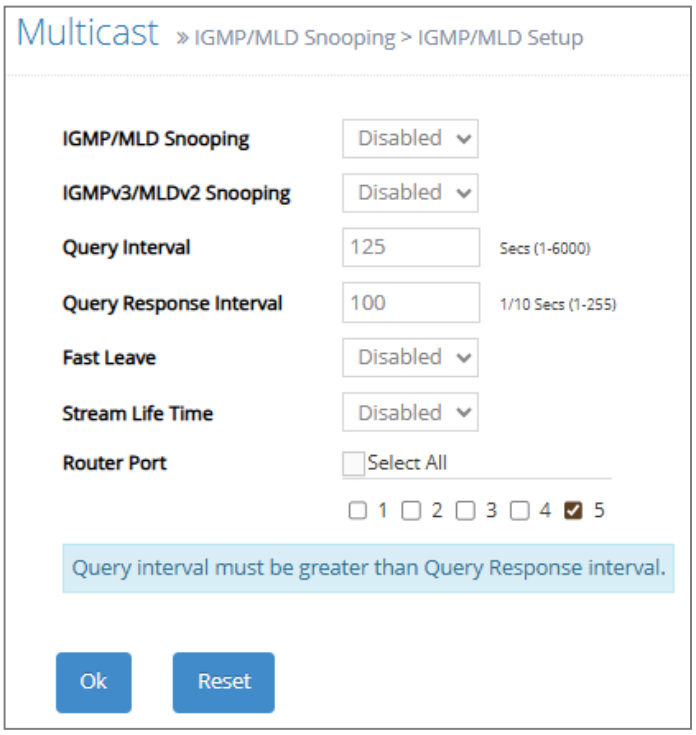
Select the subfolder **IGMP/MLD Snooping** and then 6 options will be displayed for your selection.



1. **IGMP/MLD Setup:** To enable or disable IGMP/MLD Snooping, IGMPv3/MLDv2 Snooping and set up router ports.
2. **IGMP/MLD VLAN Setup:** To set up the ability of IGMP/MLD snooping and querying with VLAN.
3. **IGMP Snooping Status:** View the IGMP snooping status.
4. **IGMP Group Table:** View the IGMP Groups table.
5. **MLD Snooping Status:** View the MLD snooping status.
6. **MLD Group Table:** View the MLD Groups table.

4.6.1.1 IGMP/MLD Setup

Select the option **IGMP/MLD Setup** from the **IGMP/MLD Snooping** menu and then the following screen page appears. Please note that Query Interval value must be greater than the value of Query Response Interval.



IGMP/MLD Snooping: When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic.

IGMPv3/MLDv2 Snooping: When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic. This is for IGMPv3 and MLDv2 only.

Query Interval: The Query Interval is used to set the time between transmitting IGMP queries, entries between 1 ~ 6000 seconds are allowed. (Default value is 125, One Unit =1 second)

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

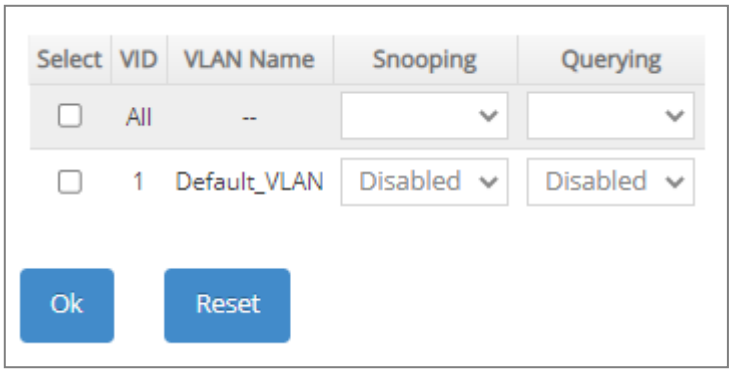
Fast Leave: The Fast Leave option may be enabled or disabled. When enabled, this allows an interface to be ignored without sending group-specific queries. The default setting is “Disabled”.

Stream Life Time: When it is enabled, the multicast traffic flow will be stopped once reaching its specified lifespan. The length of Stream Life Time is determined by the total amount of Query Interval and Query Response Interval (125 and 10 seconds in default, respectively).

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

4.6.1.2 IGMP/MLD VLAN Setup

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



VID: VID of the specific VLAN.

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

Snooping: When enabled, the port in VLAN will monitor network traffic and determine which hosts to receive the multicast traffic.

Querying: When enabled, the port in VLAN can serve as the Querier which is responsible for asking hosts whether they would like to receive multicast traffic.

4.6.1.3 IGMP Snooping Status

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

Refresh: Click **Refresh** to update the latest IGMP snooping status.

VLAN ID: VID of the specific VLAN.

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

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

Querier: The state of IGMP querier in the VLAN.

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

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

v1 Reports: The total amount of received IGMP Version 1 reports (packets).

v2 Reports: The total amount of received IGMP Version 2 reports (packets).

v3 Reports: The total amount of received IGMP Version 3 reports (packets).

v2 Leaves: The total amount of received IGMP Version 2 leaves (packets).

4.6.1.4 IGMP Group Table

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

Total Entry: The total number of entries displayed in the IGMP group table.

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

VLAN ID: VID of the specific VLAN.

Group (MAC): The multicast MAC address of IGMP querier.

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

Last Reporter: The IP address of the last interested member that sent the IGMP join/report message to join a particular multicast group.

Query Response: A countdown timer of the specified **Query Response Interval**. When the Managed Switch receives an IGMP join/report message from an interested member. It will first display “stopped” first. The Managed Switch will then access the IPTV multicast server and forward the multicast packets to the interested member. At this point, the timer will begin its countdown of the specified **Query Response Interval**.

Report Count: A counter of the received IGMP join/report message. Upon receiving, the Managed switch will reset Life Time, also a countdown timer yet of the specified Stream Life Time.

Life Time: A countdown timer of the specified Stream Life Time. Once the timer reaches zero, the multicast traffic flow will be stopped

4.6.1.5 MLD Snooping Status

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

Refresh: Click **Refresh** to update the latest MLD snooping status.

VLAN ID: VID of the specific VLAN.

Querier: The state of MLD querier in the VLAN.

Queries Transmitted: The total amount of MLD general queries transmitted will be sent to MLD hosts.

Queries Received: The total amount of received MLD general queries from MLD querier.

v1 Reports: The total amount of received MLD Version 1 reports (packets).

v2 Reports: The total amount of received MLD Version 2 reports (packets).

Done: The total amount of received MLD Version 1 done (packets).

4.6.1.6 MLD Group Table

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

Total Entry: The total number of entries displayed in the MLD group table.

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

VLAN ID: VID of the specific VLAN.

Group (MAC): The multicast MAC address of MLD querier.

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

Last Reporter: The IP address of the last interested member that sent the IGMP join/report message to join a particular multicast group.

Query Response: A countdown timer of the specified **Query Response Interval**. When the Managed Switch receives an MLD join/report message from an interested member. It will first display “stopped” first. The Managed Switch will then access the IPTV multicast server and forward the multicast packets to the interested member. At this point, the timer will begin its countdown of the specified **Query Response Interval**.

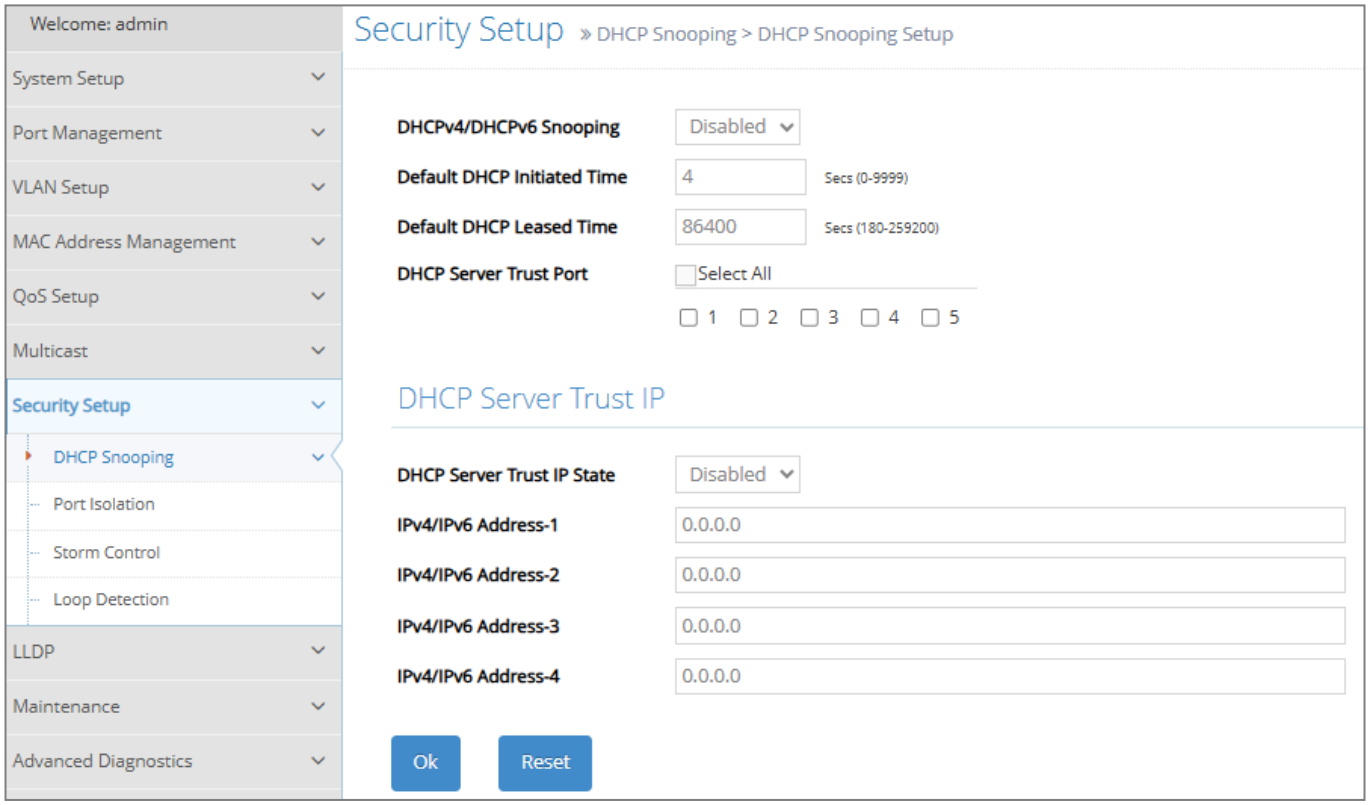
Report Count: A counter of the received MLD join/report message. Upon receiving, the Managed switch will reset Life Time, also a countdown timer yet of the specified Stream Life Time.

Life Time: A countdown timer of the specified Stream Life Time. Once the timer reaches zero, the multicast traffic flow will be stopped

4.7 Security Setup

In this section, several Layer 2 security mechanisms are provided to increase the security level of your Managed Switch. Layer 2 attacks are typically launched by or from a device that is physically connected to the network. For example, it could be a device that you trust but has been taken over by an attacker. By default, most security functions available in this Managed Switch are turned off, to prevent your network from malicious attacks, it is extremely important for you to set up appropriate security configurations. This section provides several security mechanisms to protect your network from unauthorized access to a network or redirect traffic for malicious purposes, such as Source IP Spoofing and ARP Spoofing.

Select the folder **Security Setup** from the **Main Menu** and then 4 options within this folder will be displayed



1. **DHCP Snooping:** To set up DHCP Snooping and DHCP server trust ports, enable or disable DHCP Option 82 (for DHCPv4) and Option 37 (for DHCPv6) relay agent global setting, show each port's configuration, set up suboptions such as circuit-ID and remote-ID, and view the DHCP learning table, etc.

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

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

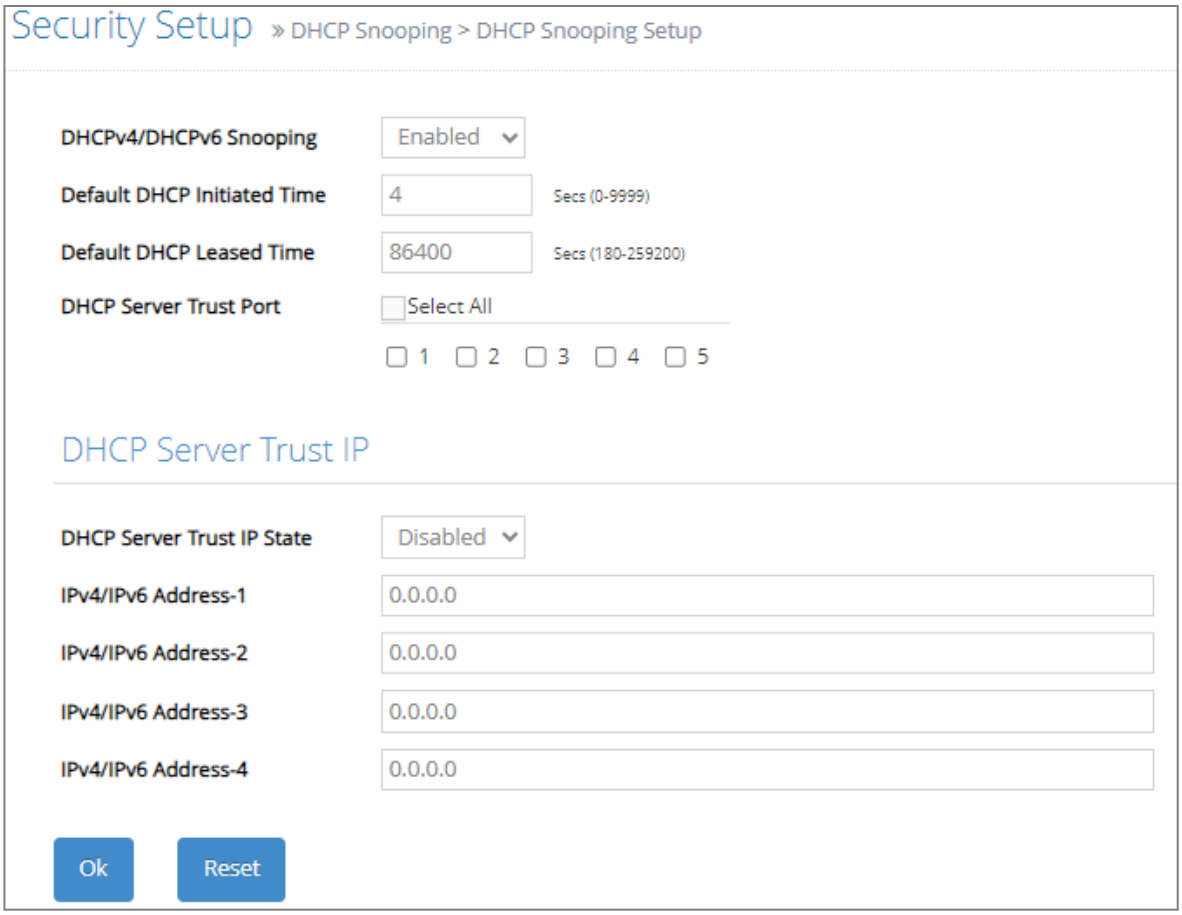
4. **Loop Detection:** Enable or disable Loop Detection function, set up Loop Detection configuration and view the Loop Detection status of each port.

4.7.1 DHCP Snooping

Select the option **DHCP Snooping** from the **Security Setup** folder and then three functions, including DHCP Snooping Setup, DHCP Option 82 / DHCPv6 Option 37 Setup and DHCP Snooping Table will be displayed for your selection.

4.7.1.1 DHCP Snooping Setup

The following screen page appears if you choose **DHCP Snooping Setup** function.



DHCPv4/DHCPv6 Snooping: Enable or disable DHCPv4/DHCPv6 Snooping function.

Default DHCP Initiated Time: Specify the time value (0~9999 Seconds) that packets might be received.

Default DHCP Leased Time: Specify packets' expired time (180~259200 Seconds).

DHCP Server Trust Port: Specify designated port(s) to be Trust Port that can give you "offer" from DHCP server. Check any port box to enable it. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

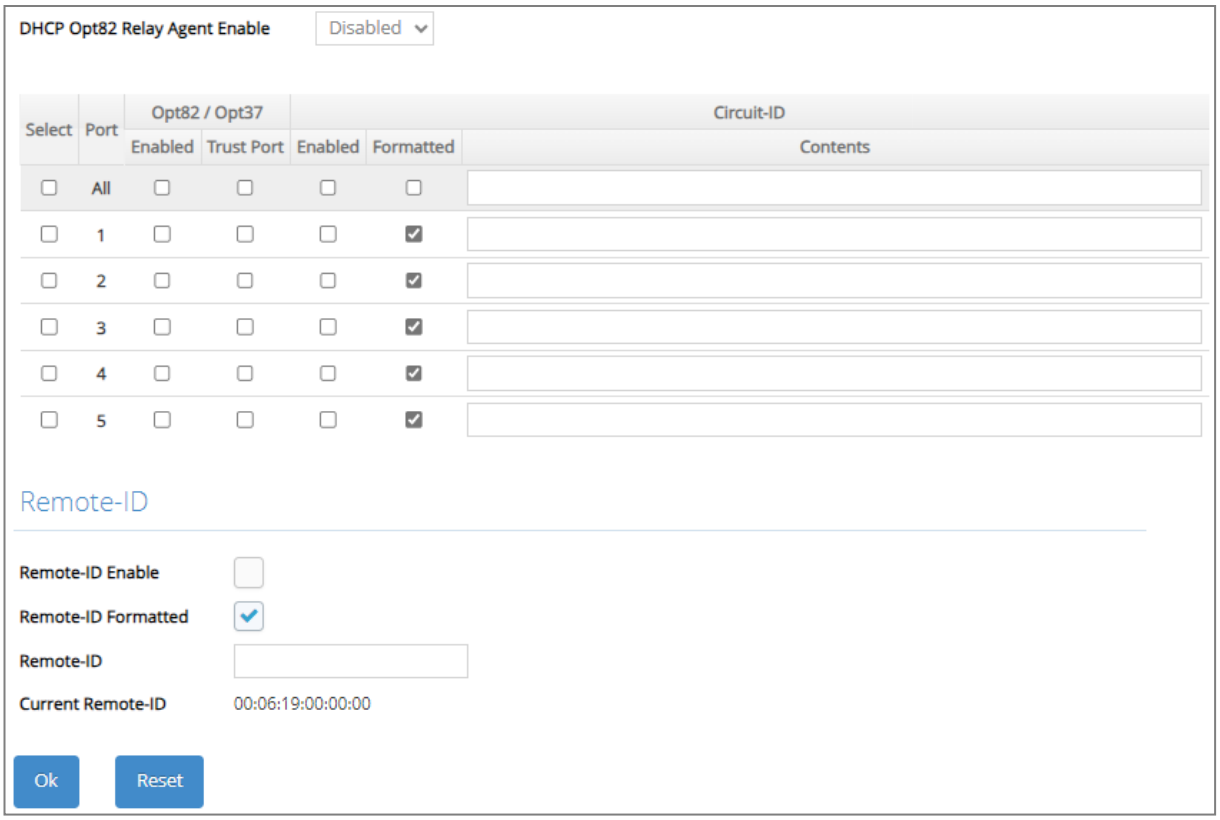
DHCP Server Trust IP State: After enabling Trust Port, you may additionally specify Trust IP address for identification of DHCP server. Click the drop-down menu and select "Enabled", then specify Trust IP address.

4.7.1.2 DHCP Option 82 / DHCPv6 Option 37 Setup

The Managed Switch can add information about the source of client DHCP requests that relay to DHCP server by adding Relay Agent Information. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. The feature of DHCP Relay Agent Information adds Agent Information field to the Option 82 field that is in the DHCP headers of client DHCP request frames.

Besides, the Managed Switch adds the option 82 information in the packet when it receives the DHCP request. In general, the switch MAC address (the remote-ID suboption) and the port identifier, vlan-mod-port or snmp-ifindex are included in the option 82 information. You can configure the remote ID and circuit ID.

The following screen page appears if you choose **DHCP Option 82 / DHCPv6 Option 37 Setup** function.



DHCP Opt82 Relay Agent Enable: To globally enable or disable DHCP Option 82 Relay Agent global setting. When enabled, Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers recognizing the Relay Agent Information option may use the Information to implement IP address or other parameter assignment policies. Switch or Router (as the DHCP relay agent) intercepting the DHCP requests, appends the circuit ID + remote ID into the option 82 fields (or Option 37 when DHCPv6) and forwards the request message to DHCP server.

Select: You can apply all the configurations specified in the first row of the table to each interface by clicking on the first checkbox. Or, select multiple ports to reset them to prior settings by clicking the intended ports' checkboxes and then the Reset button. After you are done configurating, click on the Ok button to have the setup in effect.

Port: The number of each port.

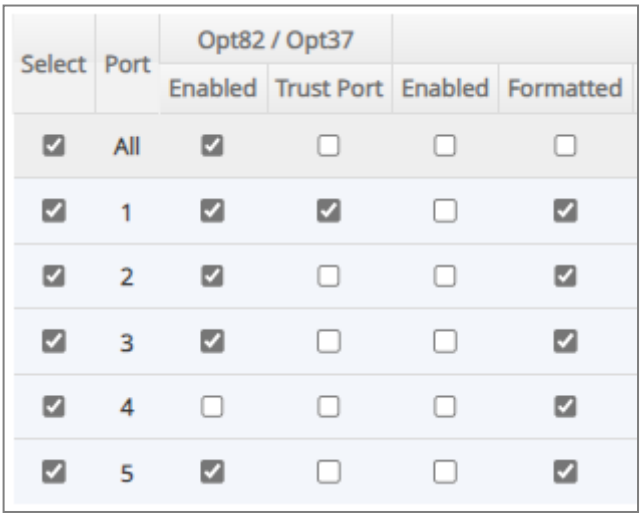
Enabled in Opt82/Opt37 field**:**

Enable (check): Add Agent information.

Disable (uncheck): Forward.

Trust Port in Opt82/Opt37 field**:** Click on the checkbox of the corresponding port number if you would like ports to become trust ports. The trusted ports will not discard DHCP messages.

For example,



Select	Port	Opt82 / Opt37			
		Enabled	Trust Port	Enabled	Formatted
☑	All	☑	☐	☐	☐
☑	1	☑	☑	☐	☑
☑	2	☑	☐	☐	☑
☑	3	☑	☐	☐	☑
☑	4	☐	☐	☐	☑
☑	5	☑	☐	☐	☑

A DHCP request is from Port 1 that is marked as both Opt82 port and trust port.

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

A DHCP request is from Port 2 that is marked as Opt82 port.

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

Circuit ID Suboption: This suboption may be added by DHCP relay agents that terminate switched or permanent circuits. It encodes an agent-local identifier of the circuit from which a DHCP client-to-server packet was received. It is intended for use by agents in relaying DHCP responses back to the proper circuit. Servers may use the circuit ID for IP and other parameter assignment policies.

Remote-ID Suboption: This suboption may be added by DHCP relay agents that terminate switched or permanent circuits and have machanisms to identify the remote host end of the circuit. DHCP servers may use this option to select parameters specific to particular users, hosts, or subscriber modems. The relay agent may use this field in addition to or instead of the Agent Circuit ID field to select the circuit on which to forward the DHCP reply.

Enabled in Circuit-ID field**:** Click on the checkbox of the corresponding port number you would like to configure with circuit ID.

Formatted in Circuit-ID field**:** Also click on the checkbox to add the circuit ID type and length of the circuit ID packet or uncheck to hide the circuit ID type and length of the circuit ID packet. The default setting is checked.

Contents in Circuit-ID field**:** Specify the VLAN and port identifier using a VLAN ID in the range of 1 to 4094. Besides, you can configure the circuit ID to be a string of up to 63 characters. The default circuit ID is the port identifier, the format of which is vlan-mod-port.

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

Remote-ID Formatted: Click on the checkbox to add the Remote ID type and length of the Remote ID packet or uncheck to hide the Remote ID type and length of the Remote ID packet. The default setting is checked.

Remote-ID: You can configure the remote ID to be a string of up to 63 characters. The default remote ID is the switch's MAC address.

Current Remote-ID: Display the current remote ID of the switch.

4.7.1.3 DHCP Snooping Table

DHCP Snooping Table displays the Managed Switch's DHCP Snooping table. The following screen page appears if you choose **DHCP Snooping Table** function.

Refresh: Click **Refresh** to update the DHCP snooping table.

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

Port of Server: View-only field that shows the port where the IP addrsss is obtained from

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

IP Address of Client: View-only field that shows the client IP address.

IP Address of Server: View-only field that shows the DHCP server IP address.

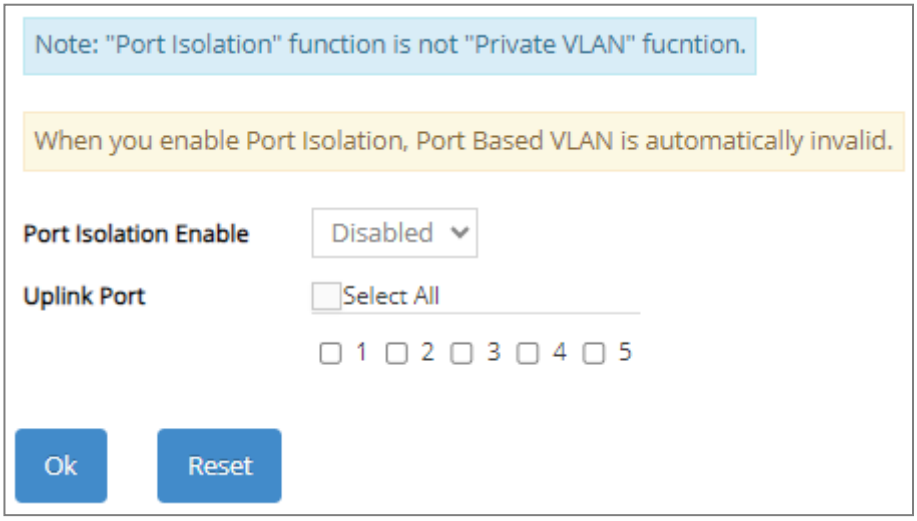
Client MAC Address: View-only field that shows the client MAC address.

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

4.7.2 Port Isolation

This is used to set up port's communication availability that they can only communicate with a given "uplink". Please note that if the port isolation function is enabled, the Port-based VLAN will be invaild automatically. Also note that "Port Isolation" function is not "Private VLAN" fucntion.

Select the option **Port Isolation** from the **Security Setup** menu and then the following screen page appears.



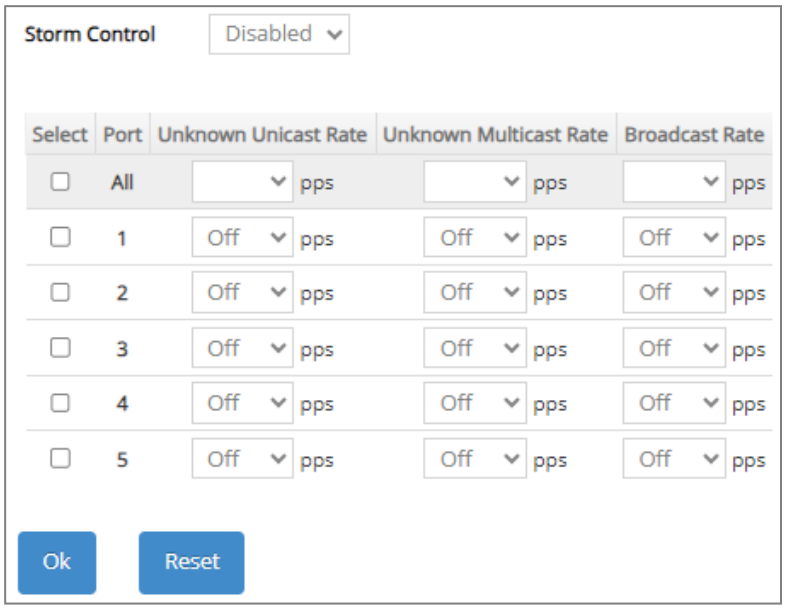
Port Isolation Enable: Enable or disable port isolation function. If port isolation is set to enabled, the ports cannot communicate with each other.

Uplink Port: By clicking on the checkbox of the corresponding port number to select the ports as uplinks that are allowed to communicate with other ports of the Managed Switch. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

4.7.3 Storm Control

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

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



Storm Control: Enable or disable the storm control function globally.

Select: You can apply all the configurations specified in the first row of the table to each interface by clicking on the first checkbox. Or, select multiple ports to reset them to prior settings by clicking the intended ports' checkboxes and then the **Reset** button. After you are done configurating, click on the **Ok** button to have the setup in effect.

Port: The number of the port.

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

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

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

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

4.7.4 Loop Detection

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

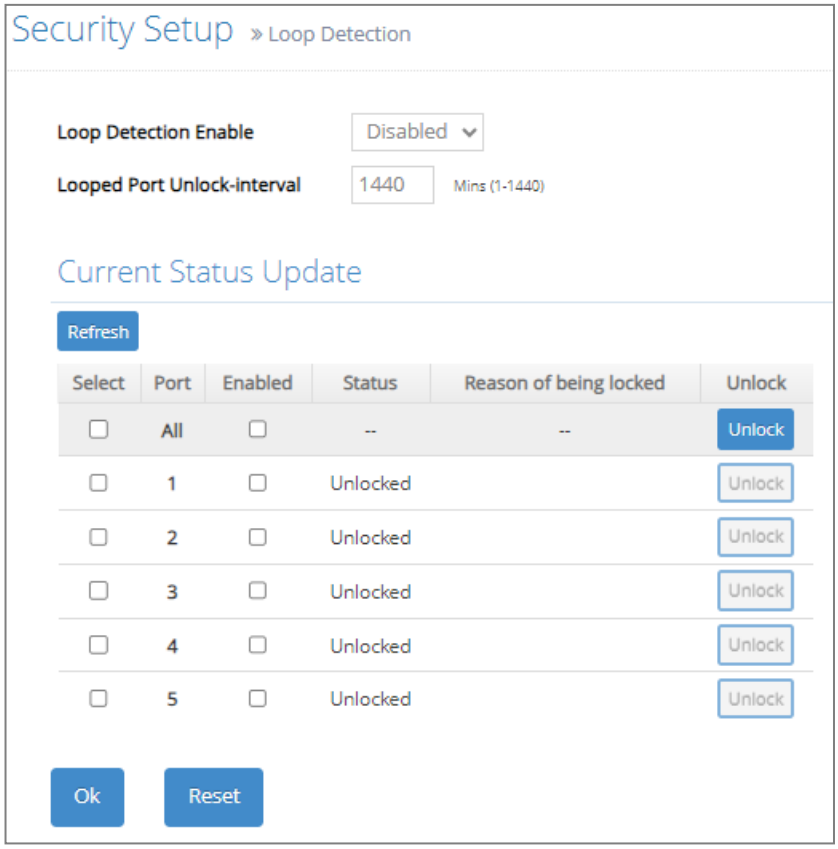
After a proper setting of Loop Detection function, the system detects loop condition by periodically sending loop detection packet. Once the system receives the loop detection packet from itself, it is claimed that it detects loop condition. Then, the system takes the following actions:

1. It blocks the relevant port to prevent broadcast storms, and send out SNMP trap to inform the network administrator. In other words, the system stops forwarding all the traffic via the looped port. However, the system will process the Loop Detection, RSTP and LLDP packets received on the looped port.
2. It slowly blinks the LED of looped port in orange.
3. It periodically sends loop detection packet to detect the existence of loop condition.

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

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

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



Loop Detection Enable: Click the pull-down menu to enabled or disabled the Loop Detection function on a system basis. The default setting is disabled.

Looped Port Unlock-interval: This is the time interval for the system to detect the existence of loop condition. System unlocks the looped port after the configured unlock-interval has elapsed. The unlock-interval can be set between 1 and 1440 minutes. The default setting is 1440 minutes.

Refresh: Click **Refresh** to update the Loop Detection status.

Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards. The new settings configured in the row of **All** port will be applied to these checked ports.

Port: The number of each port.

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

Reason of being locked: View-only field that shows the cause why the port is locked.

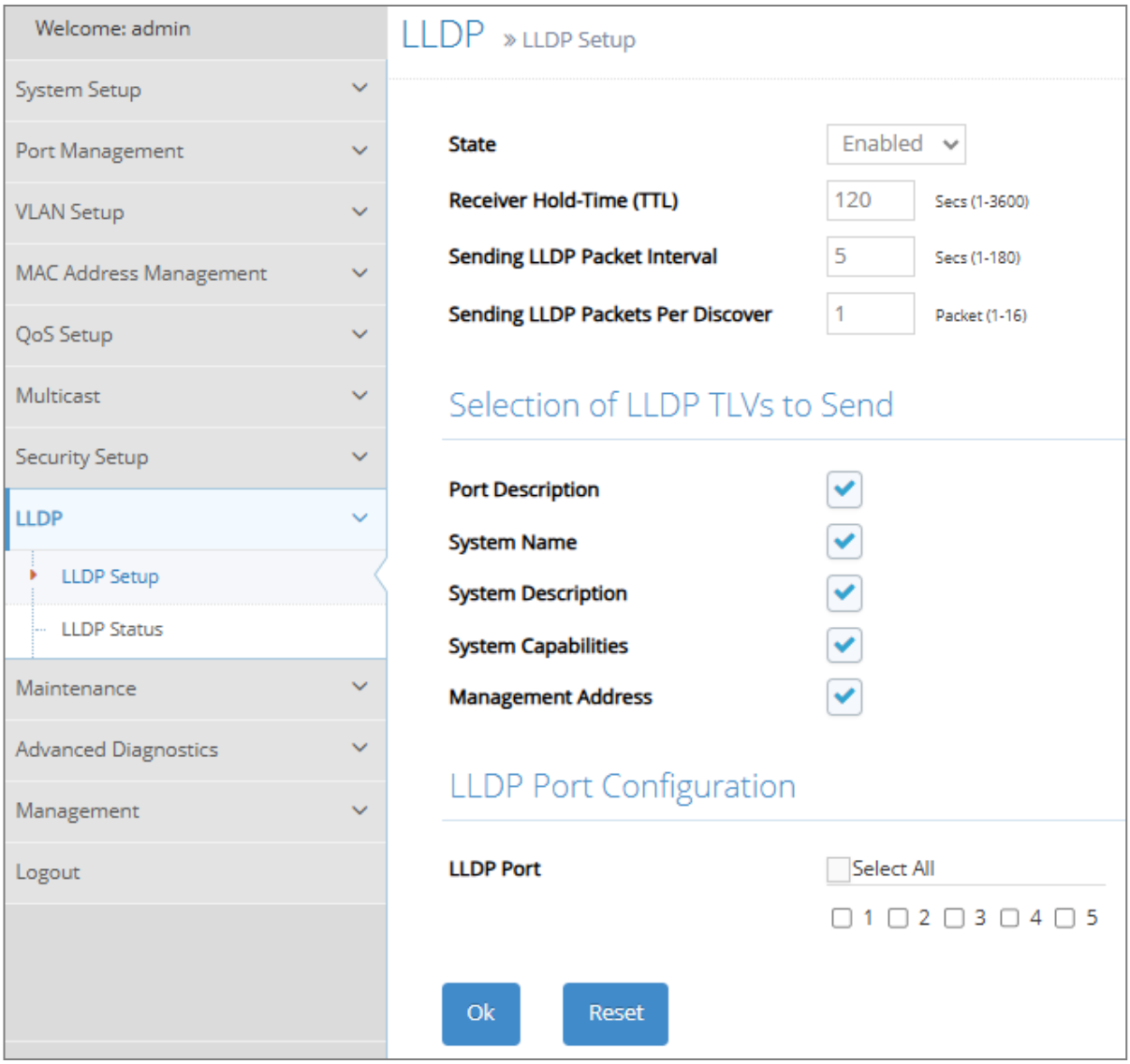
Unlock: Press the **Unlock** button to unlock the specific port if this port is locked.

Click the “**Ok**” button to apply the settings, or click the “**Reset**” button to revert to the settings saved last time.

4.8 LLDP

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

Select the folder **LLDP** from the **Main Menu** and then 2 options within this folder will be displayed as follows.

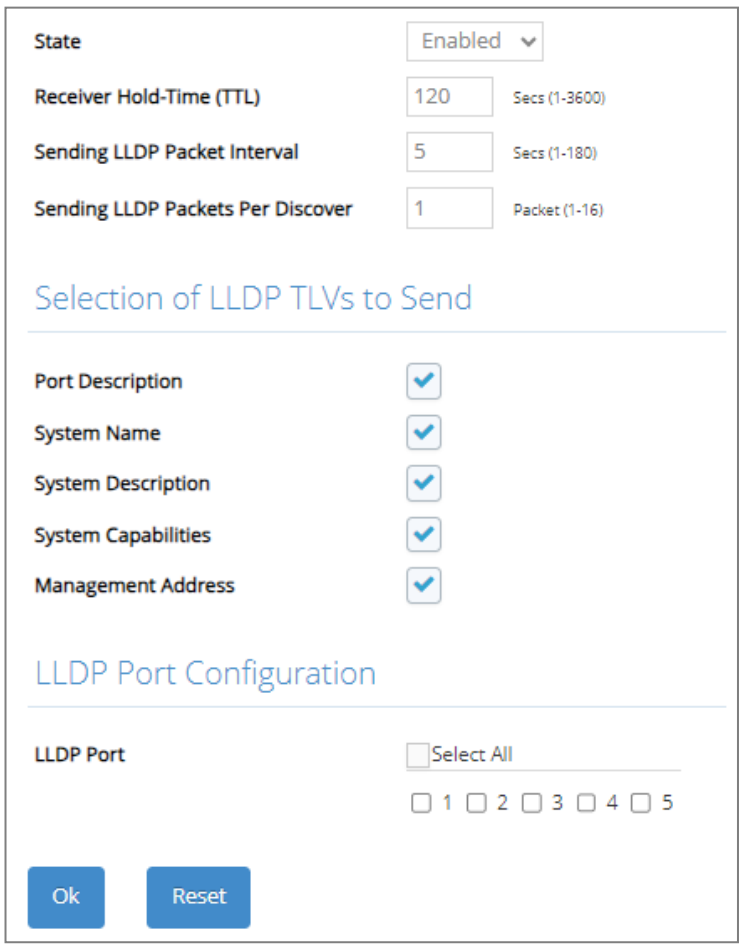


1. **LLDP Setup:** Enable or disable LLDP on ports and set up LLDP-related attributes.

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

4.8.1 LLDP Setup

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



State: Globally enable or disable LLDP function.

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

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

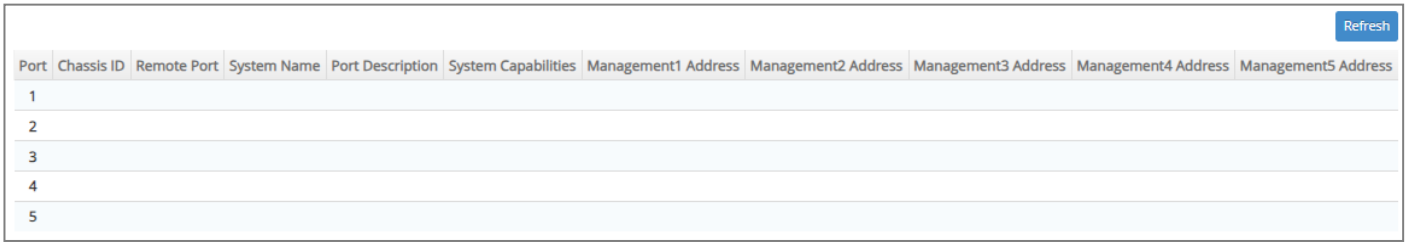
Sending LLDP Packets Per Discover: Enter the amount of packets sent in each discover.

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

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

4.8.2 LLDP Status

Click the option **LLDP Status** from the **LLDP** menu and then the following screen page appears.



Refresh: Click **Refresh** to update the LLDP Status table.

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

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

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

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

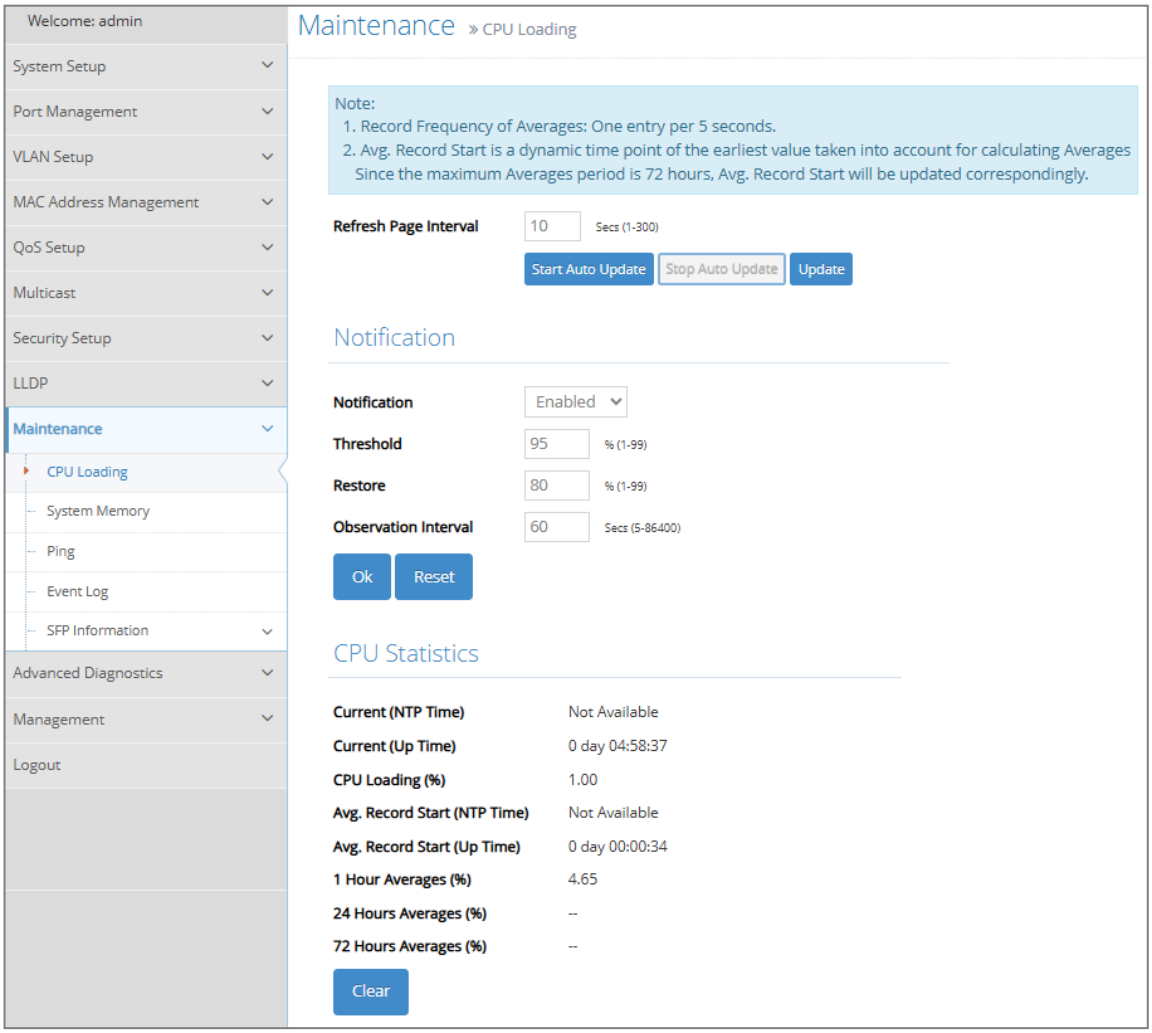
Port Description: View-only field that shows the port description of the remote port.

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

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

4.9 Maintenance

Maintenance allows users to monitor the real-time operation status of the Managed Switch for maintenance or diagnostic purposes and easily operate and maintain the system. Select the folder **Maintenance** from the **Main Menu** and then 5 options within this folder will be displayed for your selection.



1. **CPU Loading:** Manually or automatically update the current loading of CPU as well as the CPU loading record, and configure the CPU loading alarm notification.

2. **System Memory:** Manually or automatically update statistics of Memory and view them.

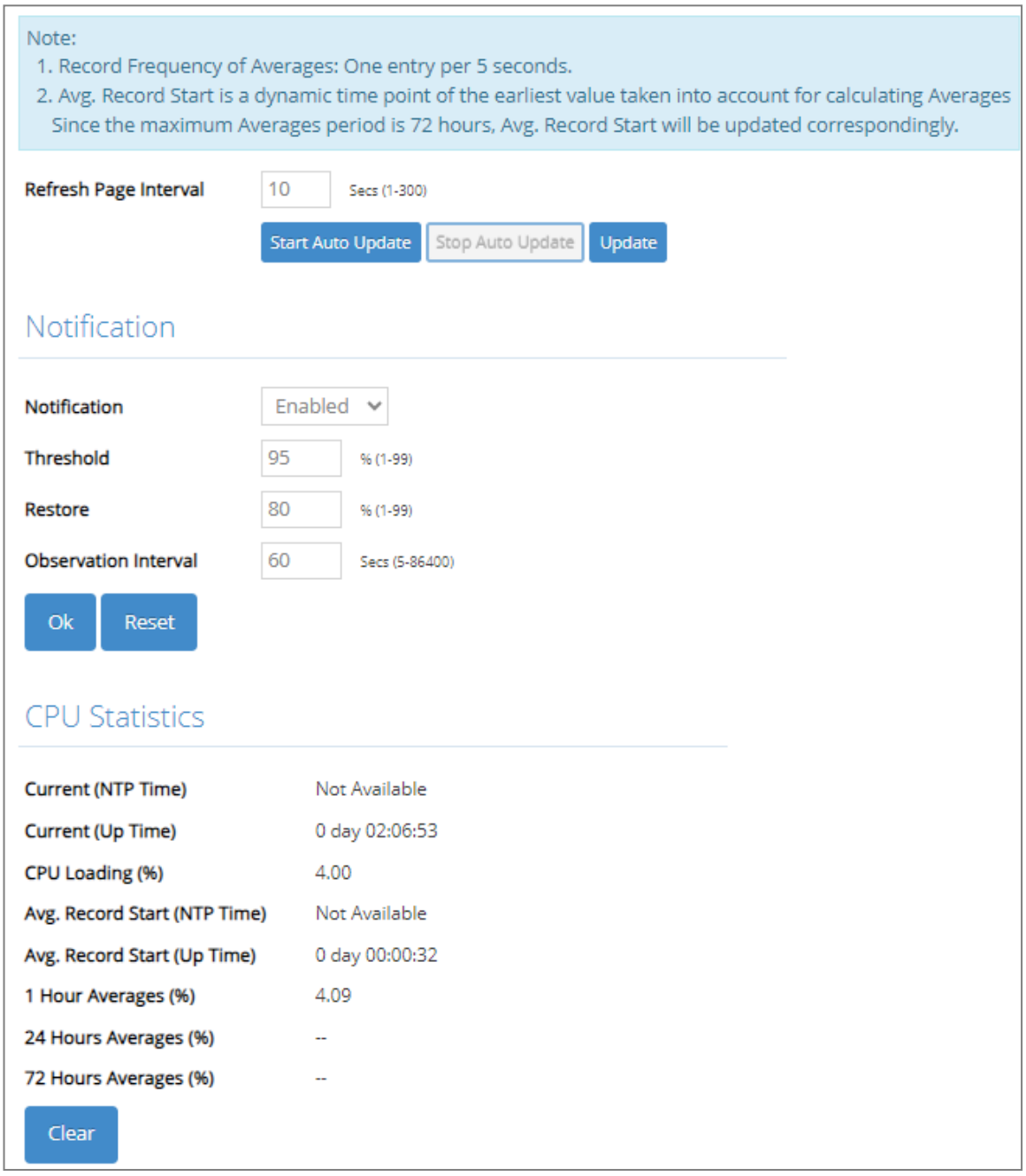
3. **Ping:** Ping can help you test the network connectivity between the Managed Switch and the host. You can also specify the counts and size of Ping packets.

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

5. **SFP Information:** View the current port's SFP information, e.g. speed, Vendor ID, Vendor S/N, etc. SFP port state shows current DMI (Diagnostic monitoring interface) temperature, voltage, TX Bias, etc.

4.9.1 CPU Loading

CPU Loading is to manually or automatically update the current loading of CPU as well as the CPU loading record, and configure the CPU loading alarm notification.
Select the option **CPU Loading** from the **Maintenance** menu and then the following screen page appears.



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

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

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

Update: Click **Update** to refresh the latest statistics of CPU loading at a time.

Notification: Enable or disable the CPU loading alarm notification.

Threshold: Specify a value for the CPU loading alarm threshold. Valid range: 1-99 (percentage).

Restore: Specify a value for the CPU loading restore threshold. Valid range: 1-99 (percentage). The Restore threshold value should be lower than the value entered in **Threshold** column.

Observation Interval: Specify a value for **Threshold** and **Restore** Observation Interval time in seconds. Valid range: 5-86400 (seconds)

NOTE: When the alarm notification is enabled,

1. *If the CPU loading (%) exceeds the threshold and persists for the assigned Observation Interval (seconds), the system will send a trap.*
2. *Once the CPU loading percentage has exceeded the threshold and a trap has been sent, if it then falls below the CPU loading Restore threshold and persists for the assigned Observation Interval (seconds), the system will send another trap.*

Current (NTP Time): Display the current NTP time.

Current (Up Time): Display the current up time.

CPU Loading (%): The percentage of current CPU loading of the system.

Avg. Record Start (NTP Time): Displays the NTP Time when the recording of the average CPU loading percentage begins.

Avg. Record Start (Up Time): Displays the Up Time when the recording of the average CPU loading percentage begins.

NOTE: *The following three items can be indicative of whether there is an unusual spike in the number of threads, thereby allowing an administrator to monitor the average system load over the past 1/24/72 hour(s).*

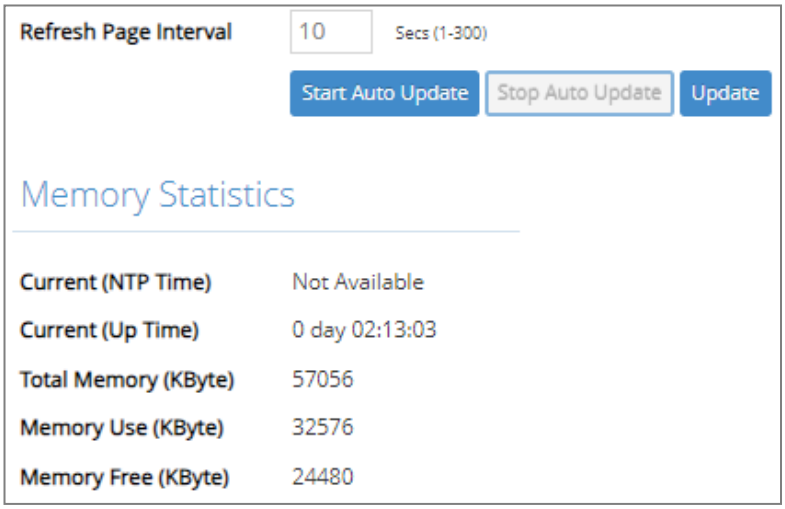
---

1 Hour Averages (%): The average of CPU loading for the past 1 hour.

24 Hours Averages (%): The average of CPU loading for the past 24 hours.

72 Hours Averages (%): The average of CPU loading for the past 72 hours.

4.9.2 System Memory



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

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

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

Update: Click **Update** to refresh the latest statistics of Memory at a time.

Current (NTP Time): Display the current NTP time.

Current (Up Time): Display the current up time.

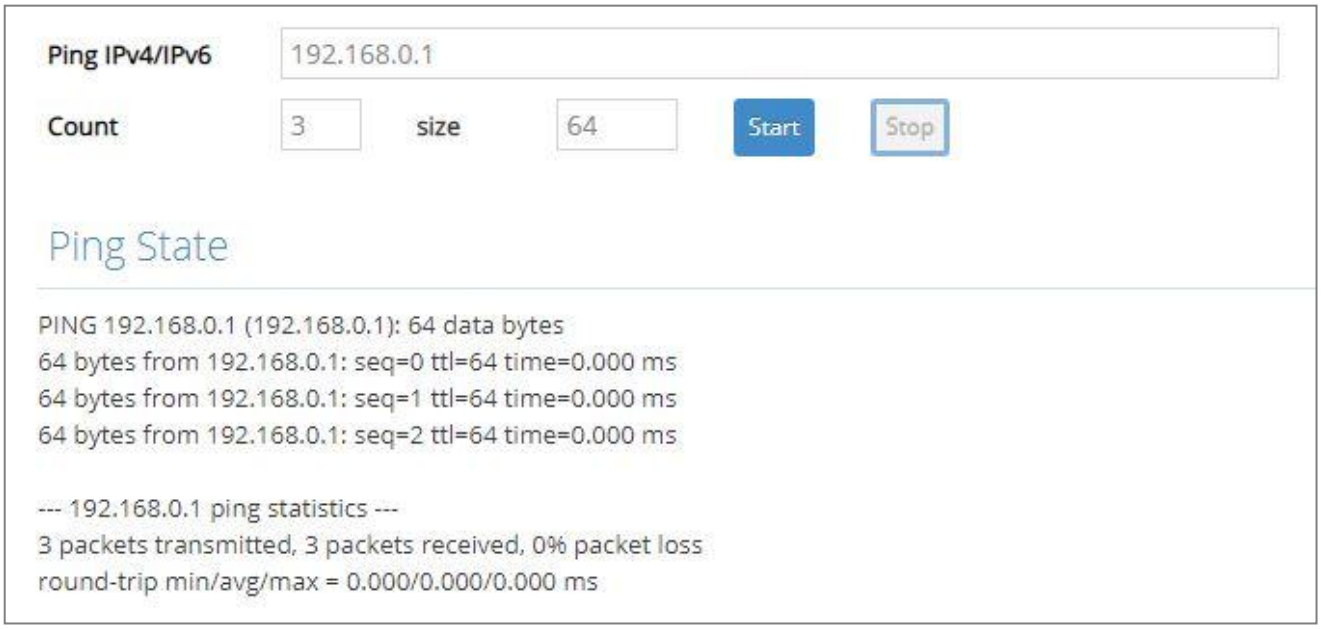
Total Memory (KByte): It shows the entire memory in kilobytes.

Memory Use (KByte): The memory in kilobytes that is in use.

Memory Free (KByte): The memory in kilobytes that is idle.

4.9.3 Ping

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

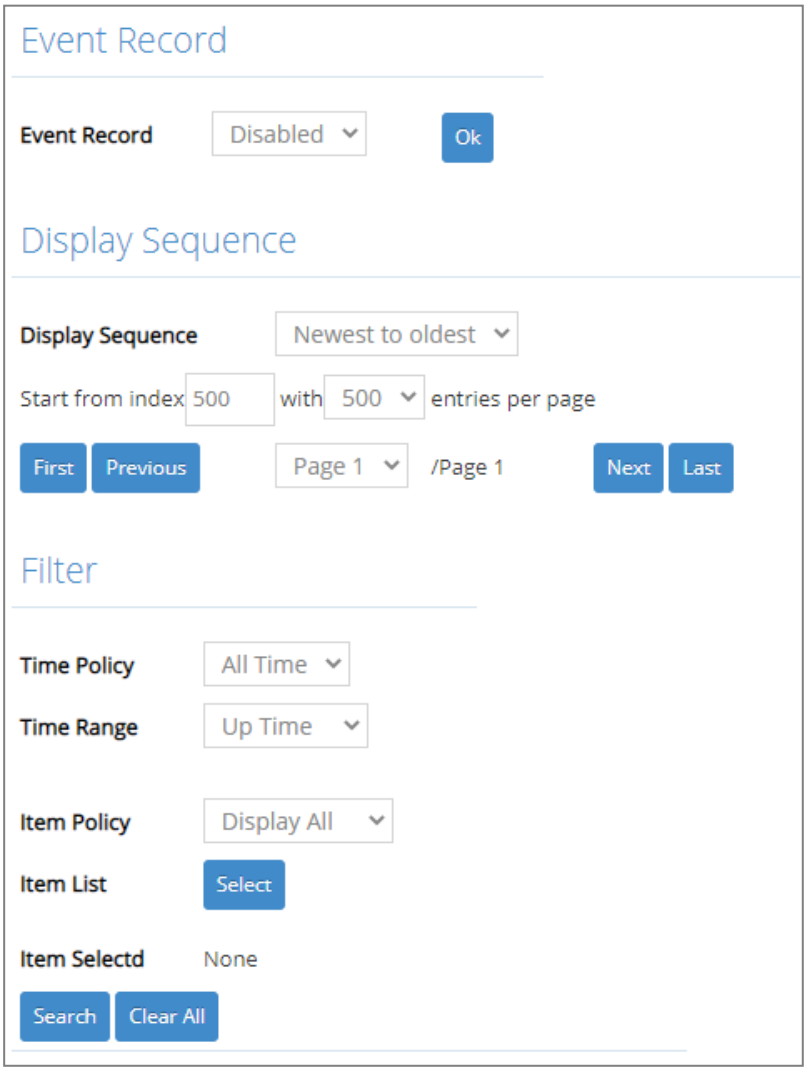


Enter the IPv4/IPv6 address of the host you would like to ping. You can also specify the count and size of the Ping packets. Click **Start** to start the Ping process or **Stop** to pause this Ping process.

4.9.4 Event Log

Event log keeps a record of switch-related information. A network manager can investigate the information captured in the Event Log and therefore analyze the network traffic, usage, and security.

Select the option **Event Log** from the **Maintenance** menu and then the following screen page appears.



Event Record: Configure the Event Record function. Once it's **enabled**, the Managed Switch will fully preserve the entire event log after reboot, while the Managed Switch will erase the entire event log if Event Record is **disabled**. Click **OK** when you have finished the configuration.

Display Sequence: Configure the display sequence of the event log table.

1. Select **Newest to oldest** or **Oldest to newest** to specify the arrangement of the event log display.

2. Set **Start from index** as a particular event index. Any event of which the index is smaller than the specified index will not be displayed if you specify the arrangement of **Oldest to newest**; any event of which the index is bigger than the specified index will not be displayed if you specify the arrangement of **Newest to oldest.**

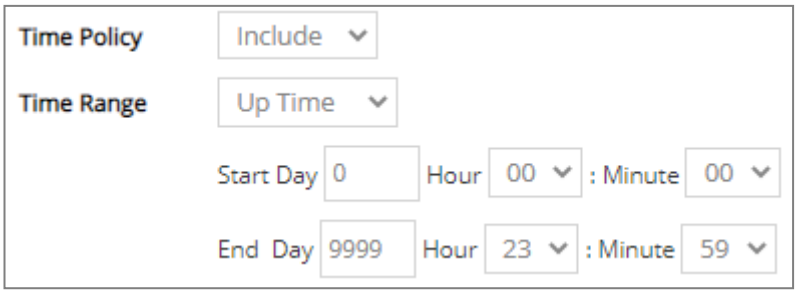
3. Click the pull-down menu of **entries per page** to select the maximum number of event entries displayed on each page.

Click **First**, **Last** or select the intended page from the pull-down menu of **Page** to achieve page jumps; click **Previous** or **Next** to maneuver the display of the event log table.

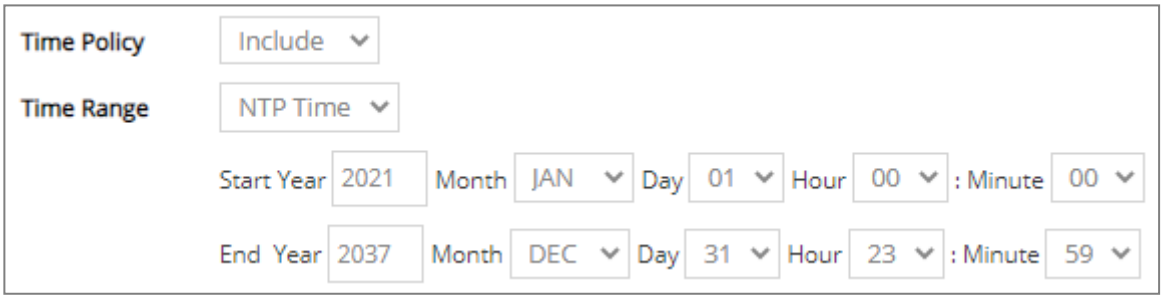
Filter: Configure each filter setting to customize the display of the event log table.

1. **Time Policy:** Select **All Time**, **Exclude**, or **Include** to determine the filtering behavior.

2. **Time Range:** Select **Up Time** or **NTP Time** to filter the events according to the Managed Switch's uptime or NTP time.



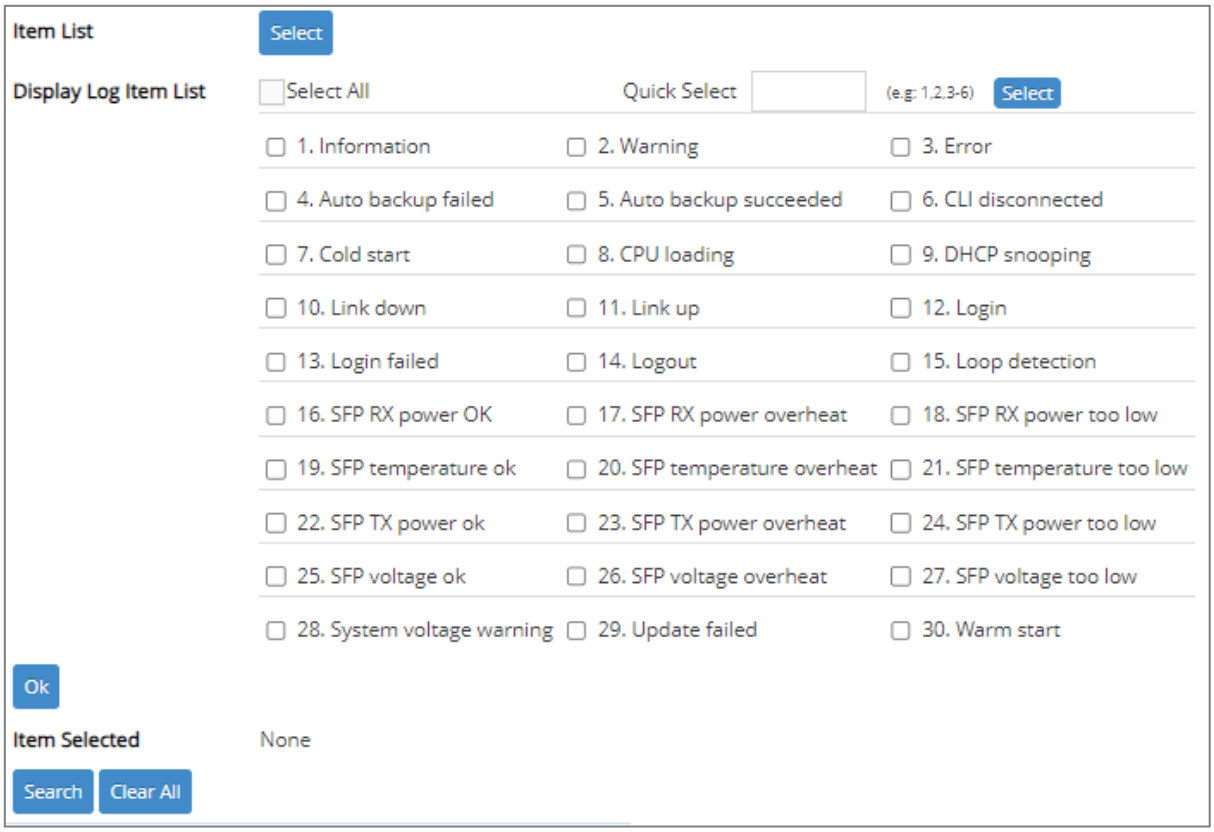
Start/End Day Hour Minute: When **Time Policy** is selected as **Exclude** or **Include**, specify the time period in which the intended events occurred according to the Managed Switch's uptime.



Start/End Year Month Day Hour Minute: When **Time Policy** is selected as **Exclude** or **Include**, specify the time period in which intended events occurred according to NTP time.

3. **Item Policy:** Select **Display All**, **Exclude Log**, or **Include Log** to determine the behavior of the event category filtering.

4. **Item List:** Click **Select** to specify certain/all event categories from the collapsible section to enable event filtering.



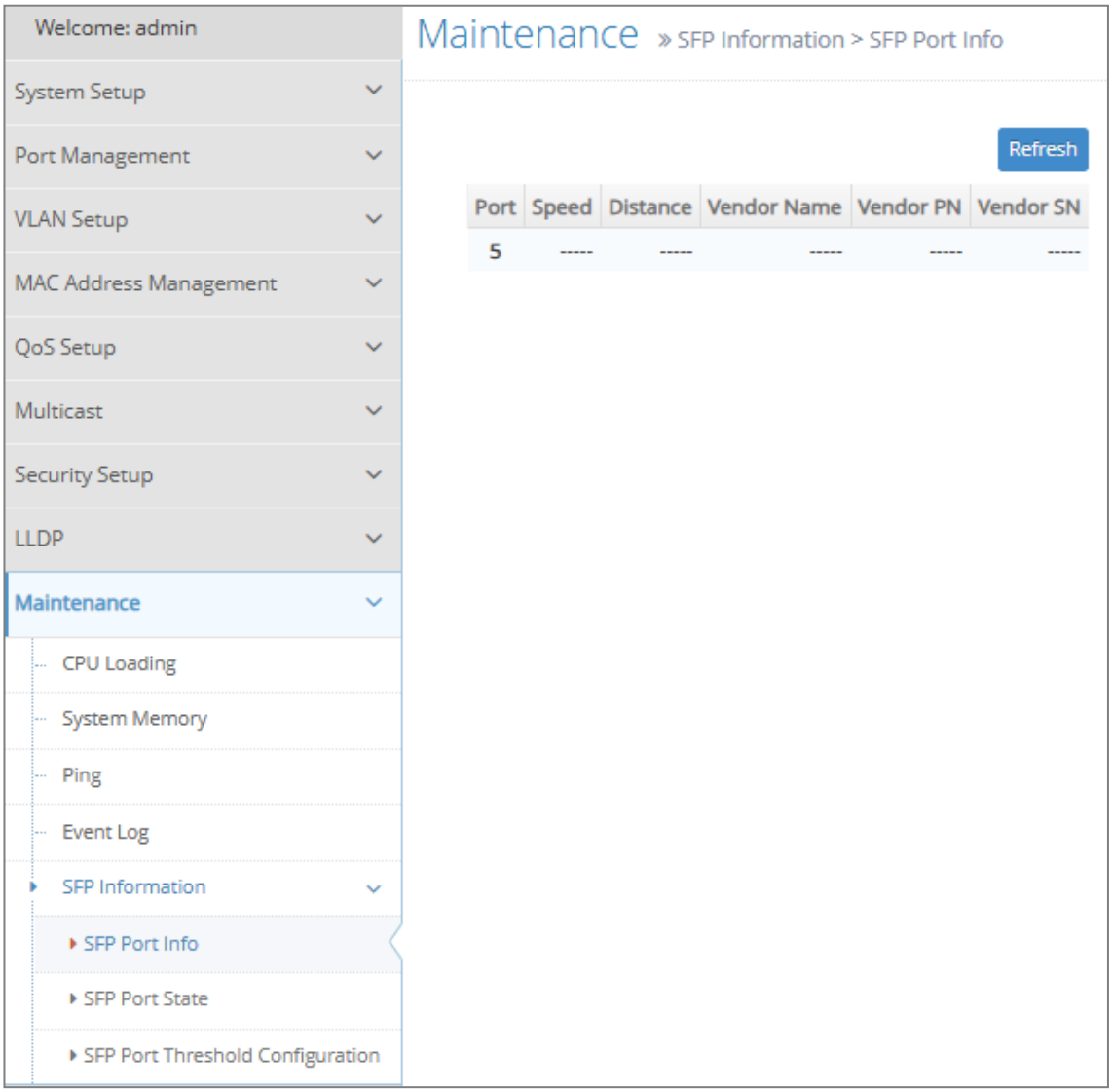
5. **Display Log Item List**: Click each checkbox of one particular event category to select the intended event categories. Or quickly configure the desired event categories at a time by directly inputting the item number (e.g.1, 2, 3-7) in the **Quick Select** field located at the top-right corner of the **Display Log Item List** table. The specified event categories will be checked immediately once you click the **Select** button next to the **Quick Select** field. Click **Ok** to finish the selection.

6. **Item Selected:** Display the event category you select from the **Item List**; display “none“ when no event category is selected.

Click **Search** to update the event log table sitting at the bottom of the webpage when you are done configuring the filtering settings; Click **Clear All** to clear the record of all event logs.

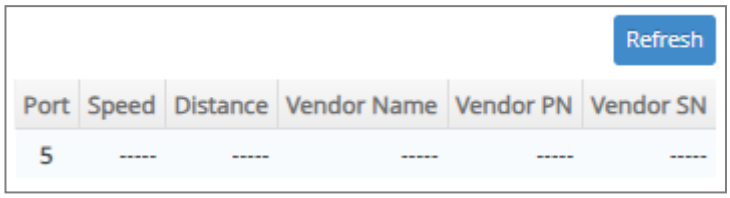
4.9.5 SFP Information

Select the option **SFP Information** from the **Maintenance** menu and then three functions, including **SFP Port Info**, **SFP Port State**, and **SFP Port Threshold Configuration** within this subfolder will be displayed.



4.9.4.1 SFP Port Info

SFP Info displays transceiver information e.g. the speed of transmission, the distance of transmission, vendor Name, vendor PN, vendor SN, etc. The following screen page appears if you choose **SFP Port Info** function.



Refresh: Click **Refresh** to update the transceiver port Info status.

Port: The port number of the transceiver module.

Speed: Data rate of the transceiver port.

Distance: Transmission distance of the transceiver port.

Vendor Name: Vendor name of the transceiver.

Vendor PN: Vendor PN of the transceiver.

Vendor SN: Vendor SN of the transceiver.

4.9.4.2 SFP Port State

SFP Port State displays transceiver information e.g. the currently detected temperature, voltage, TX Bias, etc. The following screen page appears if you choose **Transceiver State** function.

Refresh: Click **Refresh** to update the transceiver state status.

Port: The port number of the transceiver.

Temperature (Degree C): The operation temperature of the transceiver currently detected.

Voltage (V): The operation voltage of the transceiver currently detected.

TX Bias (mA): The operation current of the transceiver currently detected.

TX Power (dBm): The optical transmission power of the transceiver currently detected.

RX Power (dBm): The optical receiving power of the transceiver currently detected.

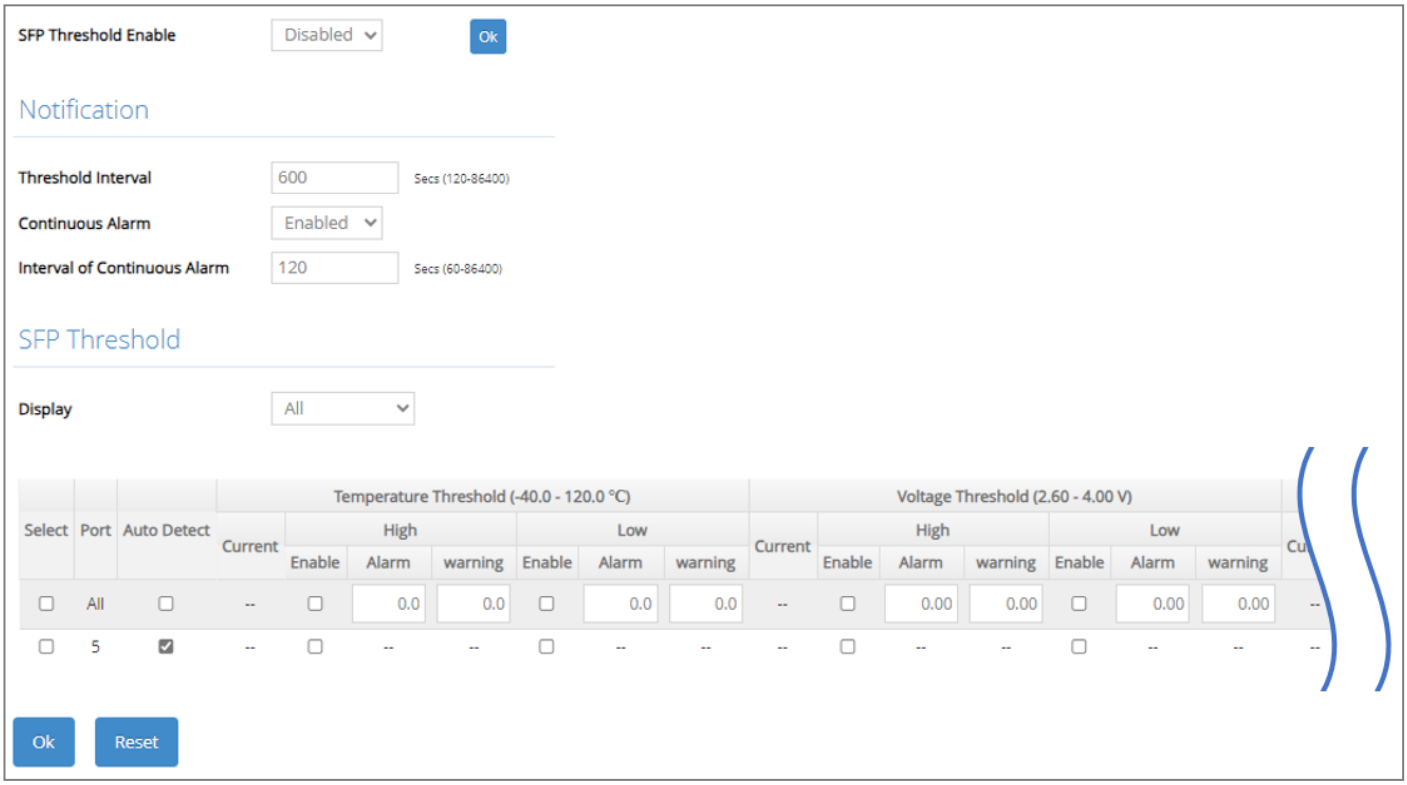
4.9.4.3 SFP Port Threshold Configuration

SFP Port Threshold Configuration function not only displays the transceiver current temperature, voltage, current, TX power and RX power information but is capable of detecting whether the transceiver is at normal status or not.

In the display of the above transceiver information, you can decide one or all items to be shown at a tme by assigning **All/Temperature/Voltage/Current/TX power/RX power** parameter upon your requriements.

Once this function is set to “Enabled”, the alarm/warning message will be sent via trap and syslog in the event of abnormal situations, including temperature/voltage/current/TX power/RX power is over the **High** value or is under the **Low** value. A normal message will also be sent to notify the user when this transceiver temperature/current/voltage/TX power/RX power higher or lower than the threshold returns to the normal status. From these notification, the user can realize the real-time transceiver status to prevent the disconnection and packets loss of any fiber ports from being taken place due to the occurrence of abnormal events.

The following screen page appears if you choose **SFP Port Threshold Configuration** function.



SFP Threshold Enable: Globally enable or disable the alarm notification of temperature/current/voltage/TX power/RX power for SFP ports of the Managed Switch.

Threshold Interval for Notification**:** Specify the time interval of sending SFP ports’ temperature/current/voltage/TX power/RX power alarm message in seconds. The interval can be set from 120 to 86400 seconds. The default setting is 600 seconds.

Continuous Alarm for Notification**:** Enable or disable the continuous alarm/warning message sending function for SFP ports’ temperature/current/voltage/TX power/RX power. Default is “Enabled”.

In case this function is enabled, the alarm/warning message will be sent continuously upon the time interval configured in **Threshold Interval** parameter to notify the user once SFP port's temperature/current/voltage/TX power/RX power is at the abnormal status.

In case this function is disabled, however, the alarm message will be sent only one time to notify the user once SFP port's temperature/current/voltage/TX power/RX power is at the abnormal status.

Interval of Continuous Alarm for Notification**:** Specify the time interval of sending the alarm message for SFP ports' temperature/current/voltage/TX power/RX power in seconds if the parameter of **Continuous Alarm** is enabled. The system will follow this specified time interval to continually send the alarm message (only for the monitored items of which the values exceed the thresholds) even if the monitored item's state remains as it was. Valid range is 60~86400 seconds. Default is "120" seconds.

Display: Select **All**, **Temperature**, **Voltage**, **Current**, **TX Power**, or **RX Power** from the pull-down menu to configure for the intended monitored item(s) altogether or individually.

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

Port: The number of the SFP port.

Auto Detect: Enable the Auto Detect mode by clicking on the checkbox. Unchecking the checkbox means the Manual mode is applied.

> **Auto Detection**: Switch will auto detect alarm & warning threshold values if the SFP/SFP+ transceiver supports and follows the full SFF-8472. The SFP/SFP+ transceiver has default alarm and warning thresholds, which are fixed and cannot be changed.
>
> **Manual**: Network manager can set alarm and warning threshold values manually when SFP/SFP+ transceiver doesn't support the full SFF-8472 or customer doesn't trust the threshold value from SFP/SFP+ transceiver (SFF-8472).

Current status of Temperature/Voltage/Current/TX power/RX power Threshold parameter**:** Display all SFP ports' temperature/Voltage/Current/TX power/RX power currently detected. It will be shown in red color if its current temperature/voltage/current/TX power/RX power is higher than the value in the **High** field or under the value in the **Low** field.

Enable in High & Low fields of Temperature/Voltage/Current/TX power/RX power Threshold parameter**:** Click on the checkbox of the corresponding port number to respectively enable the configured threshold for the specific SFP port's alarm/warning notification of temperature /voltage/current/TX power/RX power.

High/Low Value of Temperature Threshold Alarm/Warning parameter**:** Specify SFP port's temperature Alarm/Warning threshold if the manual mode is applied. Valid range: -40.0 ~ 120.0 degrees centigrade. Default threshold value of Alarm is High: 70, Low: 0; default threshold value of Warning is High: 65, Low: 5.

High/Low Value of Voltage Threshold Alarm/Warning parameter**:** Specify SFP port's voltage

Alarm/Warning threshold if the manual mode is applied. Valid range: 2.60 ~ 4.00 V. Default threshold value of Alarm is High: 3.6, Low: 3; default threshold value of Warning is High: 3.55, Low: 3.05.

High/Low Value of Current Threshold Alarm/Warning parameter**:** Specify SFP port's current Alarm/Warning threshold if the manual mode is applied. Valid range: 0.0 ~ 150.0 mA. Default threshold value of Alarm is High: 90, Low: 0.1; default threshold value of Warning is High: 80, Low: 0.3.

High/Low Value of TX Power Threshold Alarm/Warning parameter**:** Specify SFP port's TX power Alarm/Warning threshold if the manual mode is applied. Valid range: -30.0 ~ 10.0 dBm. Default threshold value of Alarm is High: 0, Low: -20; default threshold value of Warning is High: -1, Low: -19.

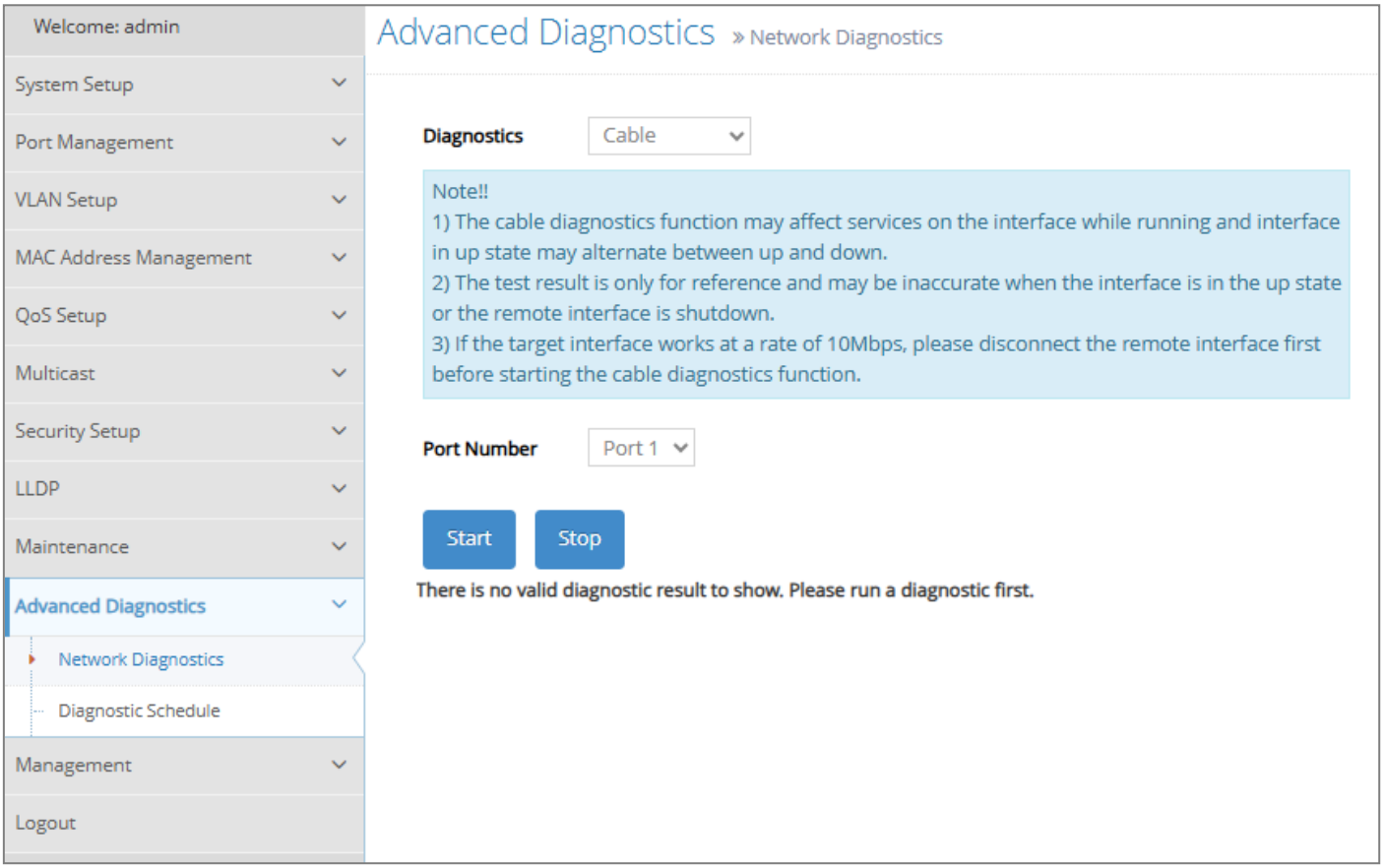
High/Low Value of RX Power Threshold Alarm/Warning parameter**:** Specify SFP port's RX power Alarm/Warning threshold. Valid range: -40.0 ~ 10.0 dBm. Default threshold value of Alarm is High: -5, Low: -25; default threshold value of Warning is High: -6, Low: -24.

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

4.10 Advanced Diagnostics

Apart from the universal monitoring functionality that comes with the Managed Switch, **Advanced Diagnosis** allows administrators to examine the device's operation at a more detailed level and therefore efficiently pinpoint the root cause of potential/existing erroneous functioning.

Please click the folder **Advanced Diagnostics** from the **Main Menu** and then 2 options will be displayed for your selection.

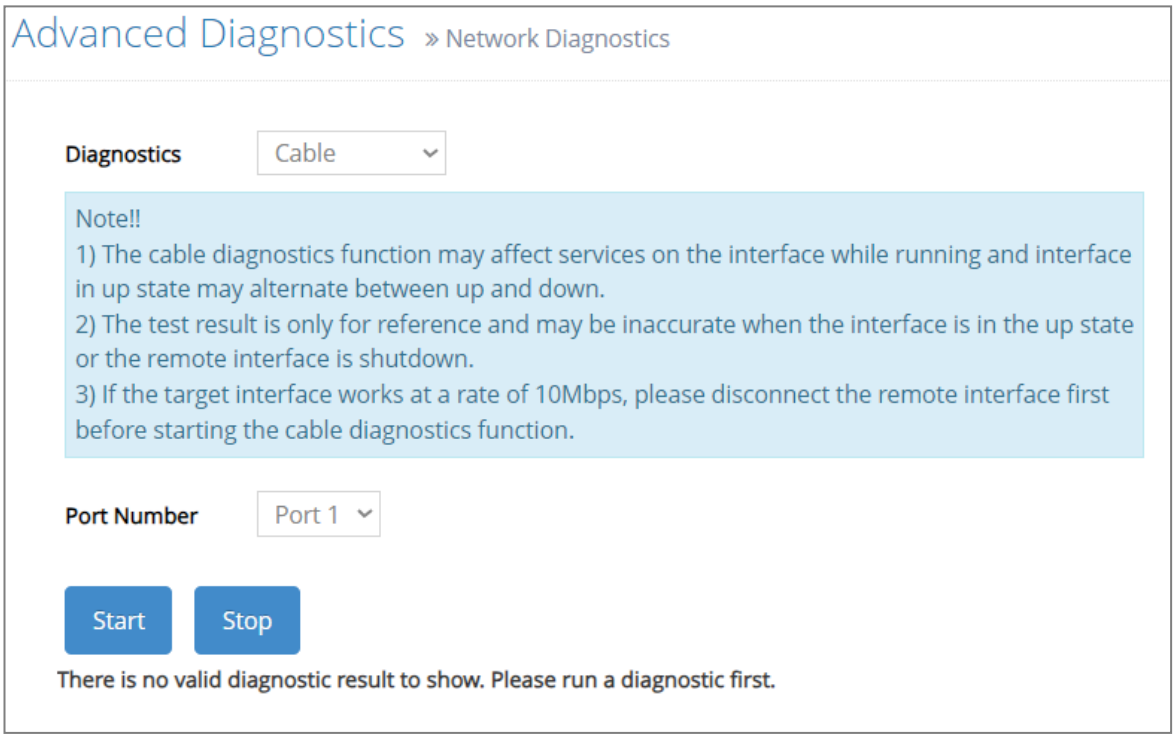


Network Diagnostics: Configure and perform one-time diagnostics, including Cable, DHCP Client, DNS, IPTV, Ping and Throughput diagnostics.

Diagnostics Schedule: Configure and perform diagnostics periodically, including Cable, DHCP Client, DNS, IPTV, Ping and Throughput diagnostics.

4.10.1 Network Diagnostics

Click the option **Network Diagnostics** from the **Advanced Diagnostics** menu and then the following screen page appears.



Click the dropdown menu next to **Diagnostics** to expand and view all the diagnostic options described below.

Cable: Perform Ethernet cable tests on the selected interfaces to enable efficient fault investigation and simplified network troubleshooting.

DHCP Client: Simulates a DHCP client to verify IP address allocation and network connectivity.

DNS: Tests DNS server accessibility and measures response performance.

IPTV: Includes tools for diagnosing IPTV metrics such as **MPEG Loss**, **PCR Jitter**, **Throughput**, **General Query Interval**, **General Query Response**, and **Zapping Time**.

Ping: Checks connectivity and measures latency by sending ICMP echo requests to a specified target.

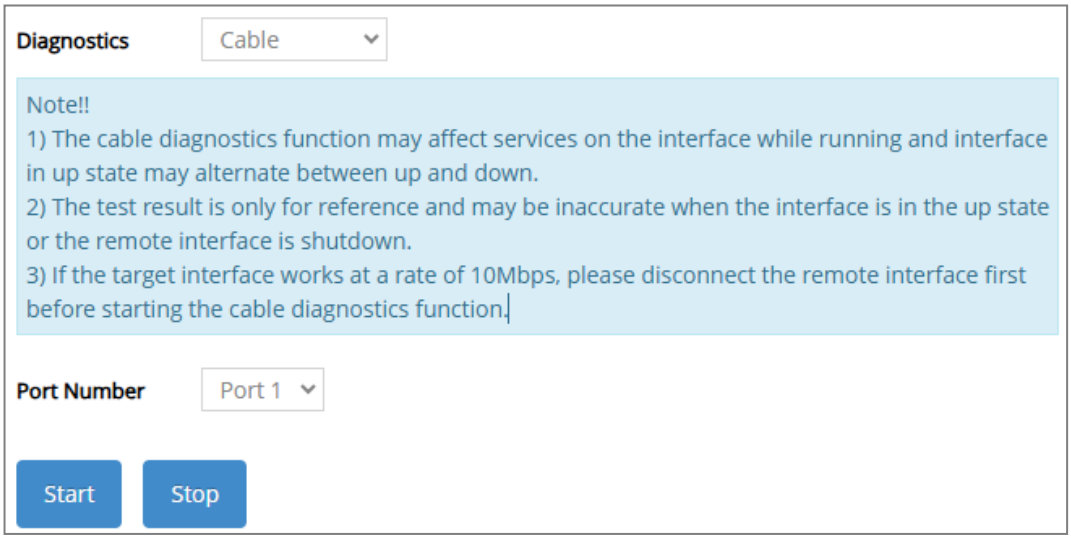
Throughput: Evaluates data transfer rates to assess network performance using tools like iPerf3 or Nuttcp.

For more details, please refer to the corresponding section that follows.

4.10.1.1 Cable Diagnostics

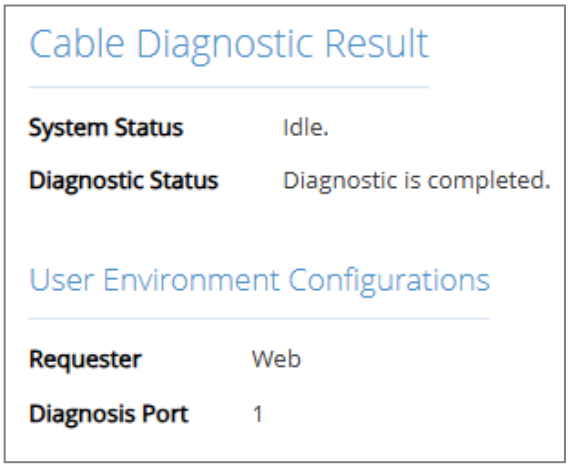
Ethernet cables, consisting of two separate pairs of insulated wires, could at times malfunction due to unknown technical issues. As troublesome as they are by nature for the data transmission interference, the difficulties in detecting where and what the cable faults stem from undoubtedly make things worse. The Cable Diagnosis does the job for you, allowing remote cable issue recognition and fault distance determination. The diagnosis delivers efficiency in troubleshooting and failure prevention since, among countless possible reasons for existing or potential defects, you can now rule out the irrelevant ones to conclude the fault investigation and therefore have your Ethernet cables ready for reliable operation.

After clicking Cable from the Diagnostics dropdown menu, the following page will appear.



Port Number: A dropdown menu with options ranging from Port 1 to Port 4. Port 1 corresponds to LAN 1, Port 2 corresponds to LAN 2, and so on. Select the port you wish to diagnose.

Click **Start** to begin the diagnostic process, and click **Stop** to halt it.
The status of the diagnostic procedure, user configurations, and diagnostic results will be displayed as shown below once **Start** is clicked.

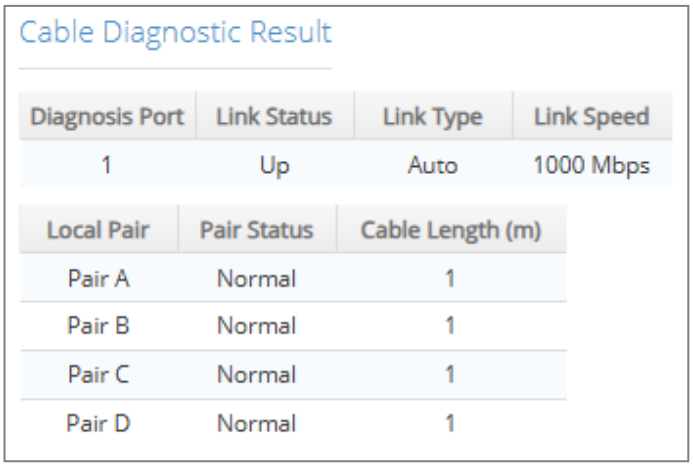


System Status: Displays the current status of the system.

Diagnostics Status: Displays the status of the diagnostics process for the most recent diagnostic result.

User Environment Configurations: Display the settings and requester information for the most recent diagnostic result.

Requester: Displays the source initiated the most recent diagnostics.



Diagnosis Port: Displays the port number being diagnosed

Link Status: Displays the link's connection status.

Link Type: The port type of the interface. It's either **Auto** or **Manual** depending on the specified port configuration right upon the testing.

Link Speed: The current transmission speed of the interface, depending on the port speed configuration right upon the testing.

Local Pair: Which pair of the wires in the connected Ethernet cable; **Local** signifies this Managed Switch.

Note:
*1. The terminology of **Pair** is used because an Ethernet cable consists of 8 wires, and typically they will be paired up in cabling deployments.*
*2. IEEE 802.3u **100Base-TX** only uses two pairs in one single cable.*

Pair Status: The diagnosis result of the target interface. Possible results are listed down below.

Normal: The pair is working properly and as expected. For Fast Ethernet, **Pair A** and **Pair B** should be in Normal status, whereas for Gigabit Ethernet, all pairs should be in Normal status.

Short: There is a short circuit in the pair.

Open: There is an open circuit in the pair.

Mismatch: There is a mismatch with the cable impedance in the pair.

Cross: There is crosstalk in the pair.

Unknown: Faulty functioning occurs but does not result from any of **Short, Open, Mismatch, or Cross**. It requires specialized cable testing equipment to find out the cause of the errors.

Cable Length (m): The pair length of the cable, or the distance between the local interface and the fault point in the pair within the cable.

4.10.1.2 DHCP Client Diagnostics

After clicking **DHCP Client** from the **Diagnostics** dropdown menu, the following page will appear.

IP Version: Choose the IP version (IPv4 or IPv6) for diagnostics. The displayed fields will vary based on the selected IP version.

Auto Configuration Type: This dropdown menu includes **Stateless** and **Stateful**. Available only when IPv6 is selected as the IP version.

> **Stateless:** The device generates its own IP address based on the network prefix, with the DHCPv6 server only providing additional configuration information (like DNS).
>
> **Stateful:** The DHCPv6 server assigns the device a full IP address and manages its lease.

VLAN: Enter the VLAN ID to specify the diagnostic scope. The valid range is from 1 to 4094.

Source MAC: Specify the MAC address of the source device to be used in diagnostics.

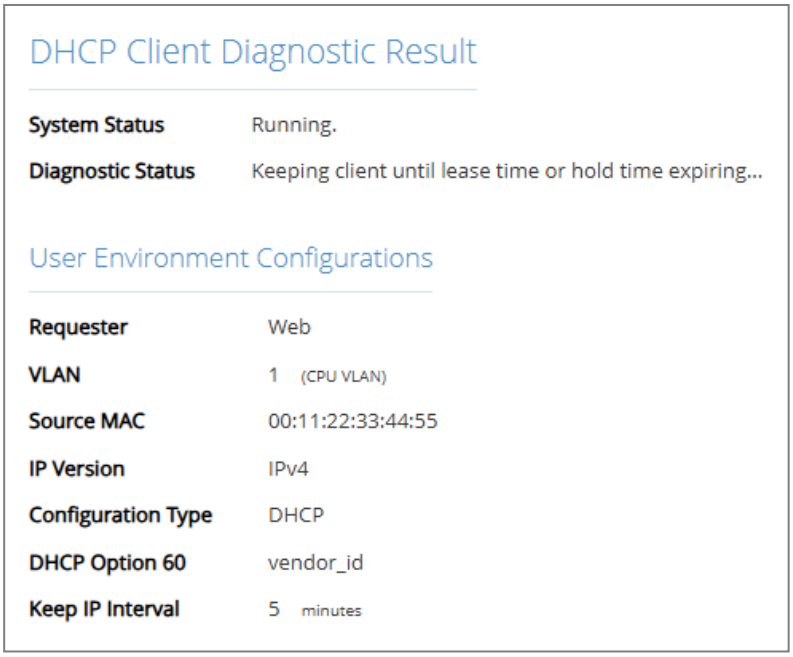
Keep IP Interval: Define the duration, in minutes, for retaining the assigned IP address. The valid range is from 0 to 30, where 0 means the IP address is released immediately after use.

Option 60: Enter the DHCP Option 60 value (Vendor Class Identifier) to identify the device type for appropriate IP assignment. A field available only when IPv4 is selected as the IP version.

Option 15: Specify the DHCPv6 domain name to identify the appropriate domain for the client, aiding in network configuration selection. A field available only when IPv6 is selected as the IP version.

Option 16: Enter a Vendor-Specific Information (VSI) value to exchange custom configuration data between the client and the DHCPv6 server. A field available only when IPv6 is selected as the IP version.

Click **Start** to begin the diagnostic process, and click **Stop** to halt it.
The status of the diagnostic procedure, user configurations, and diagnostic results will be displayed as shown below once **Start** is clicked.

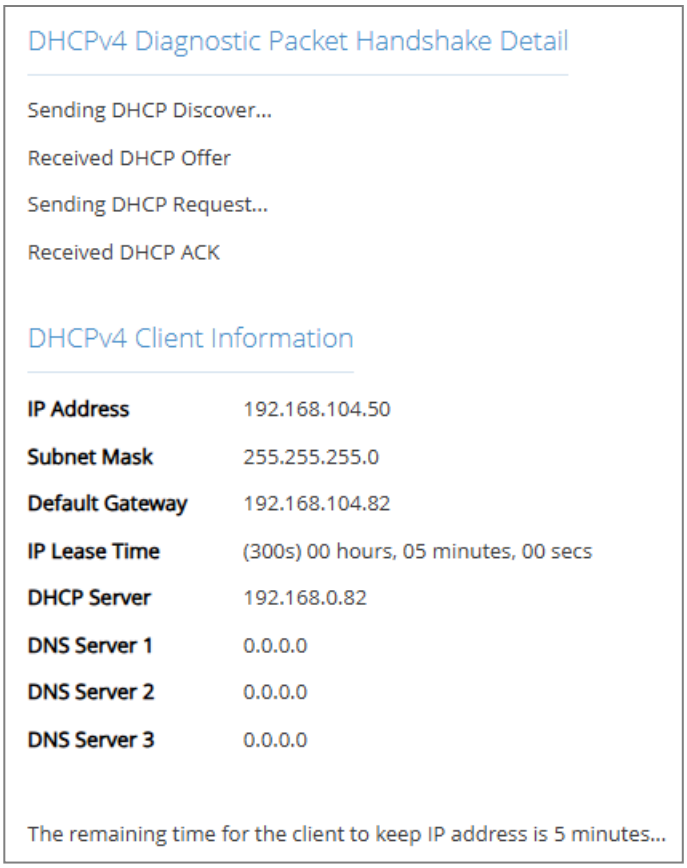


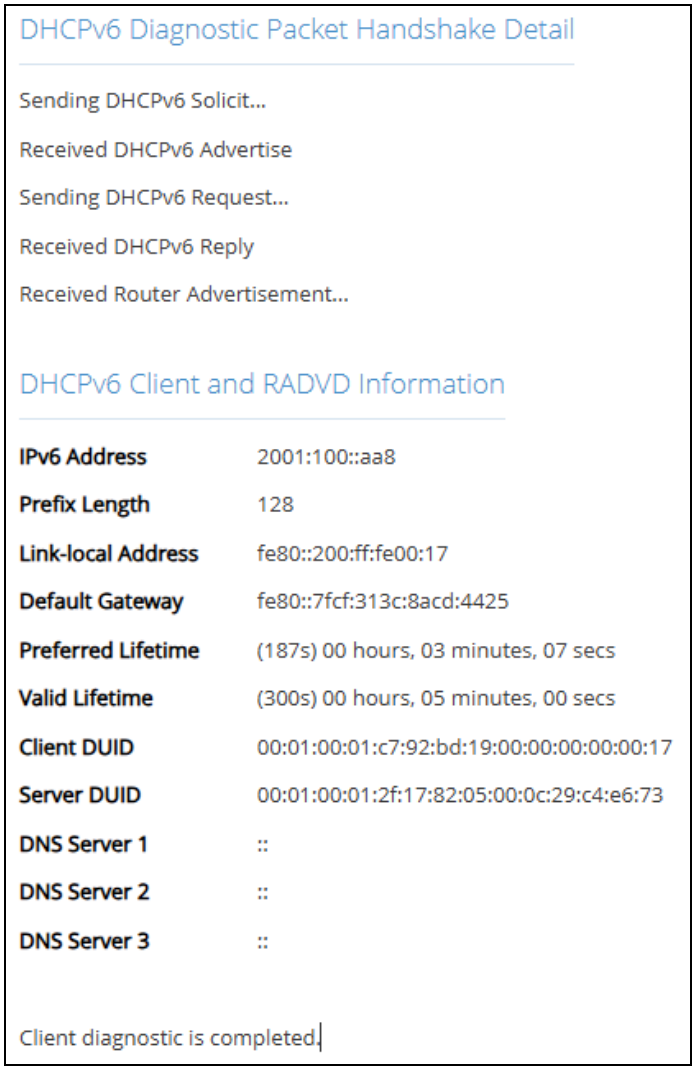
System Status: Displays the current status of the system.

Diagnostics Status: Displays the status of the diagnostics process for the most recent diagnostic result.

User Environment Configurations: Display the settings and requester information for the most recent diagnostic result.

Requester: Displays the source initiated the most recent diagnostics.





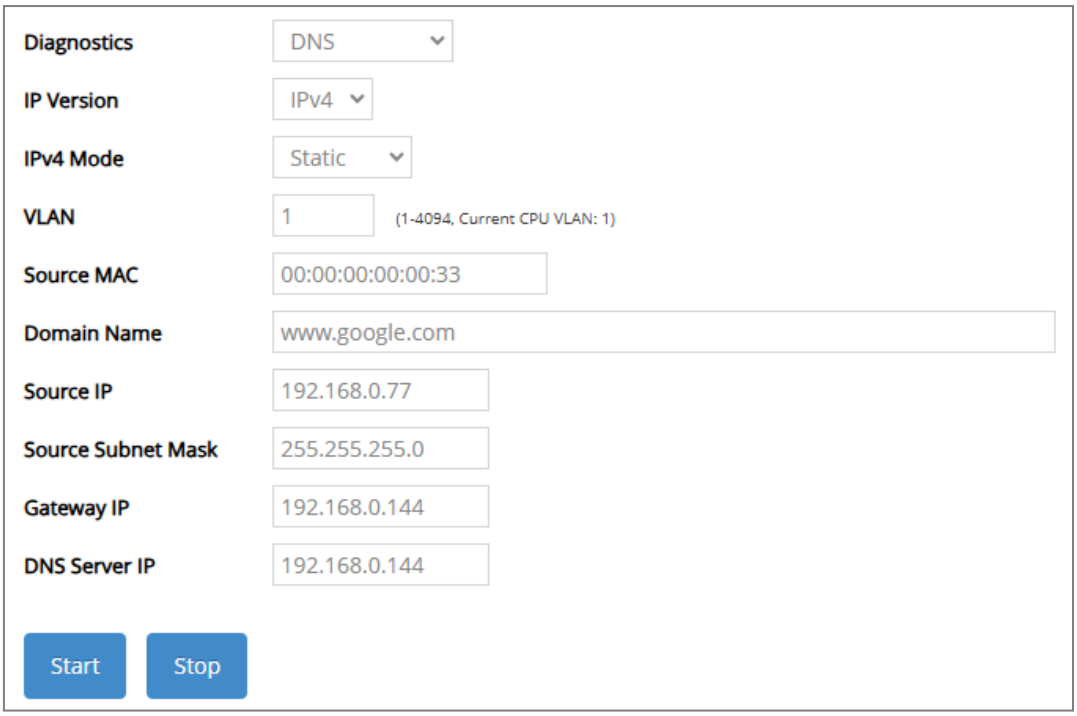
DHCPv4/v6 Diagnostic Packet Handshake Detail: Displays the sequence of DHCP packet exchanges during client emulation.

DHCPv4 Client Information: Displays the result of DHCPv4 client emulation, including the assigned IP address, subnet mask, default gateway, IP lease time, DHCP server address, and DNS server addresses.

DHCPv6 Client and RADVD Information: Displays the result of DHCPv6 client emulation and information from Router Advertisement (RADVD) messages. Includes the assigned IPv6 address, prefix length, preferred/valid life time, DHCP server address, and up to three DNS server addresses. Additionally, displays network prefixes, default gateway, and other configuration details advertised via RADVD.

4.10.1.3 DNS Diagnostics

After clicking **DNS** from the **Diagnostics** dropdown menu, the following page will appear.



IP Version: Select the IP protocol version for diagnostics. Options include IPv4 or IPv6.

IPv4/IPv6 Mode: Choose the IP assignment mode. Options include **Static** (manual IP configuration) or **DHCPv4/v6** (automatic IP assignment).

VLAN: Enter the VLAN ID (valid range: 1 to 4094) for DNS diagnostics.

Source MAC: Enter the MAC address of the source device initiating the DNS diagnostics.

Domain Name: Enter the domain name to test DNS resolution.

Source IP: Enter the source IP address. This field is available only when Static IP mode is selected.

Source Subnet Mask: Enter the source subnet mask. This field is available only when Static IPv4 mode is selected.

Source Prefix Length: Enter the source prefix length. This field is available only when Static IPv6 mode is selected.

Gateway IP: Enter the gateway IP address. This field is available only when Static IP mode is selected.

Option 60: Enter the DHCP Option 60 value (Vendor Class Identifier). This field is available only when DHCPv4 mode is selected.

Auto Configuration Type: Select the configuration type for DHCPv6. This field is available only when DHCPv6 mode is selected.

Stateless: IP addresses are assigned without maintaining state.

Stateful: Full configuration and address assignment are managed.

Option 15: Enter a list of domains to append to unqualified hostnames during DNS queries. This option is available only when DHCPv6 mode is selected.

Option 16: Enter a Vendor Class Identifier to specify the device's class, influencing DNS and other network configurations. This option is available only when DHCPv6 mode is selected.

DNS Server IP: Enter the DNS server IP address.

Click **Start** to begin the diagnostic process, and click **Stop** to halt it.
The status of the diagnostic procedure, user configurations, and diagnostic results will be displayed as shown below once **Start** is clicked.

System Status: Displays the current status of the system.

Diagnostics Status: Displays the status of the diagnostics process for the most recent diagnostic result.

User Environment Configurations: Display the settings and requester information for the most recent diagnostic result.

Requester: Displays the source initiated the most recent diagnostics.

Client IP Emulation Configuration: Display the client IP emulation settings information for the most recent diagnostic result.

DNS Diagnostic Result: Display the DNS Diagnostics Results such as DNS Server, DNS IP Address, URL Name and Address 1.

> **Server:** Display the domain name / IP address of the DNS Server.
>
> **Address:** Display the IP address and the port number of the DNS Server. The number after the "#" represents the port number.
>
> **Name:** Display the tested domain name URL.
>
> **Address 1:** Display the IP address corresponding to the domain name URL, as resolved by the DNS server.

4.10.1.4 IPTV Diagnostics

After selecting **IPTV** from the Diagnostics dropdown menu, the **Multicast** dropdown menu will appear with the following options:

MPEG-Loss: Monitors packet loss affecting video, audio, or other multicast streams.

PCR-Jitter: Analyzes time variations in program clock reference (PCR) packets.

Throughput: Evaluates data transfer rates for multicast streams.

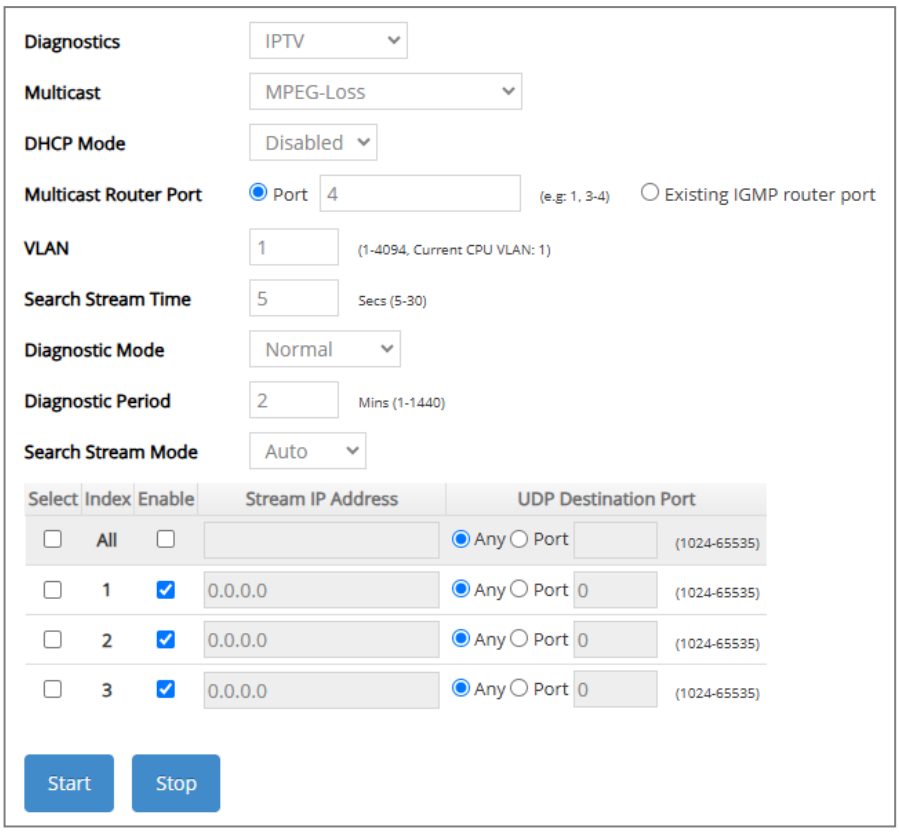
General Query Interval: Checks multicast query intervals to ensure optimal settings.

General Query Response: Measures the response time for multicast queries.

Zapping Time: Tracks channel-switching delays for IPTV streams.

4.10.1.4.1 MPEG-Loss

The IPTV Multicast MPEG-Loss Diagnostics



DHCP Mode: Enable or Disable the DHCP Mode.

Enable: Simulates a set-top box (STB) by sending IGMP Join messages to retrieve the corresponding multicast stream for diagnostics.

Disable: Captures multicast streams being forwarded by the switch for diagnostics.

Multicast Router Port: Define the multicast router port by manually entering a port or selecting an existing IGMP router port.

VLAN: Enter the VLAN ID to specify the diagnostic scope. The valid range is from 1 to 4094.

Source MAC: Specify the MAC address of the source device to be used in diagnostics.

Option 60: Enter the DHCP Option 60 value (Vendor Class Identifier). This field is available only when DHCP mode is enabled.

Search Stream Time: Define the stream search time in seconds. The valid range is 5 to 30.

Diagnostic Mode: Configure the iptv MPEG Loss diagnostic mode. Option includes **Normal**, **PID** and **Per Seconds**.

> **Normal:** Supports up to 3 streams simultaneously with a diagnostic period of up to 1440 minutes (1 day).
>
> **PID:** Supports 1 stream at a time with a diagnostic period of up to 60 minutes (1 hour).

Note:
Each stream PID is corresponding to different service (e.g. video, audio, logo, subtitle...etc.), you can easier to identify which service has been packet loss.

> **Per Seconds:** Supports up to 3 streams simultaneously with a diagnostic period of up to 60 minutes (1 hour).

Diagnostic Period: Set the diagnostic period in minutes. The valid range is from 1 to 1440.

Search Stream Mode: Configure the Search Stream mode as Auto or Manual.

> **Auto:** Captures multicast streams being forwarded by the switch for diagnostics, prioritizing the highest rate streams (up to three streams).
>
> **Manual:** Allows manual entry of the stream IP address. When DHCP Mode is set to Enable, Search Stream Mode is restricted to Manual.

Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards.

Index: Display the stream index number.

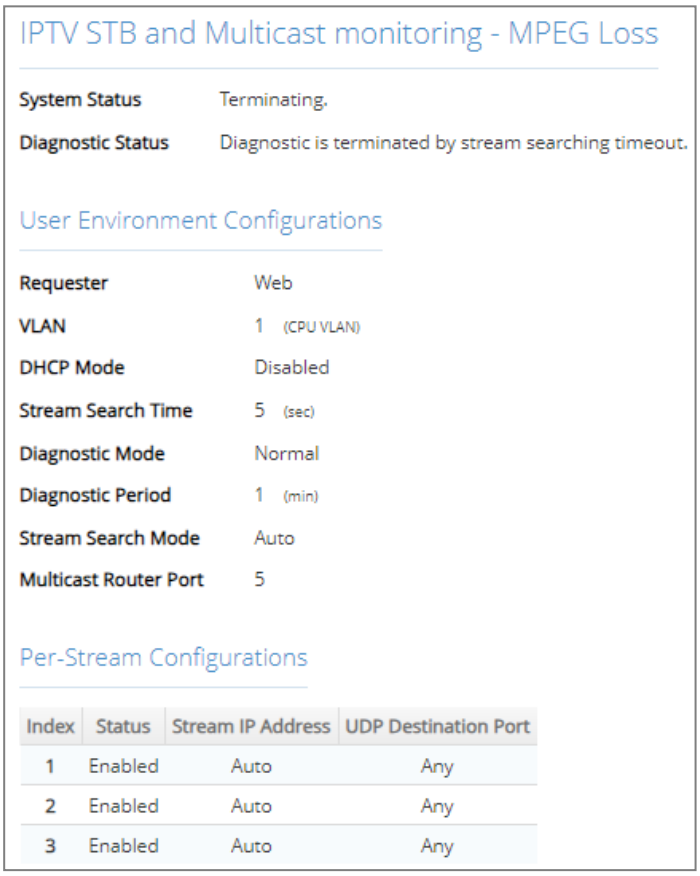
Enable: A checkbox to enable or disable the stream index.

Stream IP Address: When Search Stream Mode is set to Auto, this column displays the stream IP address. When Search Stream Mode is set to Manual, use this field to specify the stream IP address.

UDP Destination Port: Specify the destination port for the multicast stream.

> **Any**: Accept any destination port.
>
> **Port:** Enter a specific port number. The valid range is from 1024 to 65535.

Click **Start** to begin the diagnostic process, and click **Stop** to halt it.
The status of the diagnostic procedure, user configurations, and diagnostic results will be displayed as shown below once Start is clicked.



IPTV STB and Multicast monitoring - MPEG Loss

System Status	Terminating.
Diagnostic Status	Diagnostic is terminated by stream searching timeout.

User Environment Configurations

Requester	Web
VLAN	1 (CPU VLAN)
DHCP Mode	Disabled
Stream Search Time	5 (sec)
Diagnostic Mode	Normal
Diagnostic Period	1 (min)
Stream Search Mode	Auto
Multicast Router Port	5

Per-Stream Configurations

Index	Status	Stream IP Address	UDP Destination Port
1	Enabled	Auto	Any
2	Enabled	Auto	Any
3	Enabled	Auto	Any

System Status: Displays the current status of the system.

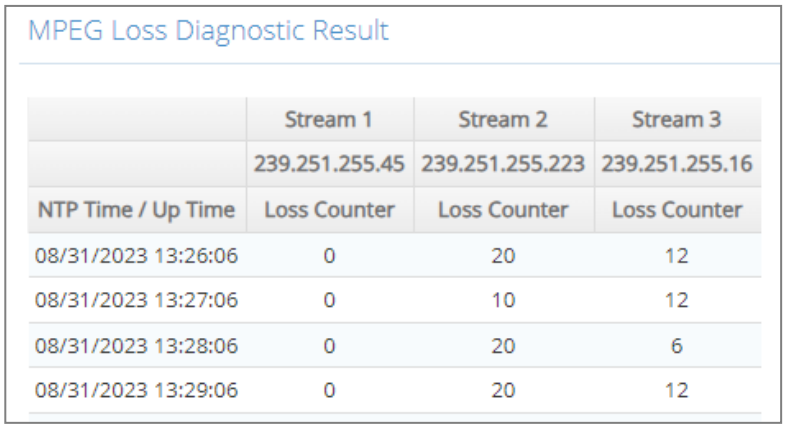
Diagnostics Status: Displays the status of the diagnostics process for the most recent diagnostic result.

User Environment Configurations: Display the settings and requester information for the most recent diagnostic result.

Requester: Displays the source initiated the most recent diagnostics.

Per-Stream Configurations: Display the configurations for streams 1 to 3.

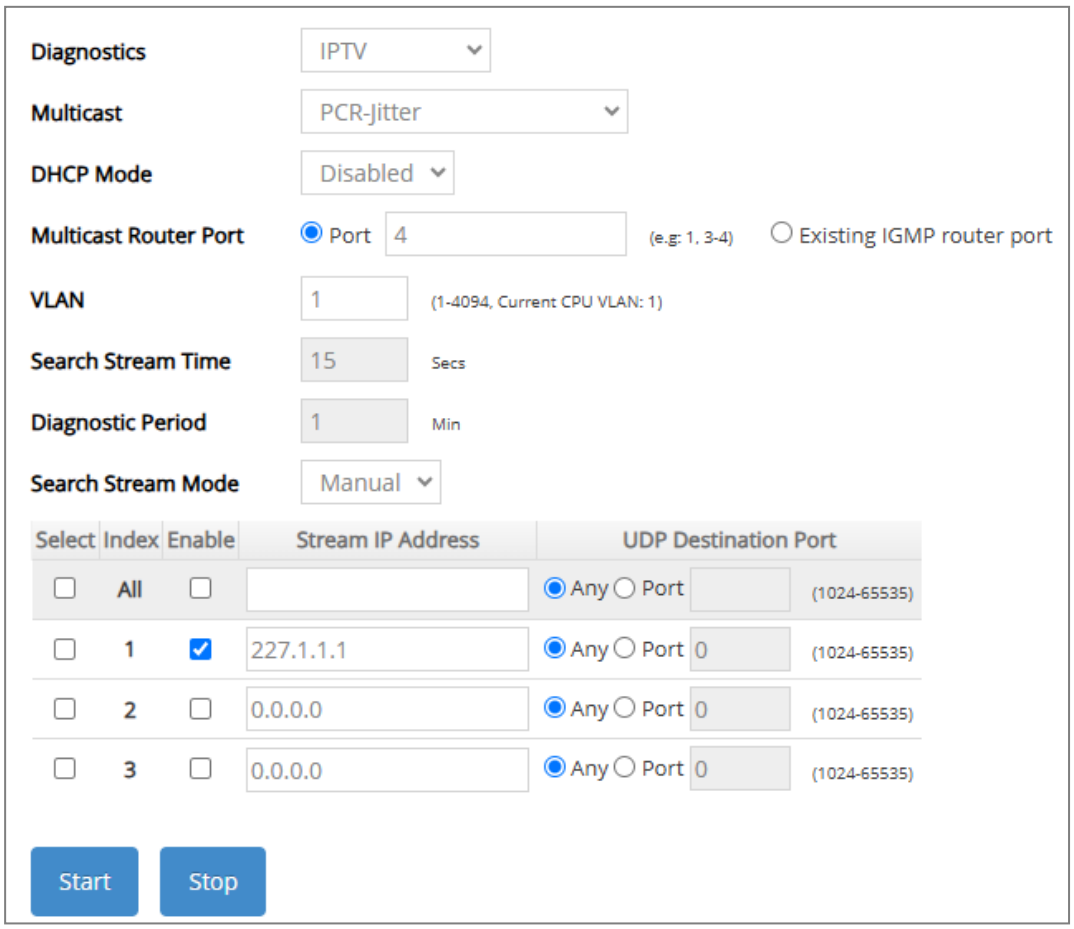
MPEG Loss Diagnostic Result: Display the IPTV MPEG Loss diagnostic result for streams 1 to 3.



MPEG Loss Diagnostic Result

	Stream 1	Stream 2	Stream 3
	239.251.255.45	239.251.255.223	239.251.255.16
NTP Time / Up Time	Loss Counter	Loss Counter	Loss Counter
08/31/2023 13:26:06	0	20	12
08/31/2023 13:27:06	0	10	12
08/31/2023 13:28:06	0	20	6
08/31/2023 13:29:06	0	20	12

4.10.1.4.2 PCR-Jitter



DHCP Mode: Enable or Disable the DHCP Mode.

> **Enable:** Simulates a set-top box (STB) by sending IGMP Join messages to retrieve the corresponding multicast stream for diagnostics.
>
> **Disable:** Captures multicast streams being forwarded by the switch for diagnostics.

Multicast Router Port: Define the multicast router port by manually entering a port or selecting an existing IGMP router port.

VLAN: Enter the VLAN ID to specify the diagnostic scope. The valid range is from 1 to 4094.

Source MAC: Specify the MAC address of the source device to be used in diagnostics. This field is available only when DHCP mode is enabled.

Option 60: Enter the DHCP Option 60 value (Vendor Class Identifier). This field is available only when DHCP mode is enabled.

Search Stream Time: Display the stream search time in seconds.

Diagnostic Period: Display the diagnostic period in minutes.

Search Stream Mode: Configure the Search Stream mode as Auto or Manual.

> **Auto:** Captures multicast streams being forwarded by the switch for diagnostics, prioritizing the highest rate streams (up to three streams).

Manual: Allows manual entry of the stream IP address. When DHCP Mode is set to Enable, Search Stream Mode is restricted to Manual.

Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards.

Index: Display the stream index number.

Enable: A checkbox to enable or disable the stream index.

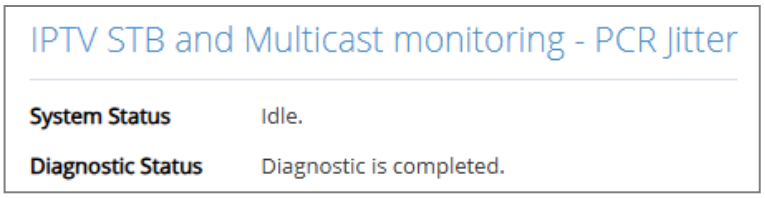
Stream IP Address: When Search Stream Mode is set to Auto, this column displays the stream IP address. When Search Stream Mode is set to Manual, use this field to specify the stream IP address.

UDP Destination Port: Specify the destination port for the multicast stream.

Any: Accept any destination port.

Port: Enter a specific port number. The valid range is from 1024 to 65535.

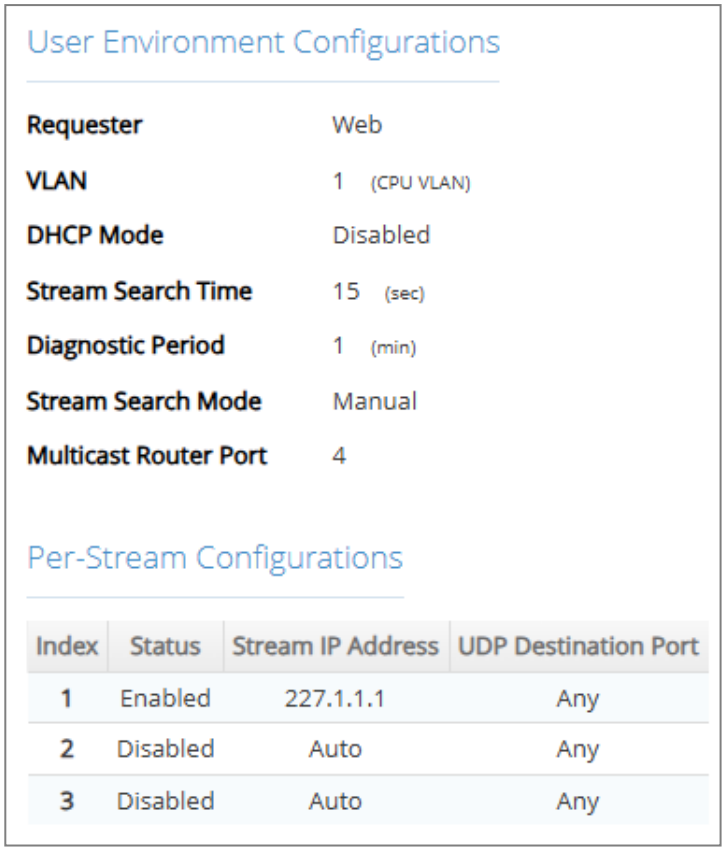
Click **Start** to begin the diagnostic process, and click **Stop** to halt it.
The status of the diagnostic procedure, user configurations, and diagnostic results will be displayed as shown below once Start is clicked.



System Status: Displays the current status of the system.

Diagnostics Status: Displays the status of the diagnostics process for the most recent diagnostic result.

User Environment Configurations: Display the settings and requester information for the most recent diagnostic result.



User Environment Configurations

Requester	Web
VLAN	1 (CPU VLAN)
DHCP Mode	Disabled
Stream Search Time	15 (sec)
Diagnostic Period	1 (min)
Stream Search Mode	Manual
Multicast Router Port	4

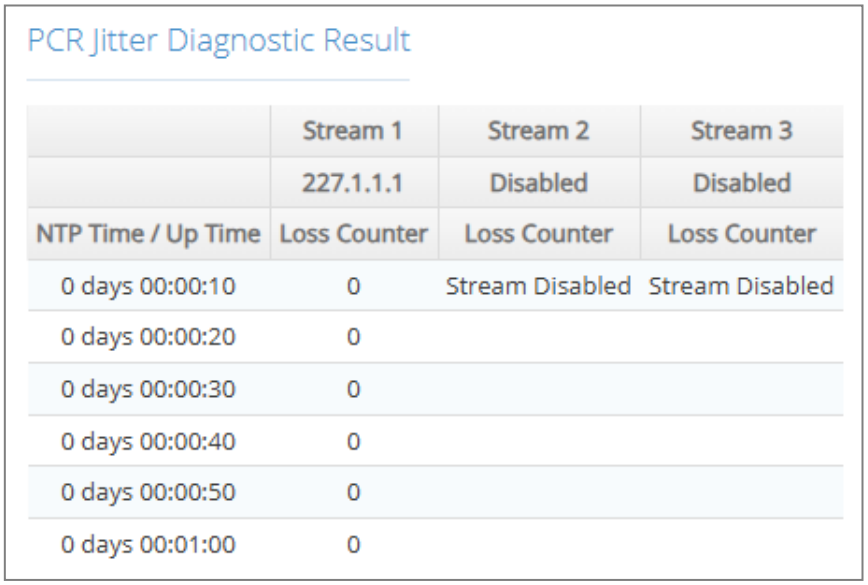
Per-Stream Configurations

Index	Status	Stream IP Address	UDP Destination Port
1	Enabled	227.1.1.1	Any
2	Disabled	Auto	Any
3	Disabled	Auto	Any

Requester: Displays the source initiated the most recent diagnostics.

Per-Stream Configurations: Display the configurations for streams 1 to 3.

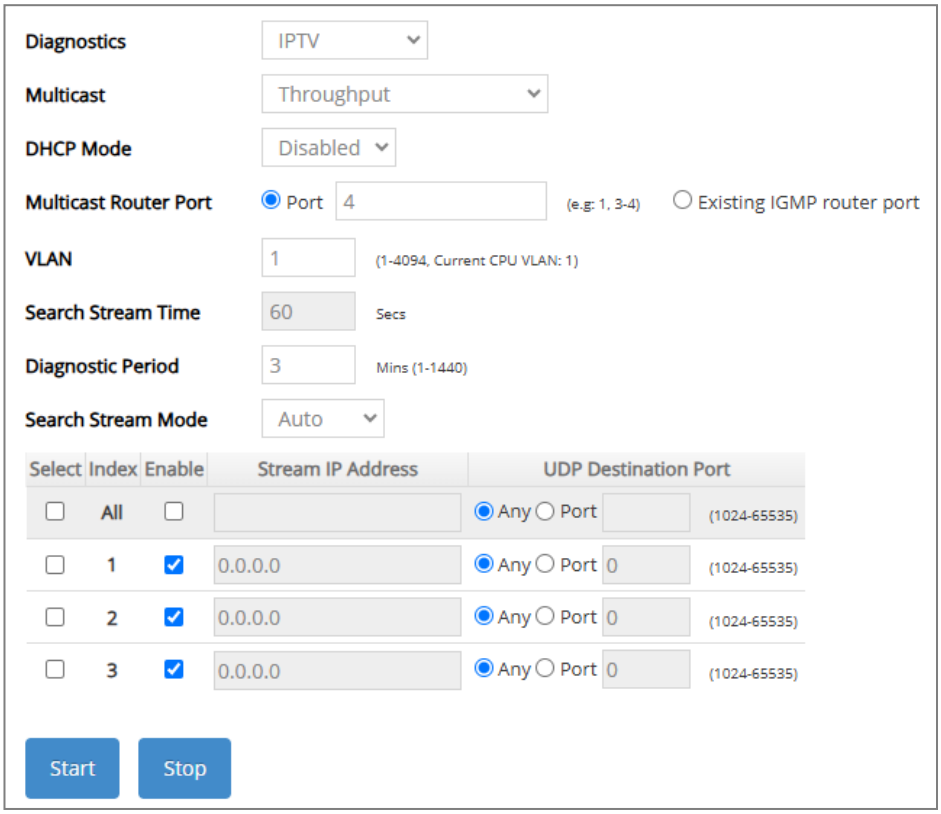
PCR Jitter Diagnostic Result: Display the IPTV PCR Jitter diagnostic result for streams 1 to 3.



PCR Jitter Diagnostic Result

	Stream 1	Stream 2	Stream 3
	227.1.1.1	Disabled	Disabled
NTP Time / Up Time	Loss Counter	Loss Counter	Loss Counter
0 days 00:00:10	0	Stream Disabled	Stream Disabled
0 days 00:00:20	0		
0 days 00:00:30	0		
0 days 00:00:40	0		
0 days 00:00:50	0		
0 days 00:01:00	0		

4.10.1.4.3 Throughput



DHCP Mode: Enable or Disable the DHCP Mode.

Enable: Simulates a set-top box (STB) by sending IGMP Join messages to retrieve the corresponding multicast stream for diagnostics.

Disable: Captures multicast streams being forwarded by the switch for diagnostics.

Multicast Router Port: Define the multicast router port by manually entering a port or selecting an existing IGMP router port.

VLAN: Enter the VLAN ID to specify the diagnostic scope. The valid range is from 1 to 4094.

Source MAC: Specify the MAC address of the source device to be used in diagnostics. This field is available only when DHCP mode is enabled.

Option 60: Enter the DHCP Option 60 value (Vendor Class Identifier). This field is available only when DHCP mode is enabled.

Search Stream Time: Display the stream search time in seconds.

Diagnostic Period: Set the diagnostic period in minutes. The valid range is from 1 to 1440.

Search Stream Mode: Configure the Search Stream mode as Auto or Manual.

Auto: Captures multicast streams being forwarded by the switch for diagnostics, prioritizing the highest rate streams (up to three streams).

Manual: Allows manual entry of the stream IP address. When DHCP Mode is set to

Enable, Search Stream Mode is restricted to Manual.

Select: Enable or disable any new settings configured in the row of **All** port to be applied as well to all ports at a time. To enable it, please click on its checkbox in the row of **All** port, and then all ports will be checked immediately afterwards.

Index: Display the stream index number.

Enable: A checkbox to enable or disable the stream index.

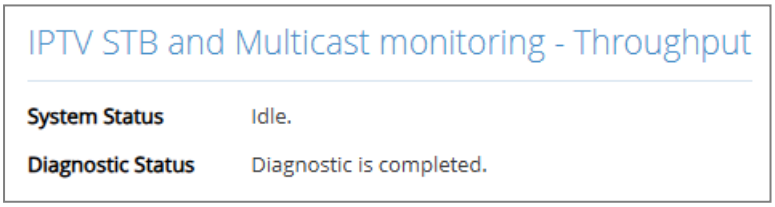
Stream IP Address: When Search Stream Mode is set to Auto, this column displays the stream IP address. When Search Stream Mode is set to Manual, use this field to specify the stream IP address.

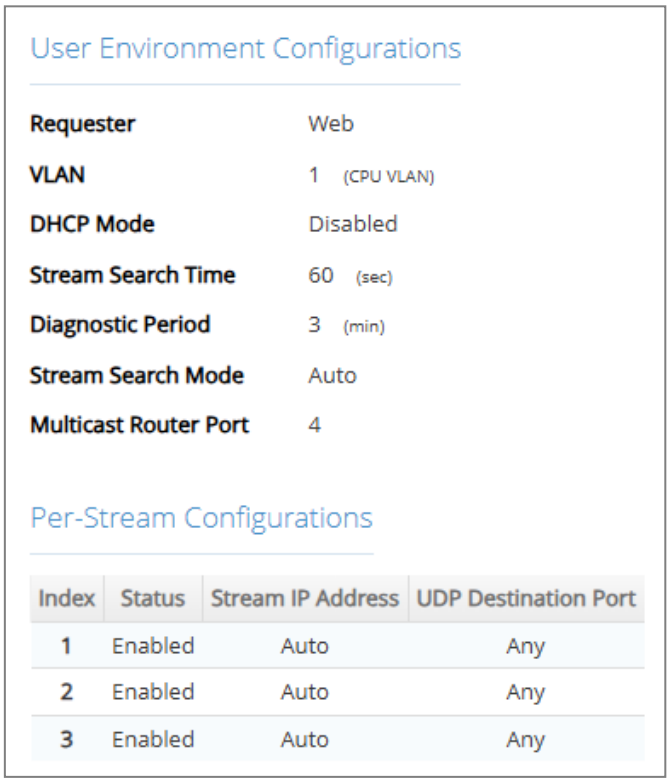
UDP Destination Port: Specify the destination port for the multicast stream.

Any: Accept any destination port.

Port: Enter a specific port number. The valid range is from 1024 to 65535.

Click **Start** to begin the diagnostic process, and click **Stop** to halt it.
The status of the diagnostic procedure, user configurations, and diagnostic results will be displayed as shown below once Start is clicked.





System Status: Displays the current status of the system.

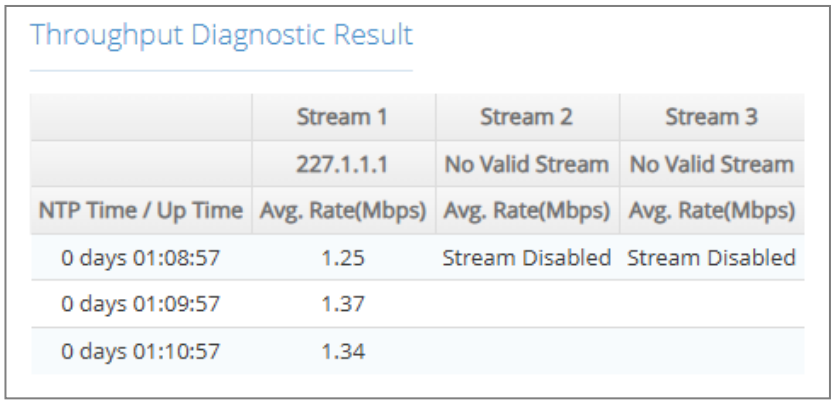
Diagnostics Status: Displays the status of the diagnostics process for the most recent diagnostic result.

User Environment Configurations: Display the settings and requester information for the most recent diagnostic result.

Requester: Displays the source initiated the most recent diagnostics.

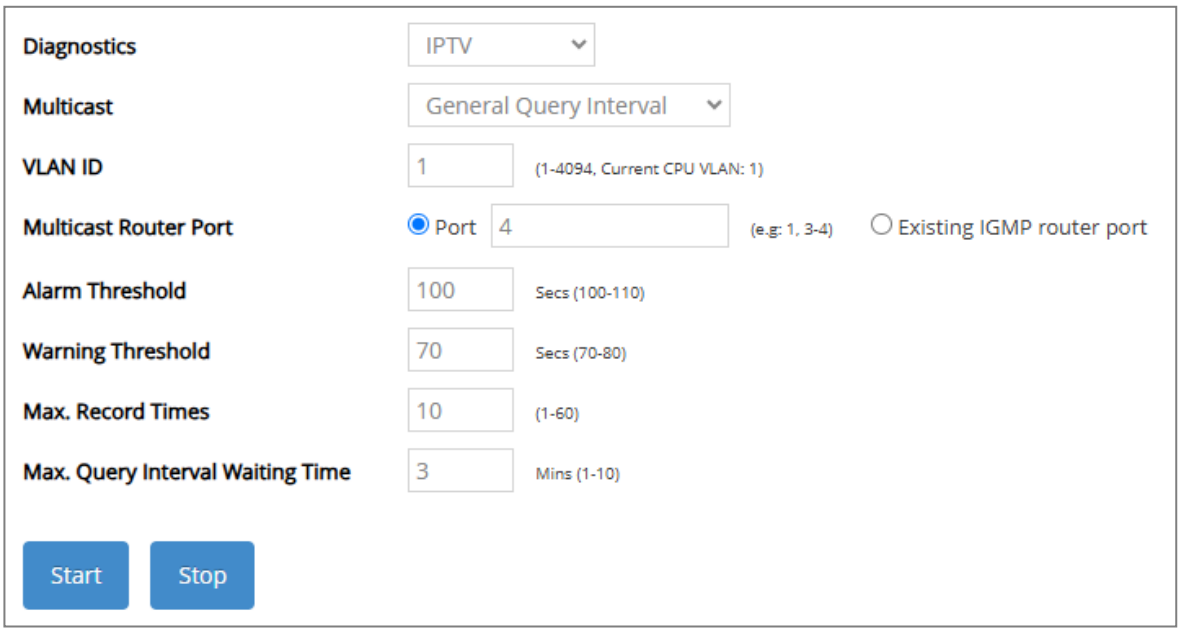
Per-Stream Configurations: Display the configurations for streams 1 to 3.

Throughput Diagnostic Result: Display the IPTV Throughput diagnostic result for streams 1 to 3.


Throughput Diagnostic Result

	Stream 1	Stream 2	Stream 3
	227.1.1.1	No Valid Stream	No Valid Stream
NTP Time / Up Time	Avg. Rate(Mbps)	Avg. Rate(Mbps)	Avg. Rate(Mbps)
0 days 01:08:57	1.25	Stream Disabled	Stream Disabled
0 days 01:09:57	1.37		
0 days 01:10:57	1.34		

4.10.1.4.4 General Query Interval



VLAN ID: Enter the VLAN ID to specify the diagnostic scope. The valid range is from 1 to 4094.

Multicast Router Port: Define the multicast router port by manually entering a port or selecting an existing IGMP router port.

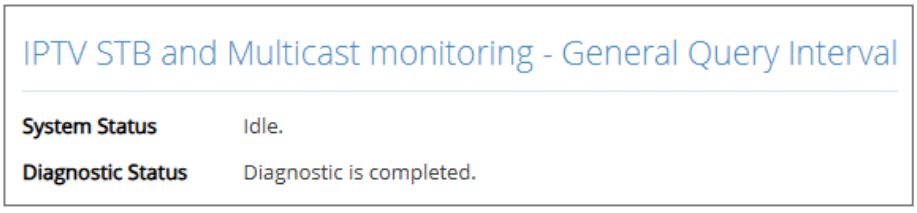
Alarm Threshold: Set the alarm threshold in seconds. The valid range is from 100 to 110.

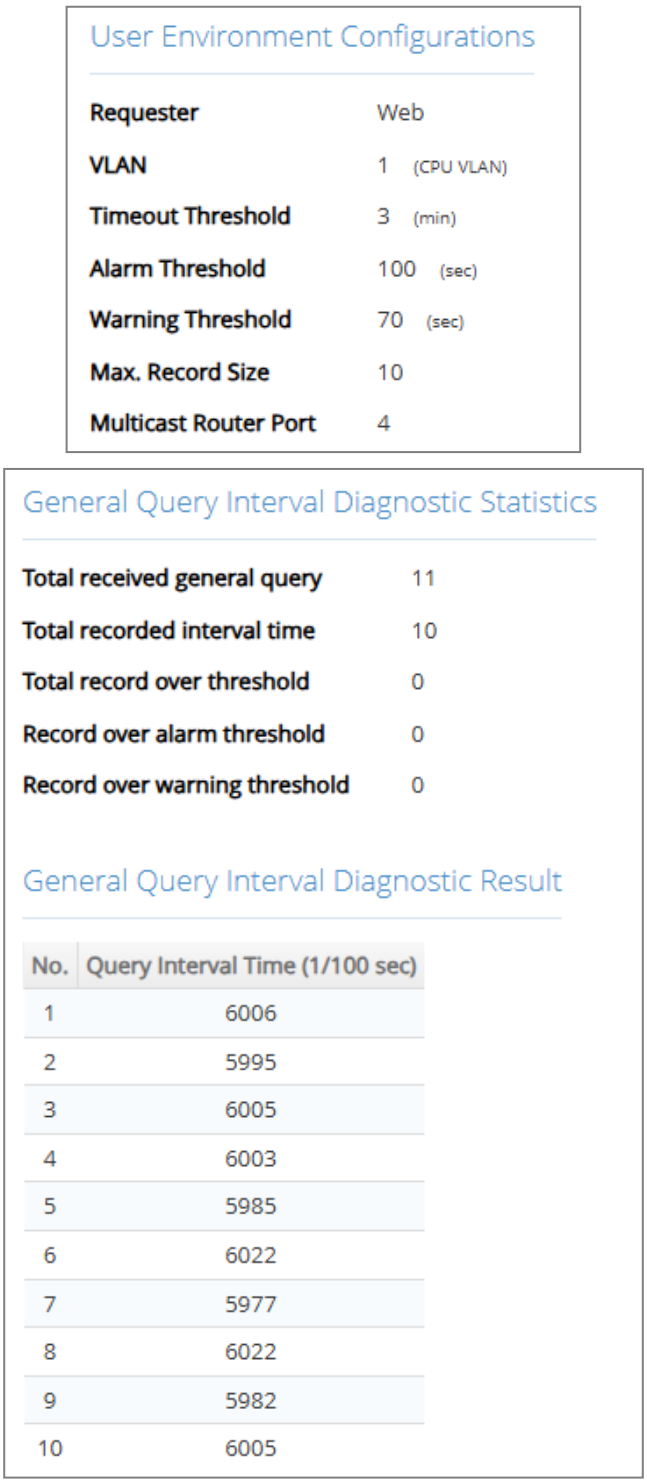
Warning Threshold: Set the warning threshold in seconds. The valid range is from 70 to 80.

Max. Record Times: Specify the maximum number of records. The valid range is from 1 to 60.

Max. Query Interval Waiting Time: Define the maximum waiting time for a query interval in minutes. The valid range is from 1 to 10.

Click **Start** to begin the diagnostic process, and click **Stop** to halt it.
The status of the diagnostic procedure, user configurations, and diagnostic results will be displayed as shown below once Start is clicked.





User Environment Configurations

Requester	Web
VLAN	1 (CPU VLAN)
Timeout Threshold	3 (min)
Alarm Threshold	100 (sec)
Warning Threshold	70 (sec)
Max. Record Size	10
Multicast Router Port	4

General Query Interval Diagnostic Statistics

Total received general query	11
Total recorded interval time	10
Total record over threshold	0
Record over alarm threshold	0
Record over warning threshold	0

General Query Interval Diagnostic Result

No.	Query Interval Time (1/100 sec)
1	6006
2	5995
3	6005
4	6003
5	5985
6	6022
7	5977
8	6022
9	5982
10	6005

System Status: Displays the current status of the system.

Diagnostics Status: Displays the status of the diagnostics process for the most recent diagnostic result.

User Environment Configurations: Display the settings and requester information for the most recent diagnostic result.

Requester: Displays the source initiated the most recent diagnostics.

Total received general query: Display the total number of general query packets received.

Total recorded interval time: Display the total time recorded for general query intervals.

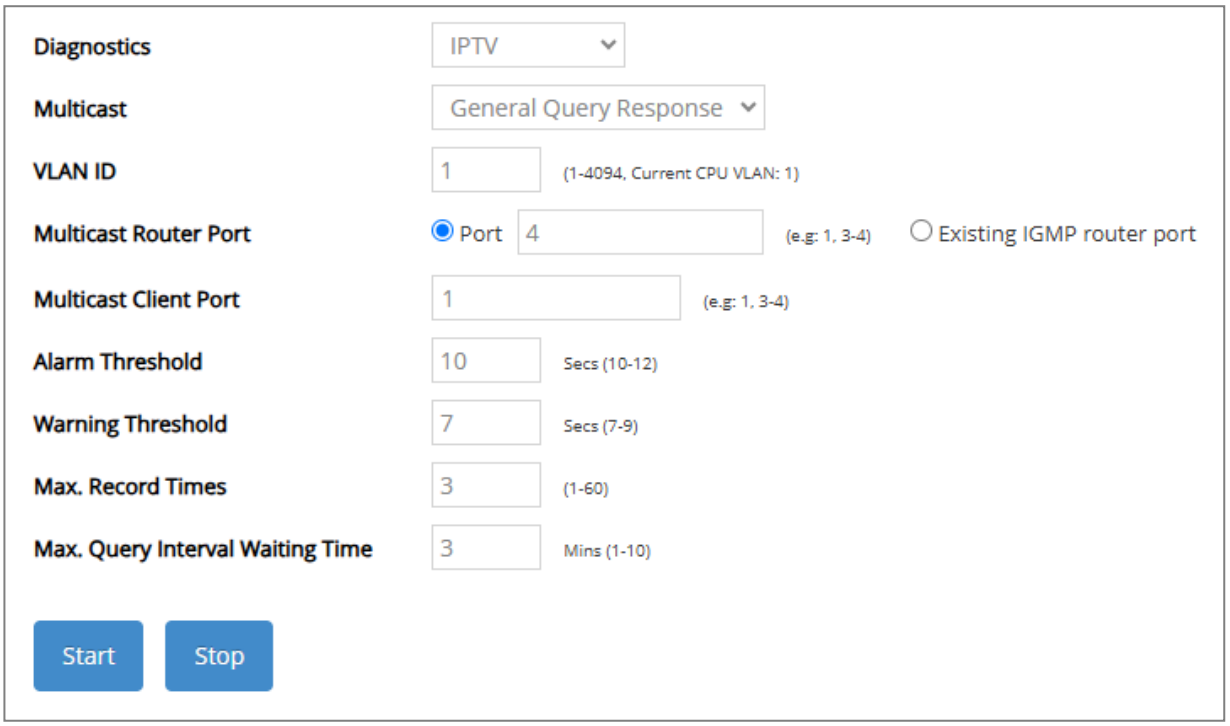
Total record over threshold: Show the total number of records exceeding the defined threshold.

Record over alarm threshold: Show the count of intervals exceeding the alarm threshold.

Record over warning threshold: Show the count of intervals exceeding the warning threshold.

General Query Interval Diagnostic Result: Display the IPTV General Query Interval diagnostic result.

4.10.1.4.5 Genaral Query Response



VLAN ID: Enter the VLAN ID to specify the diagnostic scope. The valid range is from 1 to 4094.

Multicast Router Port: Define the multicast router port by manually entering a port or selecting an existing IGMP router port.

Multicast Client Port: Specify the port used by the multicast client for receiving queries.

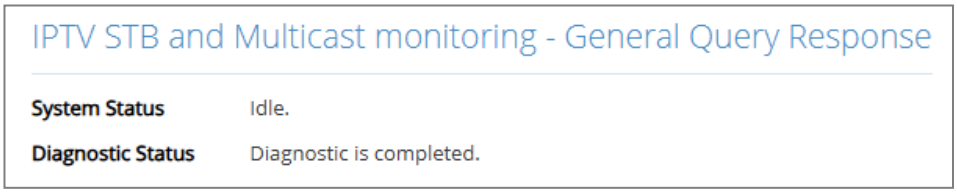
Alarm Threshold: Set the alarm threshold in seconds. The valid range is from 10 to 12.

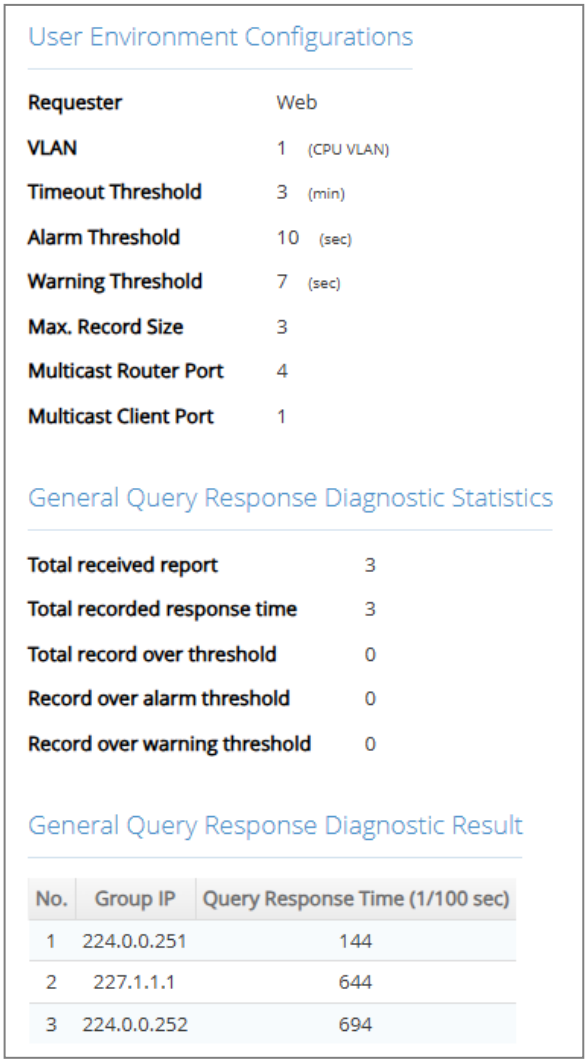
Warning Threshold: Set the warning threshold in seconds. The valid range is from 7 to 9.

Max. Record Times: Specify the maximum number of records. The valid range is from 1 to 60.

Max. Query Interval Waiting Time: Define the maximum waiting time for a query interval in minutes. The valid range is from 1 to 10.

Click **Start** to begin the diagnostic process, and click **Stop** to halt it.
The status of the diagnostic procedure, user configurations, and diagnostic results will be displayed as shown below once Start is clicked.





System Status: Displays the current status of the system.

Diagnostics Status: Displays the status of the diagnostics process for the most recent diagnostic result.

User Environment Configurations: Display the settings and requester information for the most recent diagnostic result.

Requester: Displays the source initiated the most recent diagnostics.

Total received report: Display the total number of reports received.

Total recorded response time: Display the total recorded response time for general query responses.

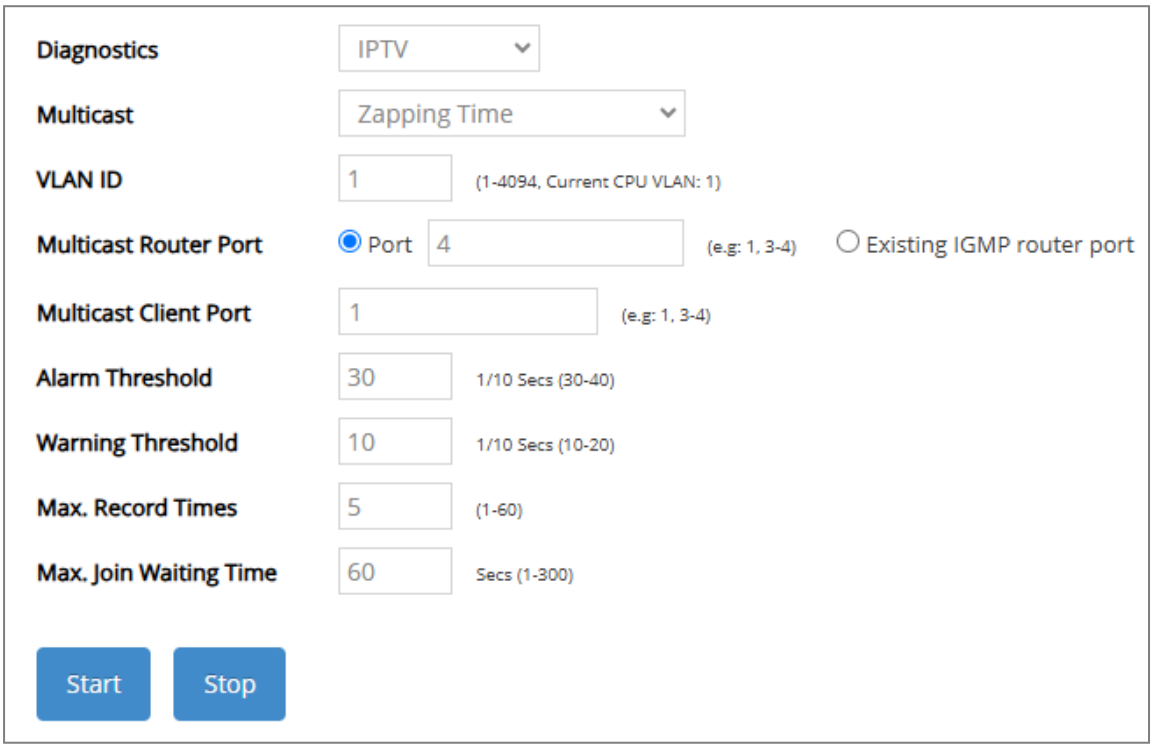
Total record over threshold: Show the total number of records exceeding the defined threshold.

Record over alarm threshold: Show the count of response times exceeding the alarm.

Record over warning threshold: Show the count of response times exceeding the warning threshold.

General Query Response Diagnostic Result: Display the IPTV General Query Response diagnostic result.

4.10.1.4.6 Zapping Time



VLAN ID: Enter the VLAN ID to specify the diagnostic scope. The valid range is from 1 to 4094.

Multicast Router Port: Define the multicast router port by manually entering a port or selecting an existing IGMP router port.

Multicast Client Port: Specify the port used by the multicast client for receiving queries.

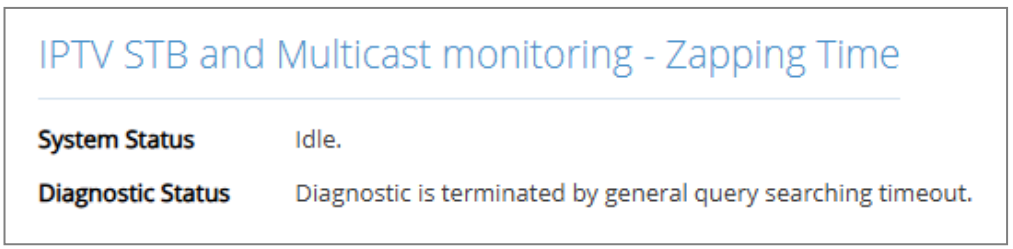
Alarm Threshold: Set the alarm threshold in seconds. The valid range is from 10 to 12.

Warning Threshold: Set the warning threshold in seconds. The valid range is from 7 to 9.

Max. Record Times: Specify the maximum number of records. The valid range is from 1 to 60.

Max. Join Waiting Time: Define the maximum join waiting time for channel switching, from sending the channel change request to receiving the stream of the new channel. The valid range is from 1 to 300 seconds.

Click **Start** to begin the diagnostic process, and click **Stop** to halt it.
The status of the diagnostic procedure, user configurations, and diagnostic results will be displayed as shown below once Start is clicked.



System Status: Display the current status of the system.

Diagnostics Status: Display the status of the diagnostics process for the most recent diagnostic result.

User Environment Configurations: Display the settings and requester information for the most recent diagnostic result.

Requester: Display the source initiated the most recent diagnostics.

Total received report: Display the total number of reports received.

Total recorded zapping time: Display the total recorded zapping time for channel switching.

Total record over threshold: Show the total number of records exceeding the defined threshold.

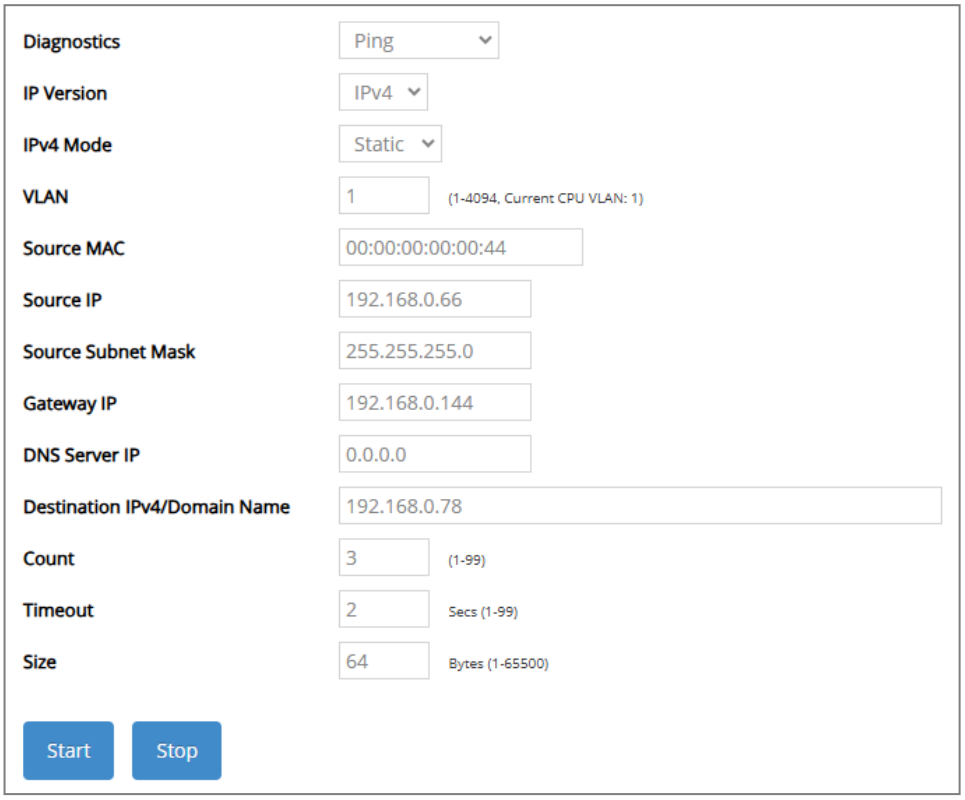
Record over alarm threshold: Show the count of records exceeding the alarm threshold.

Record over warning threshold: Show the count of records exceeding the warning threshold.

Zapping Time Diagnostic Result: Display the IPTV Zapping time diagnostic result.

4.10.1.5 Ping Diagnostics

After clicking **Ping** from the **Diagnostics** dropdown menu, the following page will appear.



IP Version: Select the IP protocol version for diagnostics. Options include IPv4 or IPv6.

IPv4/IPv6 Mode: Choose the IP assignment mode. Options include **Static** (manual IP configuration) or **DHCPv4/v6** (automatic IP assignment).

VLAN: Enter the VLAN ID to specify the diagnostic scope. The valid range is from 1 to 4094.

Source MAC: Enter the MAC address of the source device for diagnostics.

Auto Configuration Type: Select the configuration type for DHCPv6. This field is available only when DHCPv6 mode is selected.

Stateless: IP addresses are assigned without maintaining state.

Stateful: Full configuration and address assignment are managed.

Source IP: Enter the source IP address. This field is available only when Static IP mode is selected.

Source Subnet Mask: Enter the source subnet mask. This field is available only when Static IPv4 mode is selected.

Source Prefix Length: Enter the source prefix length. This field is available only when Static IPv6 mode is selected.

Gateway IP: Enter the gateway IP address. This field is available only when Static IP mode is selected.

Option 60: Enter the DHCP Option 60 value (Vendor Class Identifier). This field is available only when DHCPv4 mode is selected.

Option 15: Specify the DHCP Option 15 value. This option allows the client to request the domain name from the DHCPv6 server. This field is available only when DHCPv6 mode is selected.

Option 16: Specify the DHCP Option 16 value. This option is used to define and exchange vendor-specific information between the client and the DHCPv6 server. This field is available only when DHCPv6 mode is selected.

DNS Server IP: Enter the IP address of the DNS server for name resolution during diagnostics.

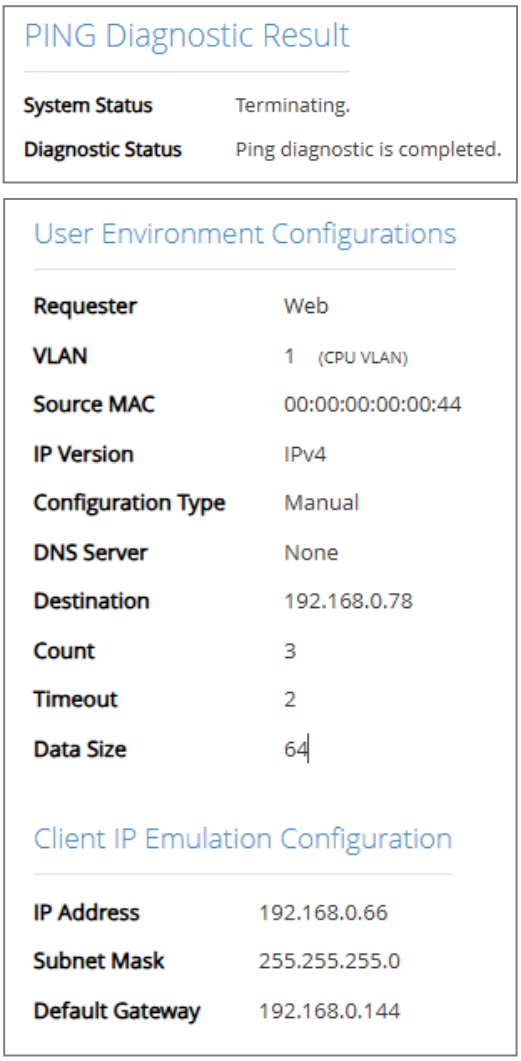
Destination IP(v4/v6)/Domain Name: Specify the target IP address (IPv4 or IPv6) or domain name to perform the ping test.

Count: Specify the number of echo requests to send. The valid range is from 1 to 99.

Timeout: Set the maximum time to wait for a reply in seconds. The valid range is from 1 to 99.

Size: Define the size of the ICMP packet to send in bytes. The valid range is from 1 to 65,500.

Click **Start** to begin the diagnostic process, and click **Stop** to halt it.
The status of the diagnostic procedure, user configurations, and diagnostic results will be displayed as shown below once **Start** is clicked.



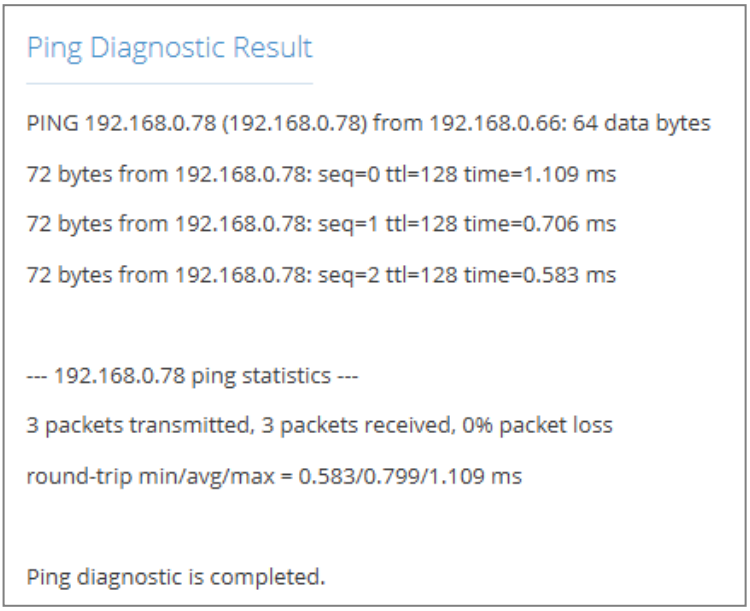
System Status: Display the current status of the system.

Diagnostics Status: Display the status of the diagnostics process for the most recent diagnostic result.

User Environment Configurations: Display the settings and requester information for the most recent diagnostic result.

Requester: Display the source initiated the most recent diagnostics.

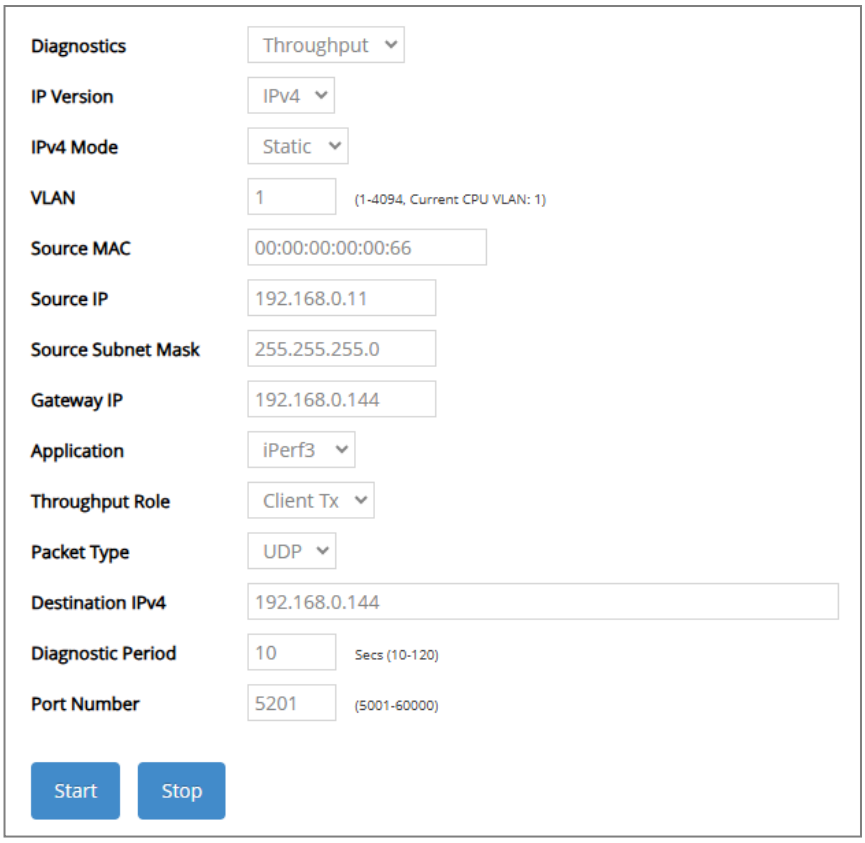
Client IP Emulation Configuration: Display the configuration details for client IP emulation, including parameters such as source IP, Default Gateway and related settings.



Ping Diagnostic Result: Display the Ping diagnostic result.

4.10.1.6 Throughput Diagnostics

After clicking **Throughput** from the **Diagnostics** dropdown menu, the following page will appear.



IP Version: Select the IP protocol version for diagnostics. Options include IPv4 or IPv6.

IPv4/IPv6 Mode: Choose the IP assignment mode. Options include **Static** (manual IP configuration) or **DHCPv4/v6** (automatic IP assignment).

VLAN: Enter the VLAN ID to specify the diagnostic scope. The valid range is from 1 to 4094.

Source MAC: Enter the MAC address of the source device for diagnostics.

Auto Configuration Type: Select the configuration type for DHCPv6. This field is available only when DHCPv6 mode is selected.

Stateless: IP addresses are assigned without maintaining state.

Stateful: Full configuration and address assignment are managed.

Source IP: Enter the source IP address. This field is available only when Static IP mode is selected.

Source Subnet Mask: Enter the source subnet mask. This field is available only when Static IPv4 mode is selected.

Source Prefix Length: Enter the source prefix length. This field is available only when Static IPv6 mode is selected.

Gateway IP: Enter the gateway IP address. This field is available only when Static IP mode is selected.

Option 60: Enter the DHCP Option 60 value (Vendor Class Identifier). This field is available only when DHCPv4 mode is selected.

Option 15: Specify the DHCP Option 15 value to request domain name settings. This field is available only when DHCPv6 mode is selected.

Option 16: Specify the DHCP Option 16 value for vendor-specific configuration. This field is available only when DHCPv6 mode is selected.

Application: Select the diagnostic tool for throughput measurement. Available options include **iPerf3** and **nuttcp**.

Throughput Role: Select the role for throughput testing

Client Tx: Acts as a client transmitting data.

Client Rx: Acts as a client receiving data.

Server: Acts as a server in the throughput test.

Packet Type: Specify the type of packets for diagnostics. Options include **TCP** and **UDP**.

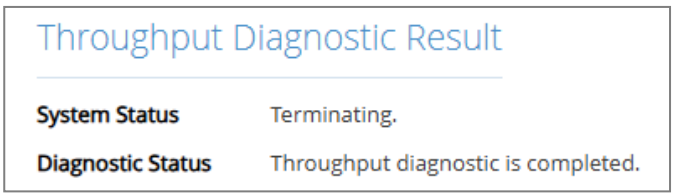
Destination IPv4/IPv6: Specify the target IP address (IPv4 or IPv6) for throughput diagnostics.

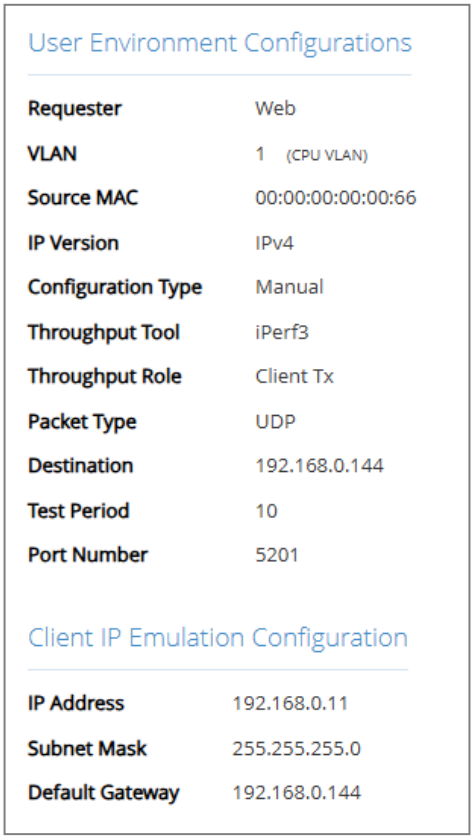
Diagnostic Period: Set the duration for the throughput test. The valid range is from 10 to 120 seconds.

Server Lifetime: Specify the duration for the server role in throughput diagnostics. The valid range is 10 to 1440 minutes. This option is available when the server is selected as the throughput role.

Port Number: Specify the port number for diagnostics. The valid range is from 5001 to 60000.

Click **Start** to begin the diagnostic process, and click **Stop** to halt it.
The status of the diagnostic procedure, user configurations, and diagnostic results will be displayed as shown below once **Start** is clicked.





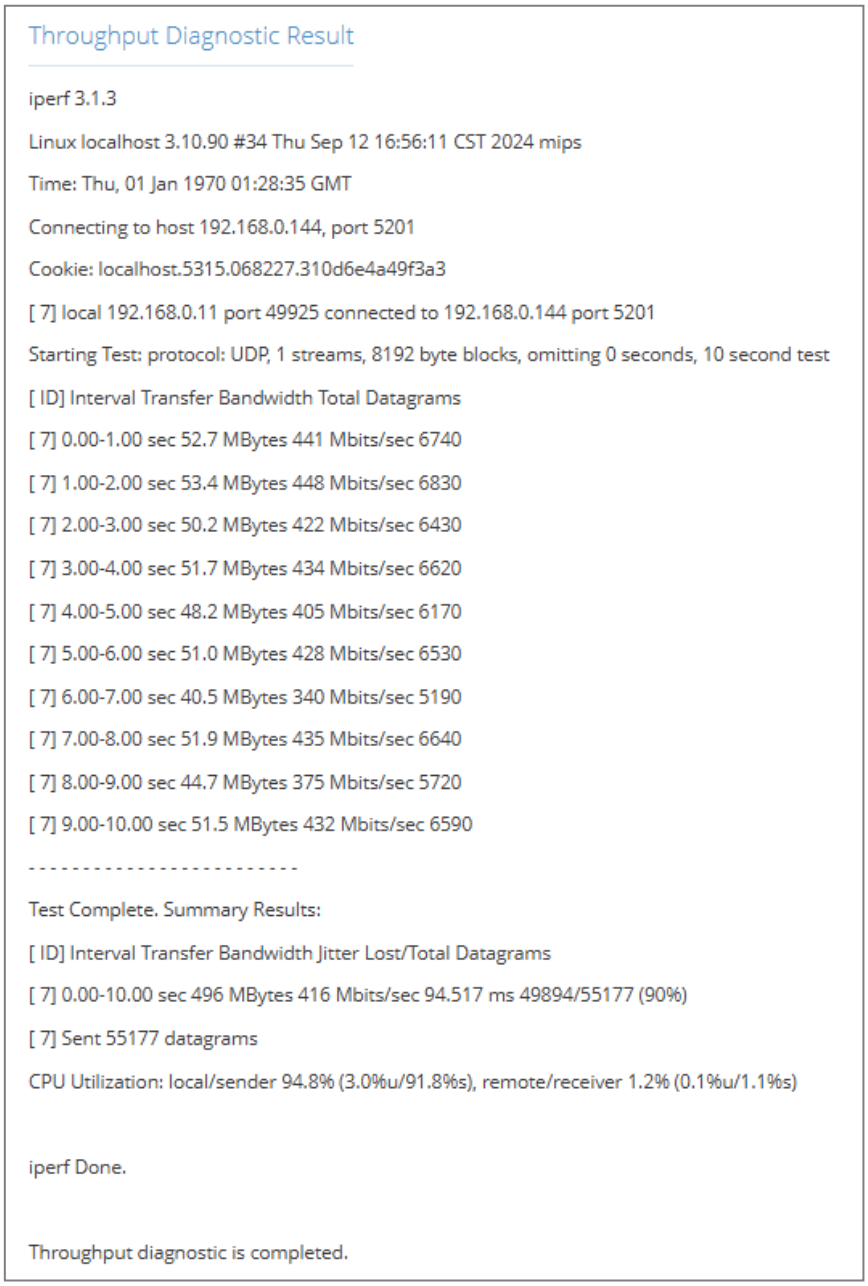
System Status: Display the current status of the system.

Diagnostics Status: Display the status of the diagnostics process for the most recent diagnostic result.

User Environment Configurations: Display the settings and requester information for the most recent diagnostic result.

Requester: Display the source initiated the most recent diagnostics.

Client IP Emulation Configuration: Display the configuration details for client IP emulation, including parameters such as source IP, Default Gateway and related settings.



Throughput Diagnostic Result: Display the Throughput diagnostic result.

4.10.2 Diagnostics Schedule

Click the option **Diagnostic Schedule** from the **Advanced Diagnostics** menu and then the following screen page appears.

Occupied/Max Entry: View-only field.

Occupied: Show the total number of schedule entries already created.

Max: Indicates the maximum number of schedule entries allowed.

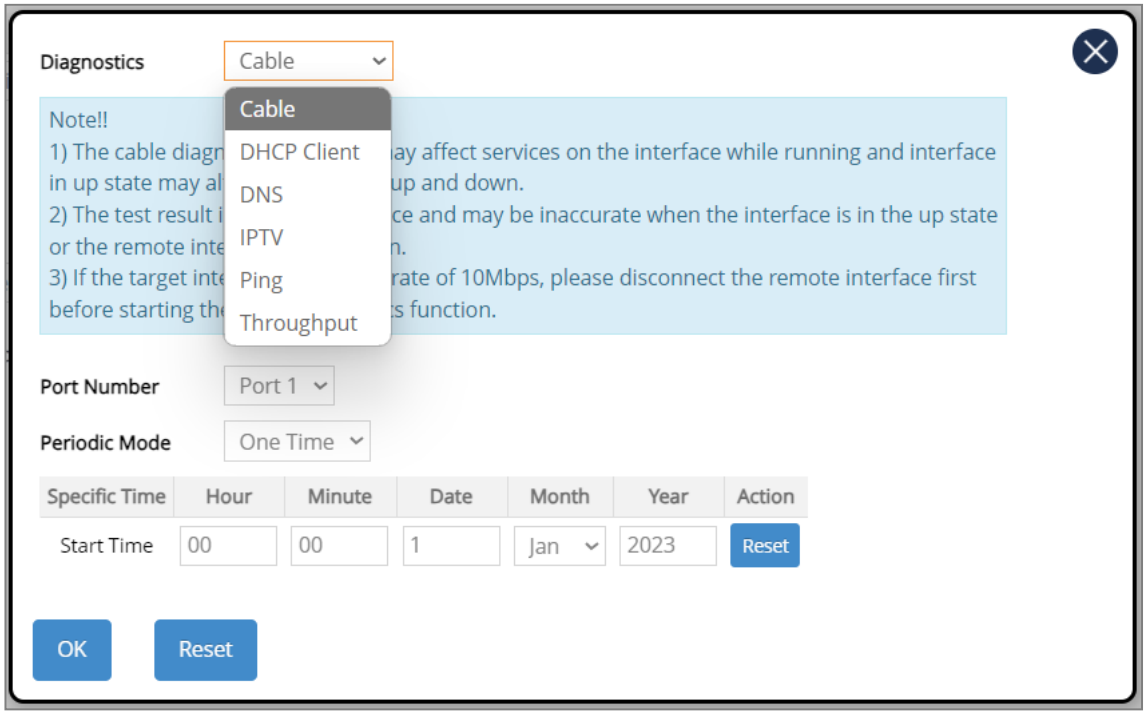
Index: The entry of the Diagnostics Schedule.

Status: Enable or Disable the diagnostics schedule for the specified index.

Diagnostics: Display the diagnostic item configured to perform for this schedule index.

Diagnostics Time: Show the scheduled time for the diagnostic task in the specified index.

Click **Add Diagnostics Schedule** to add a new schedule index. A pop-up window will then appear for further settings, as shown in the image below.



The configuration details for scheduled diagnostics are identical to those in Section 4.10.1, Network Diagnostics. Please refer to the corresponding section for more information.

Periodic Mode: Select the periodic mode for executing diagnostics for this schedule index. Available options include: **One Time**, **Daily**, **Weekly** and **Monthly**.

NOTE:
1. The NTP function must be globally enabled and synchronized with the server before operating scheduled diagnostics. Please refer to Section 4.1.4 Time Server Setup for more details
*2. The **Hour** column should be entered using 24-hour format.*

Click the **Reset button under the Action column** to revert the changes made to the currently selected **Periodic Mode**.

Click the "**Ok**" button to apply the settings, or click the "**Reset**" button to revert to the settings saved last time.

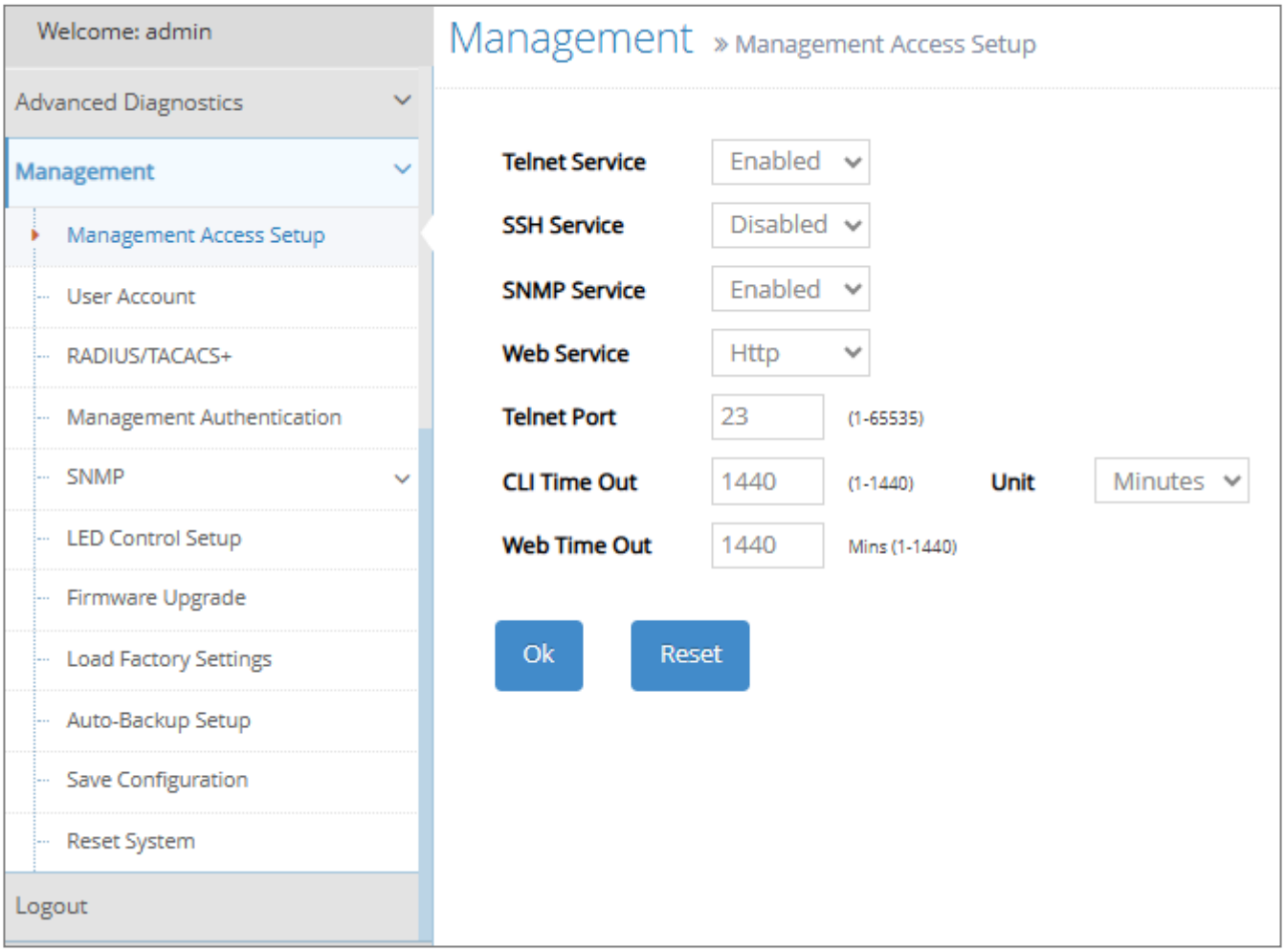
Click the icon to modify the settings of a specified community.

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

Record Status: A drop-down menu to select the specified schedule index and view its most recent diagnostic result.

4.11 Management

In order to do the firmware upgrade, load the factory default settings, etc. for the Managed Switch, please click the folder **Management** from the **Main Menu** and then 11 options will be displayed for your selection.



1. **Management Access Setup:** Enable or disable the specified network services

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

3. **RADIUS/TACACS+:** Set up the RADIUS/TACACS+ server authentication method against which a user accessing the Managed Switch can be authenticated.

4. **Management Authentication:** Set up a planned authentication scheme to be accordingly applied by the Managed Switch authenticating a user's credentials.

5. **SNMP:** Allow administrator to configure password and encryption method of user accounts generated in User Account for SNMPv3; view the registered SNMP community name list, add a new community name or remove an existing community name; view the registered SNMP trap destination list, add a new trap destination or remove an existing trap destination; view the Managed Switch trap configuration, enable or disable a specific trap.

6. **LED Control Setup:** Toggle between the on and off state of the LED status light.

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

8. **Load Factory Settings:** Load Factory Setting will reset the configuration including or excluding the IP and Gateway addresses of the Managed Switch back to the factory default settings.

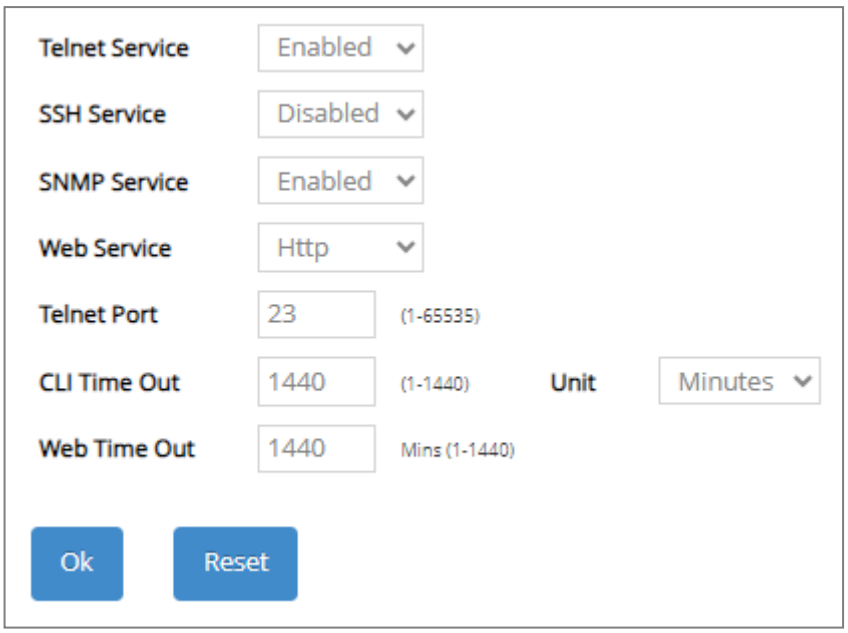
9. **Auto-Backup Setup:** Allows users to set up automatic backups for the managed switch settings.

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

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

4.11.1 Management Access Setup

Click the option **Management Access Setup** from the **Management** menu and then the following screen page appears.



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

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

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

Web Service: To enable or disable the Web Management service. Either **Http** or **Https** option can be selected to enable this service. The difference between these two options is as follows:

- When the **Http** option is chosen, the user is allowed to access the Managed Switch only by inputting its IP address with the format of http://192.168.0.1 in URL.

- When the **Https** option is chosen, this communication protocol is encrypted using Transport Layer Security(TLS) or Secure Sockets Layer (SSL) for secure communication over a computer network. 335 HTTPS is provided for authentication of the accessed website and protection of the privacy and integrity of the exchanged data while in transit. It protects against attacks by hackers. The user is allowed to access the Managed Switch either by inputting its IP address with the format of https://192.168.0.1

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

CLI Time Out: Specify the desired time that the Managed Switch will wait before disconnecting an inactive telnet/ssh session. Valid range:1-1440 seconds or minutes.

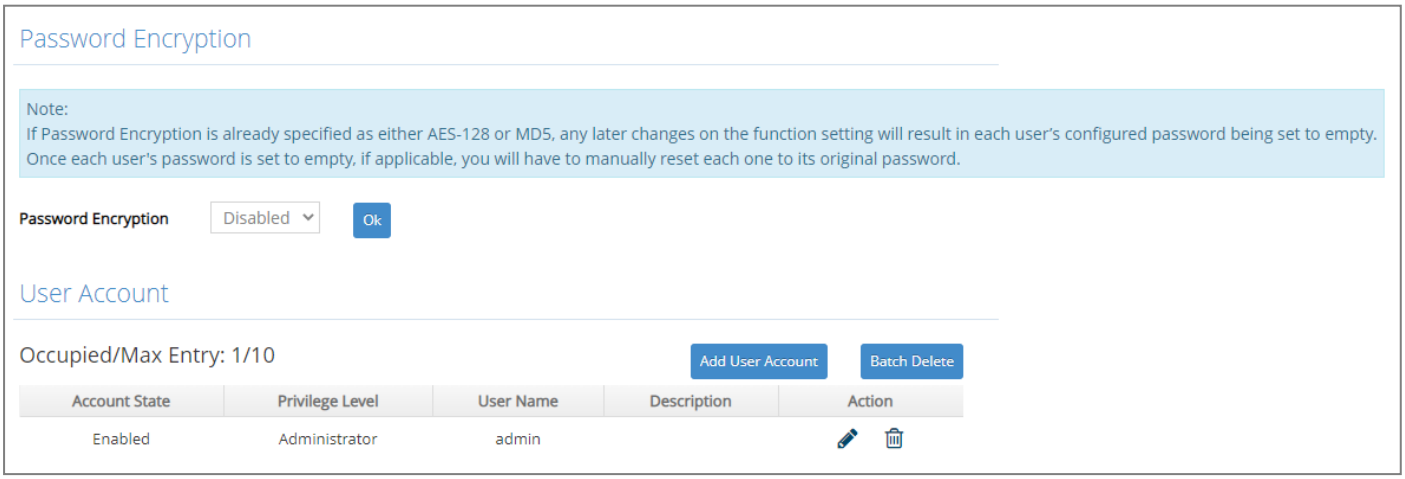
Unit: Specify the unit for the **System Time Out** parameter.

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

4.11.2 User Account

To prevent any unauthorized operations, only registered users are allowed to operate the Managed Switch. Users who would like to operate the Managed Switch need to create a user account first.

To view or change current registered users, select the option **User Account** from the **Management** menu and then the following screen page shows up.



Password Encryption: Pull down the menu of **Password Encryption** to select one method to secure the password against potential malicious attacks.

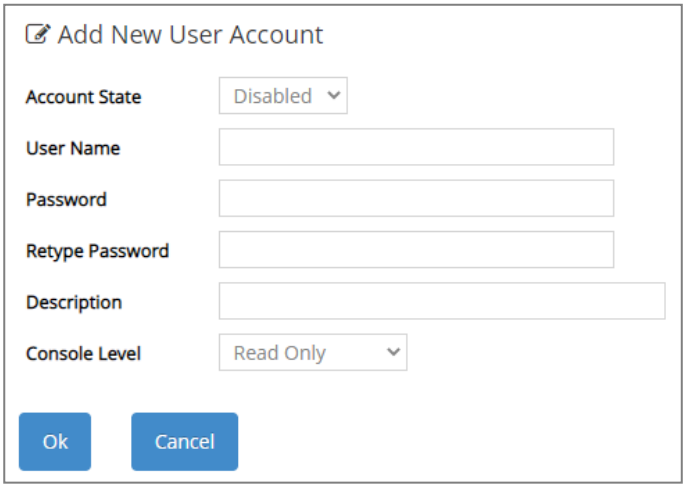
> **None:** Disable the password encryption function. Select “None” from the pull-down menu to disable it.
>
> **AES-128 (Advanced Encryption Standard):** An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data. Select “AES-128” from the pull-down menu to enable this password encryption method.

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

Occupied/Max Entry: View-only field.

> **Occupied:** This shows the amount of total users who have already registered.
>
> **Max:** This shows the maximum number available for the user registration. The maximum number is 10.

Click **Add User Account** to add a new user and then the following screen page appears for the further user registration settings.



Account State: Enable or disable this user account.

User Name: Specify the authorized user login name. Up to 32 alphanumeric characters can be accepted.

Password: Enter the desired user password. Up to 64 alphanumeric characters can be accepted.

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

Description: Enter a unique description for this user. Up to 35 alphanumeric characters can be accepted. This is mainly used for reference only.

Console Level: Select the desired privilege level for the management operation from the pull-down menu. Three operation levels of privilege are available in Managed Switch:

> **Administrator:** Own the full-access right. The user can maintain user account as well as system information, load the factory default settings, and so on.
>
> **Read & Write:** Own the partial-access right. The user is unable to modify user account and system information, do the firmware upgrade, load the factory default settings, and set up auto-backup.
>
> **Read Only:** Allow to view only.

Click the icon to modify the settings of a registered user you specify.

Click the icon to remove the selected registered user account from the user list. Or click **Batch Delete** to remove a number of /all user accounts at a time by clicking on the checkbox belonging to the corresponding user in the **Action** field and then click **Delete Select Item**, the selected user(s) will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

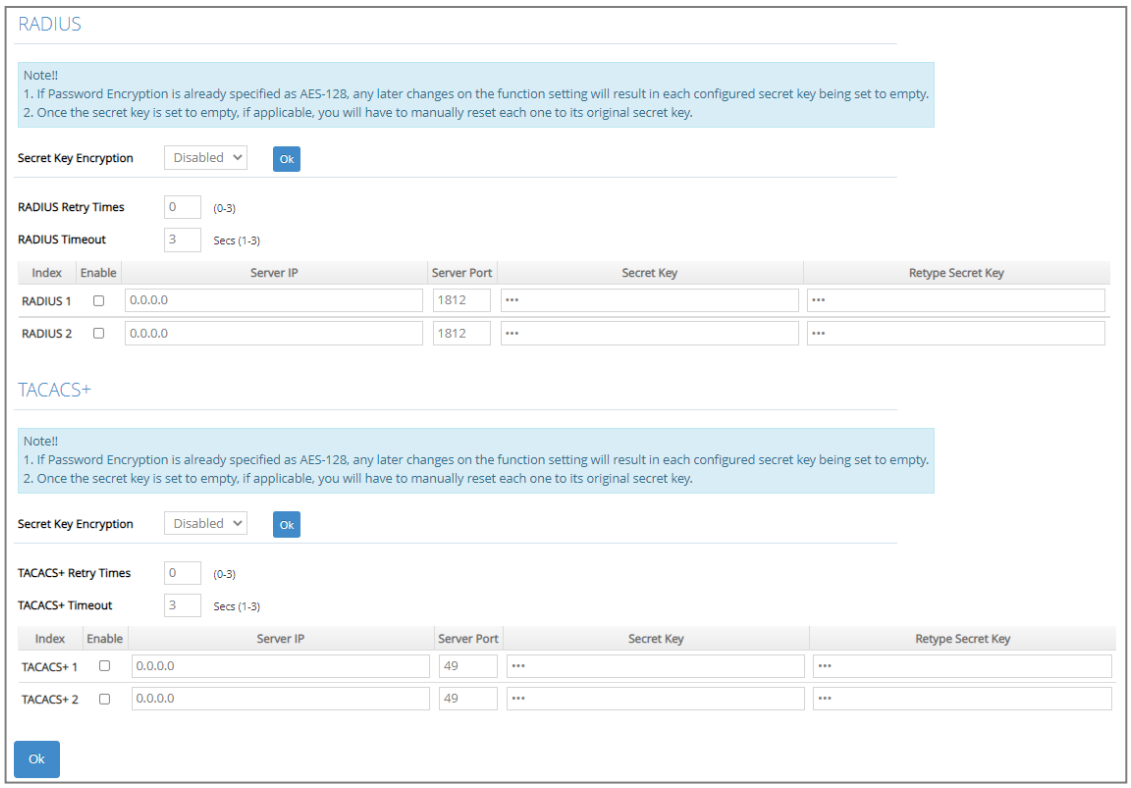
NOTE:

1. *To prevent incautious operations, users cannot delete their own account, modify their own user name and change their own account state.*
2. *The acquired hashed password from backup config file is not applicable for user login on CLI/Web interface.*
3. *We strongly recommend not to alter off-line Auth Method setting in backup configure file.*
4. *If Auth-Method is enabled and do firmware downgrade, users must reset default config.*

4.11.3 RADIUS/TACACS+

RADIUS and TACACS+ are namely two protocols used in the centralized management over the access into the network mainly for preventing the unauthorized connection, both working under the framework AAA (authentication, authorization, and accounting). The first “A” denotes that a RADIUS/TACACS+ client is required to transmit its username and its password for the authentication against the RADIUS/TACACS+ server. If the credentials are valid, the access-accept message will then be sent, and the client at this point will gain the approval of access into the Managed Switch, which in return delivers effective protection against unauthorized operation from malicious users.

To configure RADIUS/TACACS+, select the option **RADIUS/TACACS+** from the **Management** menu and then the following screen page shows up.



RADIUS: Configure the RADIUS server authentication method.

Secret Key Encryption: Pull down the menu of **Secret Key Encryption** to select one method to secure the secret key against potential malicious attacks.

None: Disable the secret key encryption function. Select “None” from the pull-down menu to disable it.

AES-128 (Advanced Encryption Standard): An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data. Select “AES-128” from the pull-down menu to enable the secret key encryption method.

1. **RADIUS Retry Times:** The maximum number of attempts to reconnect if the RADIUS server is not reachable. Valid values are 0 through 3.

2. **RADIUS Timeout:** The amount of time (second) that the Managed Switch will wait if the RADIUS server is not responding. Valid values are 1 through 3.

3. **Index:** The entry of the RADIUS servers. Up to 2 servers can be configured as the RADIUS authentication server.

4. **Enable:** Click the checkbox of the intended RADIUS server to enable RADIUS authentication. Once it's enabled, the user login will be upon those settings on the RADIUS server.

5. **Server IP:** The IPv4/IPv6 address of the RADIUS server.

6. **Server Port:** The RADIUS service port on the RADIUS server. Valid values are 1025 through 65535.

7. **Secret Key:** The secret key for the RADIUS server; it is used to validate communications with the RADIUS server. Up to 32 alphanumeric characters can be set up.

8. **Retype Secret Key:** Enter the secret key again for double-checking.

NOTE: *For FreeRADIUS server setup, please refer to APPENDIX A for the creation of CTS vendor-specific dictionary and modification of the configuration files.*

TACACS+: Configure the TACACS+ server authentication method.

Secret Key Encryption: Pull down the menu of **Secret Key Encryption** to select one method to secure the secret key against potential malicious attacks.

None: Disable the secret key encryption function. Select "None" from the pull-down menu to disable it.

AES-128 (Advanced Encryption Standard): An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data. Select "AES-128" from the pull-down menu to enable the secret key encryption method.

1. **TACACS+ Retry Times:** The maximum number of attempts to reconnect if the TACACS+ server is not reachable. Valid values are 0 through 3.

2. **TACACS+ Timeout:** The amount of time (second) that the Managed Switch will wait if the TACACS+ server is not responding. Valid values are 1 through 3.

3. **Index:** The entry of the TACACS+ servers. Up to 2 servers can be configured as the TACACS+ authentication server.

4. **Enable:** Click the checkbox of the intended TACACS+ server to enable TACACS+ authentication. Once it's enabled, the user login will be upon those settings on the RADIUS server.

5. **Server IP:** The IPv4/IPv6 address of the TACACS+ server.

6. **Server Port:** The TACACS+ service port on the TACACS+ server. Valid values are 49, and 1025 through 65535.

7. **Secret Key:** The secret key for the TACACS+ server; it is used to validate communications with the TACACS+ server. Up to 32 alphanumeric characters can be set up.

8. **Retype Secret Key:** Enter the secret key again for double-checking.

4.11.4 Management Authentication

Management Authentication makes possible the versatile approaches to authentication on the Managed Switch. Network administrators can opt for multiple authentication methods and prioritize them in accordance with their most desired plan. This function brings not only enhanced flexibility to the authentication management, but also a smart countermeasure for an unexpected user authentication failure.

To configure the authentication method, select the option **Management Authentication** from the **Management** menu and then the following screen page shows up.

Service: The interfaces via which the user accesses the Managed Switch, including **All**, **Telnet**, **SSH** and **Web**.

> **All:** Every user accessing the Managed Switch will be authenticated against the same authentication method scheme, regardless of the interface adopted by the user.

Method 1-5: Select **Local**, **RADIUS 1**, **RADIUS 2**, **TACACS+ 1**, **TACACS+ 2,** or **Disable** from each Method's pull-down menu to form a chain of authentication methods. However, **Local** must be set after **RADIUS** and **TACACS+** servers throughout the specified method scheme, and the 1st method cannot be configured as **Disable**.

> **Local:** The user information stored in the Managed Switch against which the user will be authenticated when accessing the Managed Switch.
>
> **RADIUS 1/2:** The RADIUS server against which the user will be authenticated when accessing the Managed Switch.
>
> **TACACS+ 1/2:** The TACACS+ server against which the user will be authenticated when accessing the Managed Switch.

Continue To Next Method When Authentication Fail: Select **Enabled** or **Disabled** from the pull-down menu to enable or disable the function.

Note:
1. *Once this function is enabled, the Managed Switch will continue to the next method if Method 1 fails, say, due to invalid client credentials. It indeed delivers extra flexibility for an ought-to-be-authenticated user, yet at the expense of network security. To fully protect*

against malicious users, it's recommended to set this function disabled.

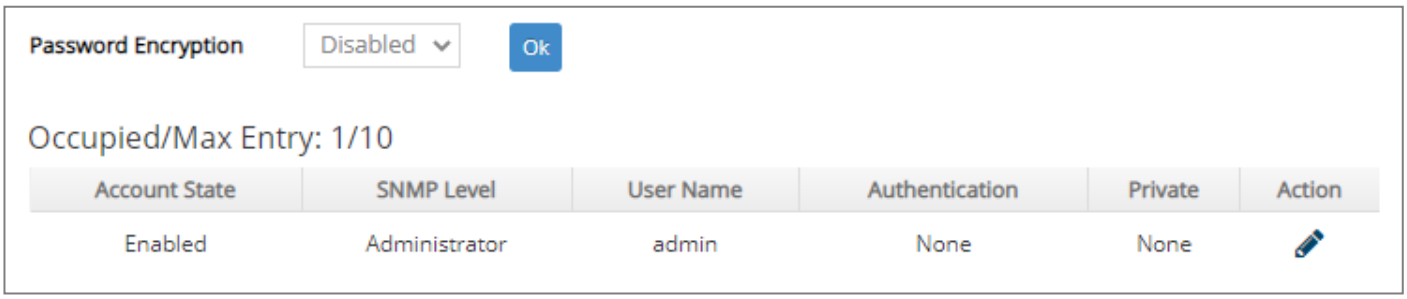
2. Disabling this function means the device will only apply Method 1. Access to the Managed Switch will be denied to those who fail the authentication with Method 1.

4.11.5 SNMP

Select the option **SNMP** from the **Management** menu and then four functions, including SNMPv3 USM User, Device Community, Trap Destination and Trap Setup will be displayed for your selection.

4.11.5.1 SNMPv3 USM User

Simple Network Management Protocol Version 3, SNMPv3 in short, features stronger security mechanism, including authentication and encryption that helps ensure that the message is from a valid source and scramble the content of a packet, to prevent from being learned by an unauthorized source. The following screen page appears if you choose **SNMPv3 USM User** function.



Password Encryption: Pull down the menu of **Password Encryption** to select one method to secure the password against potential malicious attacks.

None: Disable the password encryption function. Select "None" from the pull-down menu to disable it.

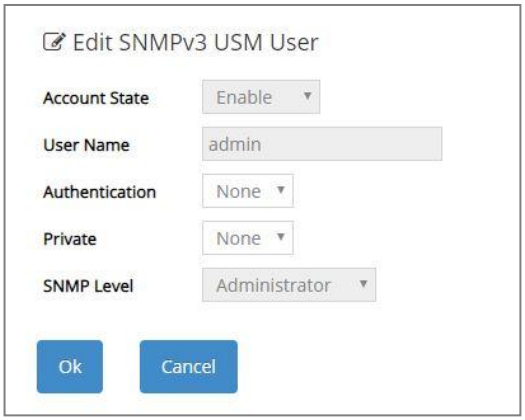
AES-128 (Advanced Encryption Standard): An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data. Select "AES-128" from the pull-down menu to enable this password encryption method.

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total registered communities.

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

Click the icon to modify the SNMPv3 USM User settings for a registered user.



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

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

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

> **None:** Disable authentication function. Select “None” from the pull-down menu to disable it.
>
> **MD5 (Message-Digest Algorithm):** A widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32-digit hexadecimal number. Select “MD5” from the pull-down menu to enable this authentication.
>
> **SHA (Secure Hash Algorithm):** A 160-bit hash function which resembles the said MD5 algorithm. Select “SHA” from the pull-down menu to enable this authentication.

Authentication-Password: Specify the passwords if “MD5” or “SHA” is chosen. Up to 20 characters can be accepted.

Retype Authentication-Password: Enter again the passwords specified in the **Authentication-Password** field.

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

> **None:** Disable Private function. Select “None” from the pull-down menu to disable it.
>
> **DES (Data Encryption Standard):** An algorithm to encrypt critical information such as message text message signatures, etc. Select “DES” from the pull-down menu to enable it.
>
> **AES-128 (Advanced Encryption Standard):** An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data. Select “AES128” from the pull-down menu to enable it.

Private-Password: Specify the passwords if “DES” is chosen. Up to 20 characters can be accepted.

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

> **Administrator:** Own the full-access right, including maintaining user account & system information, load factory settings …etc.

Read & Write: Own the full-access right but cannot modify user account & system information, cannot load factory settings.

Read Only: Allow to view only.

A combination of a security event shown as below indicates which security mechanism is used when handling an SNMP packet.

Authentication	Private	Result
None	None	Uses a username match for authentication
Message Digest Algorithm(MD5) or Secure Hash Algorithm(SHA)	None	Enables authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms.
MD5 or SHA	Data Encryption Standard(DES)	Enables authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms. What's more, enables DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES standard.
MD5 or SHA	Advanced Encryption Standard (AES-128)	Enables authentication based on the Hashed Message Authentication Code(HMAC)-MD5 or HMAC-SHA algorithms. What's more, enables 128-bit AES encryption based on the symmetric-key algorithm.

4.11.5.2 Device Community

The following screen page appears if you choose **Device Community** function.

This table will display the overview of each configured devcie community. Up to 10 devcie communities can be registered.

Occupied/Max Entry: View-only field.

Occupied: his shows the amount of total registered communities.

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

Click **Add Device Community** to add a new community and then the following screen page appears for the further devcie community settings.

Account State: Enable or disable this Community Account.

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

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

Community: Specify the authorized SNMP community name, up to 20 alphanumeric characters.

Description: Enter a unique description for this community name. Up to 35 alphanumeric characters can be accepted. This is mainly for reference only.

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

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

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

4.11.5.3 Trap Destination

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

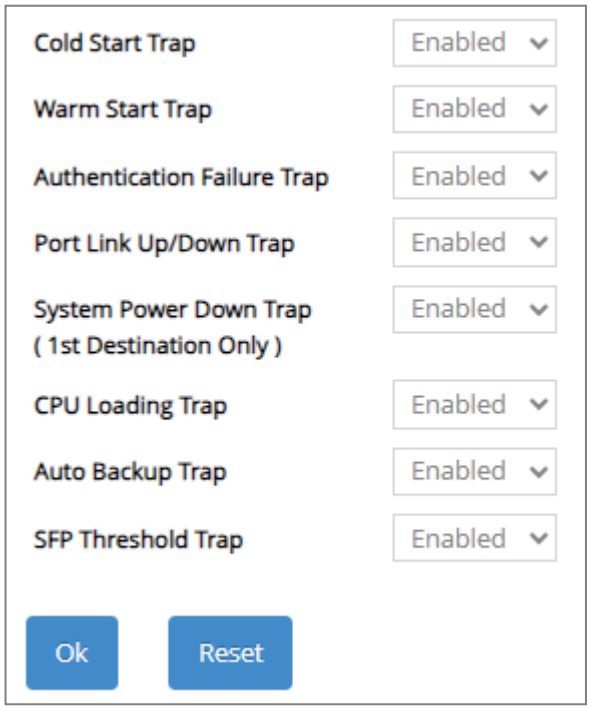
State: Enable or disable the function of sending trap to the specified destination.

Destination IP: Enter the specific IPv4/IPv6 address of the network management system that will receive the trap.

Community: Enter the description for the specified trap destination.

4.11.5.4 Trap Setup

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



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

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

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

NOTE: *The authentication failure trap is triggered only when an SNMP community error occurs. A failed login attempt using an incorrect user account on the WEB/CLI will not trigger the trap, but it will be recorded in the event log.*

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

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

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

Auto Backup Trap: Enable or disable the Managed Switch to send a trap whether the Auto Backup is successful or fail.

SFP Threshold Trap: Enable or disable Managed Switch to send a trap when Temperature/ Voltage/Current/TX Power/RX Power of SFP transceiver is over the **High** value, under the **Low** value, or returning to the normal status from abnormal status.

4.11.6 LED Control Setup

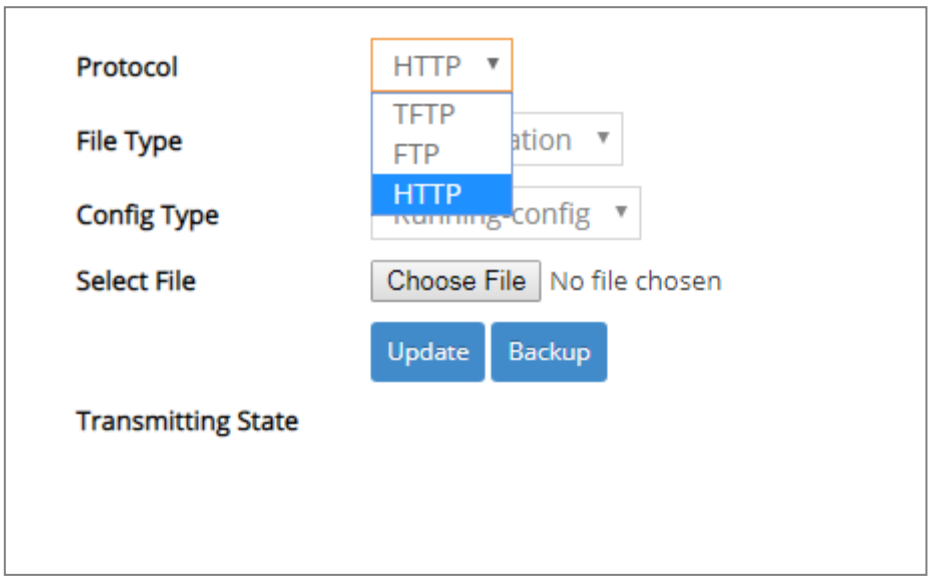
Users can turn on and off the LED status light on the top panel of the Managed Switch remotely.

To toggle between the on and off state of the LED status light, select the option **LED Control Setup** from the **Management** menu and then the following screen page shows up.

LED State: When disabled, the status light of the System Status LED and Port Link LEDs will be turned off. However, the Power LED indicator will always stay on regardless of the LED State configuration.

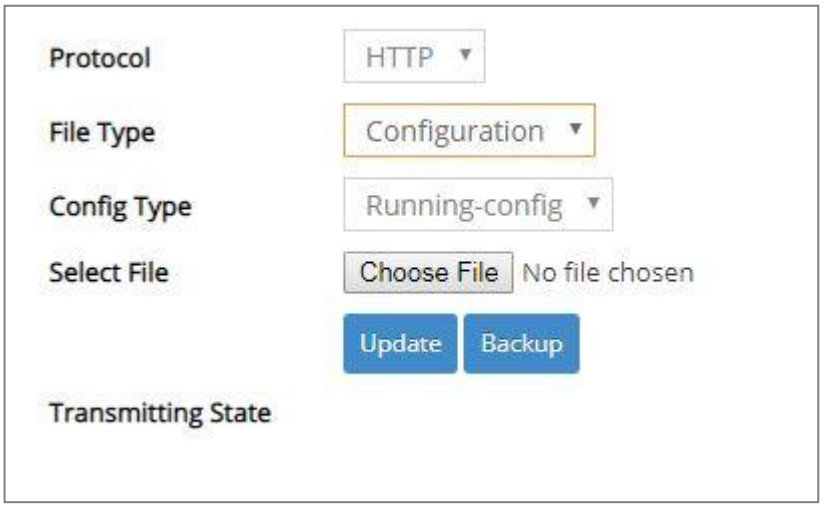
4.11.7 Firmware upgrade

The Managed Switch offers three methods, including HTTP, FTP and TFTP to back up/restore the configuration and update the firmware. To do this, please select the option **Firmware Upgrade** from the **Management** menu and then the following screen page appears.



4.11.7.1 Configuration Backup/Restore via HTTP

To back up or restore the configuration via HTTP, just pull down the **Protocol** menu and select **HTTP**. Also configure the type of file as **"Configuration"** to process. The related parameter description is as below.



Config Type: There are three types of the configuration file: Running-config, Default-config and Start-up-config.

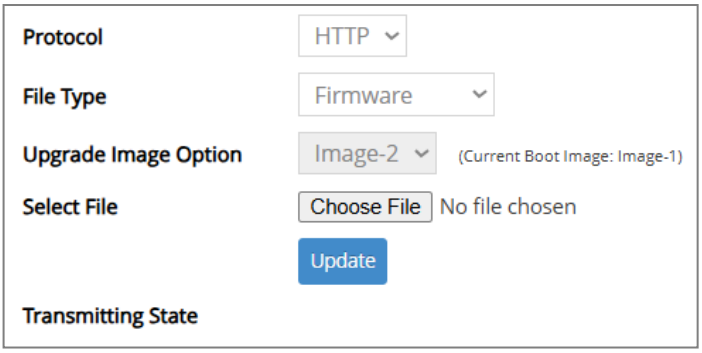
- **Running-config:** Back up the data you're processing.
- **Default-config:** Back up the data same as the factory default settings.
- **Start-up-config:** Back up the data same as last saved data.

Backup: Click **Backup** to begin download the configuration file to your PC.

Select File: Click **Choose File** to select the designated data and then click **Update** to restore the configuration.

4.11.7.2 Firmware Upgrade via HTTP

To update the firmware via HTTP, just pull down the **Protocol** menu and select **HTTP**. Also configure the type of file as **"Firmware"** to process. The related parameter description is as below.

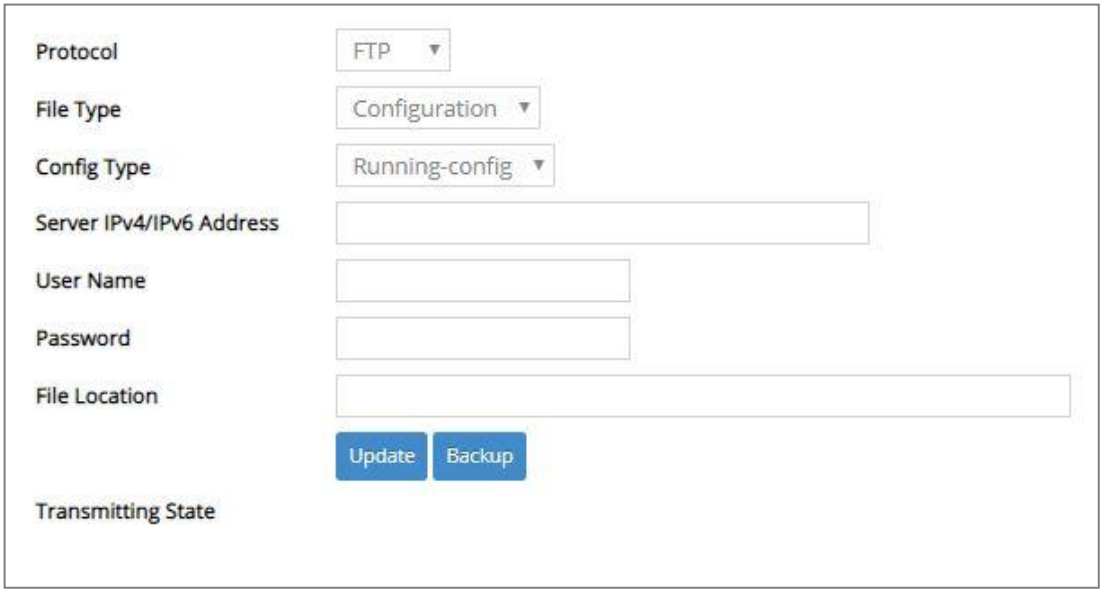


Upgrade Image Option: Display the image that will be upgraded.

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

4.11.7.3 Configuration Backup/Restore via FTP/TFTP

The Managed Switch has both built-in TFTP and FTP clients. Users may back up or restore the configuration via FTP/TFTP. Just pull down the **Protocol** menu and select **FTP** or **TFTP**, also configure the type of file as **"Configuration"** to process. The related parameter description is as below.



Protocol: Select the preferred protocol, either FTP or TFTP.

Config Type: Choose the type of the configuration file that will be saved or restored among "Running-config", "Default-config" or "Start-up-config".

Server IPv4/IPv6 Address: Enter the specific IPv4/IPv6 address of the FTP/TFTP file server.

User Name (for FTP only): Enter the specific username to access the FTP file server.

Password (for FTP only): Enter the specific password to access the FTP file server.

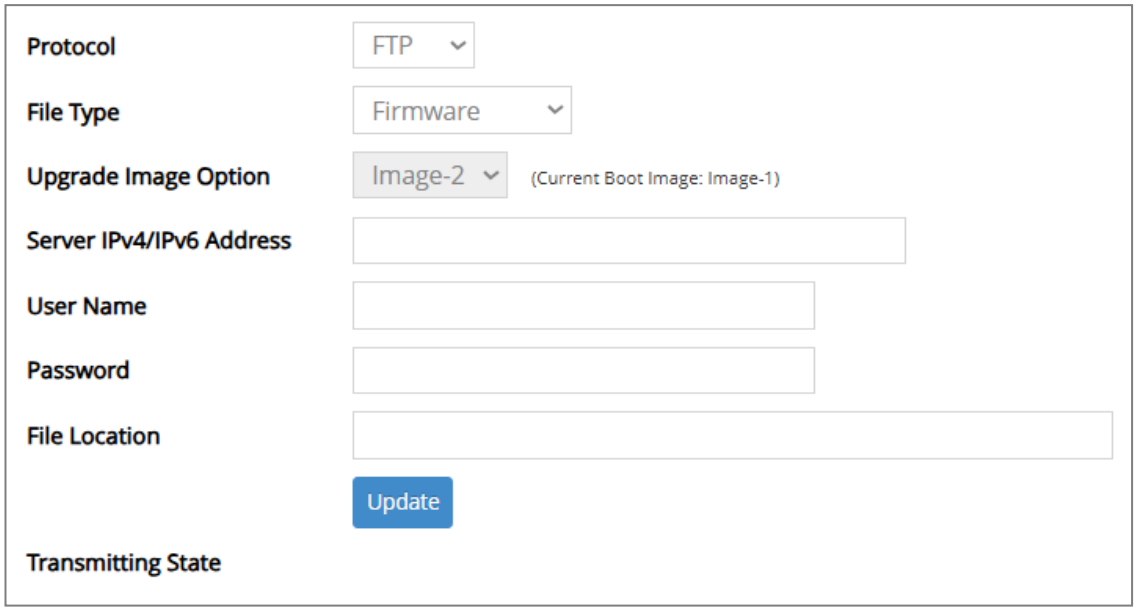
File Location: Enter the specific path and filename within the FTP/TFTP file server.

Click **Backup** to start the download process and receive files from the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind the user.

Click **Update** to start the upload process and transmit files to the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind users.

4.11.7.4 Firmware Upgrade via FTP/TFTP

The Managed Switch has both built-in TFTP and FTP clients. Users may update the firmware via FTP/TFTP. Just pull down the **Protocol** menu and select **FTP** or **TFTP**, also configure the type of file as **"Firmware"** to process. The related parameter description is as below.



Protocol: Select the preferred protocol, either FTP or TFTP.

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

Server IPv4/IPv6 Address: Enter the specific IPv4/IPv6 address of the FTP/TFTP file server.

User Name (for FTP only): Enter the specific username to access the FTP file server.

Password (for FTP only): Enter the specific password to access the FTP file server.

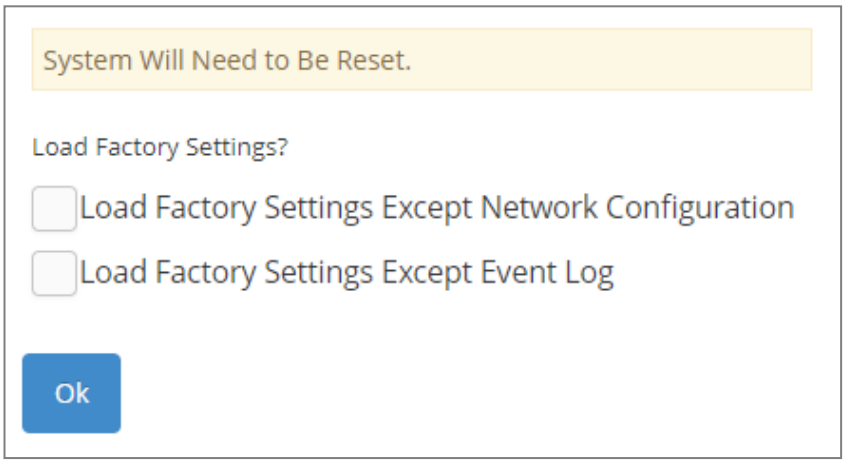
File Location: Enter the specific path and filename within the FTP/TFTP file server.

Click **Update** to start the upload process and transmit files to the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind users.

4.11.8 Load Factory Settings

Load Factory Settings will set all the configurations of the Managed Switch back to the factory default settings, including the IP and Gateway address. **Load Factory Setting** is useful when network administrators would like to re-configure the system. A system reset is required to make all changes effective after Load Factory Setting.

Select the option **Load Factory Settings** from the **Management** menu and then the following screen page appears.



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

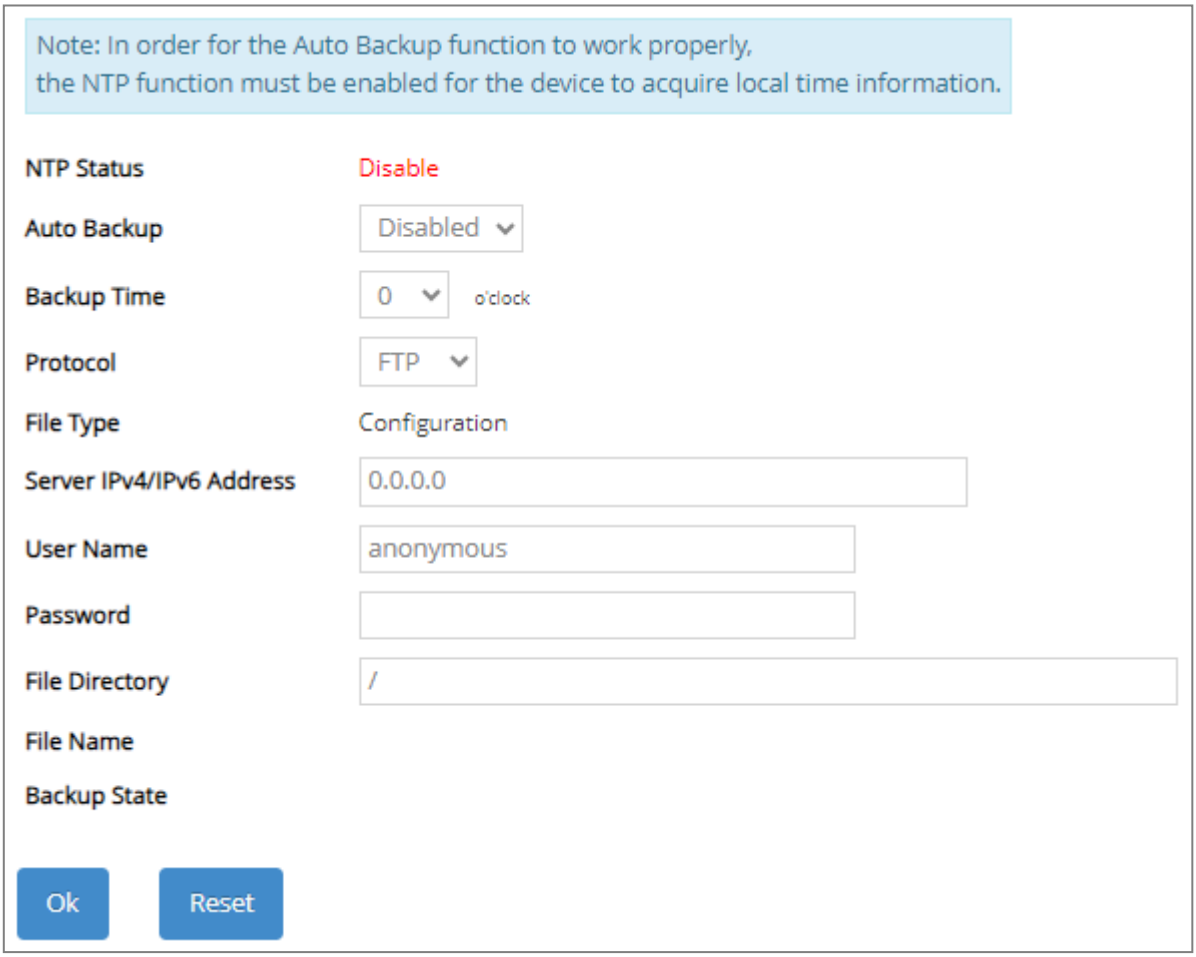
Load Factory Settings Except Event Log: It will set all the configurations of the Managed Switch back to the factory default settings except for all the event data stored in the event log. However, to ensure intact log data, the Event Record function must be enabled prior to the system resetting.

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

4.11.9 Auto-Backup Setup

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

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



NTP Status: Display the current state of NTP server. Include Disable, Inactive and active 3 states.

Disable: NTP server is disabled.

Inactive: NTP server is enabled, but the Managed Switch does not obtain the local time from NTP server.

Active: NTP server is enabled, and the Managed Switch obtains the local time from NTP server.

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

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

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

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

Server IPv4/IPv6 Address: Set up the IPv4/IPv6 address of FTP/TFTP server.

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

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

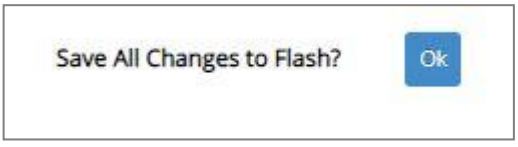
File Name: The filename assigned to the auto- backup configuration files. The format of filename generated automatically is as follows:

> **ip address_Device Name_yyyyMMdd-HHmm.txt** , for example, 192.168.0.3_SRS-3106_20240829-1600.txt

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

4.11.10 Save Configuration

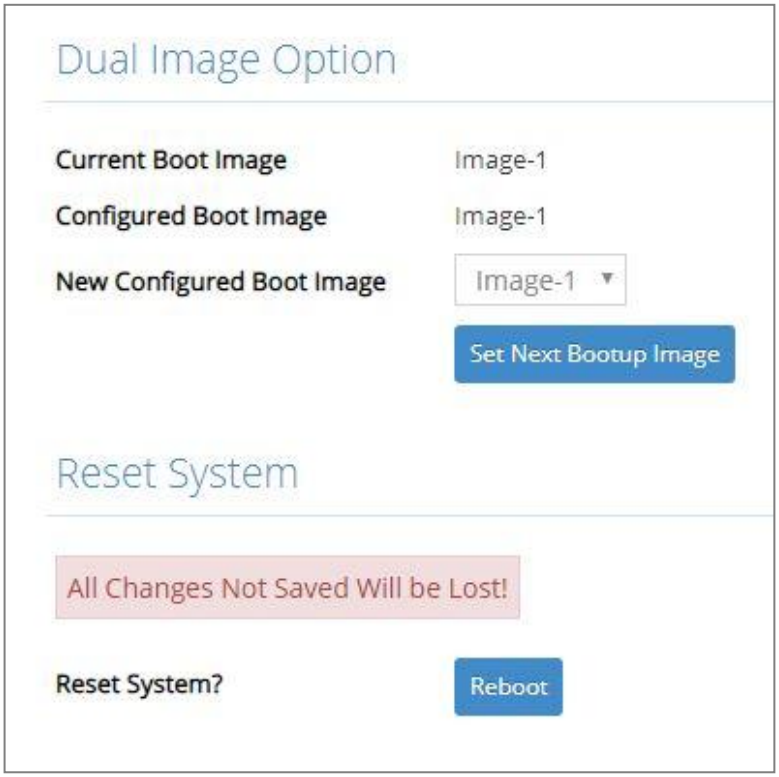
In order to save the configuration permanently, users need to save configuration first before resetting the Managed Switch. Select the option **Save Configuration** from the **Management** menu and then the following screen page appears.



Click **OK** to save the configuration. Alternatively, you can also press the **Save** quick button located on the top-right side of the webpage, which has the same function as Save Configuration.

4.11.11 Reset System

To reboot the system, please select the option **Reset System** from the **Management** menu and then the following screen page appears. From the pull-down menu of **New Configured Boot Image**, you can choose the desired image for the next system reboot if necessary.



Click **Set Next Bootup Image** to change the image into the new boot-up image you select.
Click **Reboot** to restart the Managed Switch.

APPENDIX A: FreeRADIUS Readme

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

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

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

1. Creating a CTS vendor-specific dictionary

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

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

VENDOR    cts  9304

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

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

BEGIN-VENDOR    cts

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


VALUE ACCOUNT_VALID  Valid         1
VALUE ACCOUNT_VALID  Invalid       0

VALUE ACCOUNT_STATUS    Valid          1
VALUE ACCOUNT_STATUS    Invalid        0

VALUE IP_SECURITY  Enable       1
VALUE IP_SECURITY  Disable      0
```

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

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

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

END-VENDOR  cts
```

2. Modifying three configuration files

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

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

Append the following include statement to enable dictionary-referencing:

$INCLUDE dictionary.cts

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

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

Snippet from within the "**authorize**" file:

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

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

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

Snippet from within the "**clients.conf**" file:

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

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

APPENDIX B: Set Up DHCP Auto-Provisioning

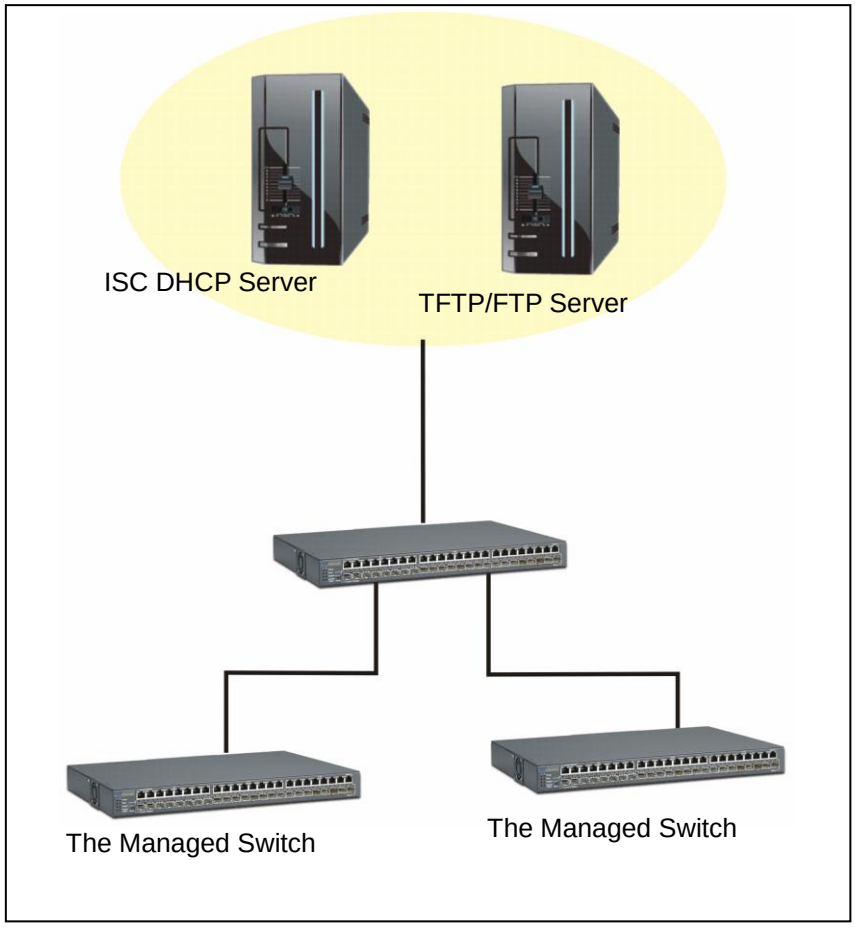
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the Managed Switch that you purchased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

A. Setup Procedures

Follow the steps below to set up Auto Provisioning server, modify dhcpd.conf file and generate a copy of configuration file.

Step 1. Set up Environment

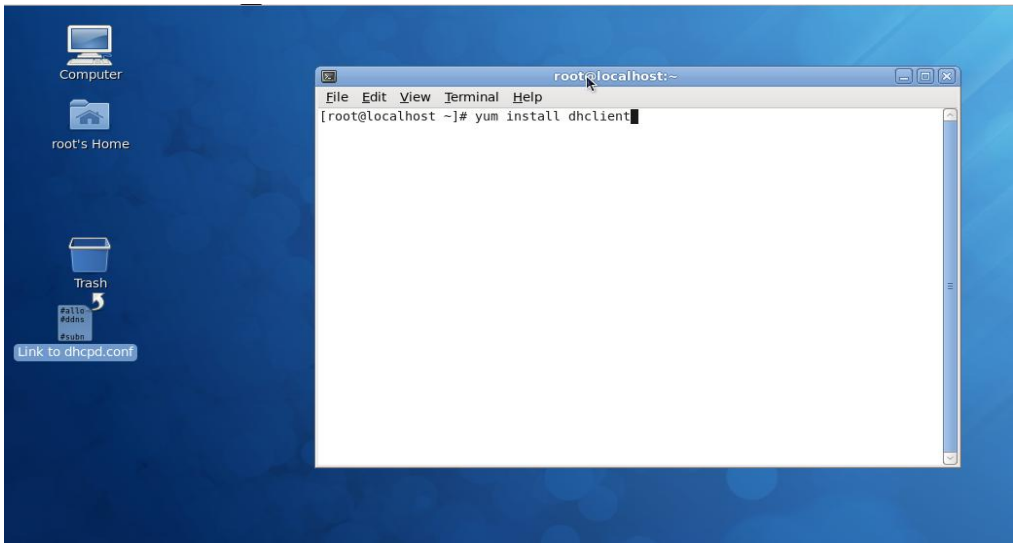
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Topology Example

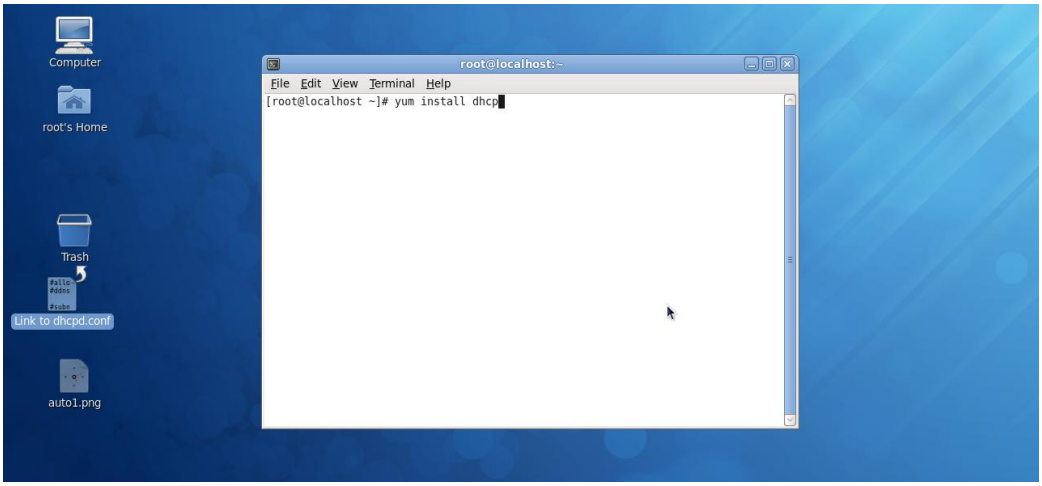
Step 2. Set up Auto Provision Server

- **Update DHCP Client**



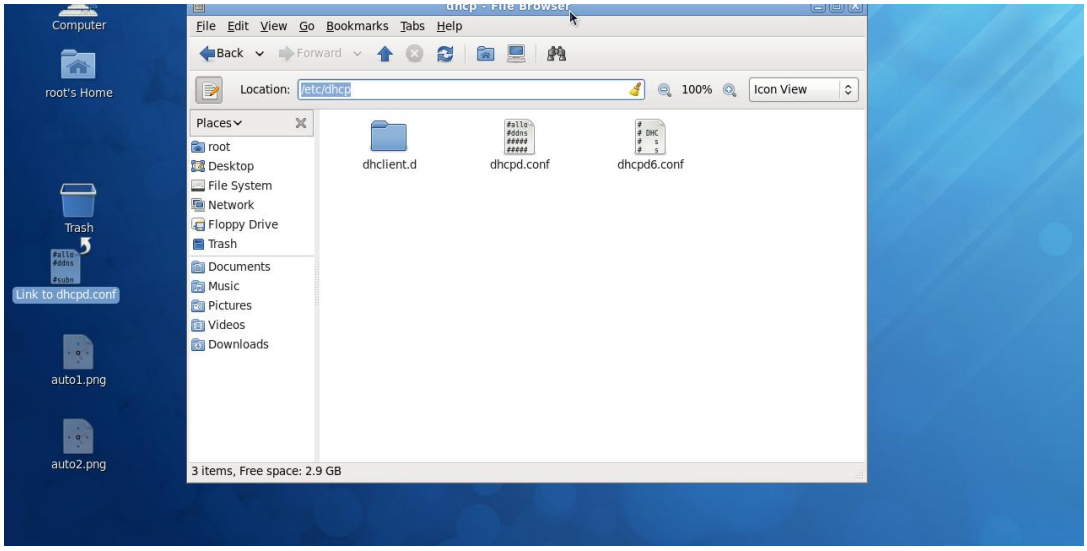
Linux Fedora 12 supports “yum” function by default. First of all, update DHCP client function by issuing “yum install dhclient” command.

- **Install DHCP Server**



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

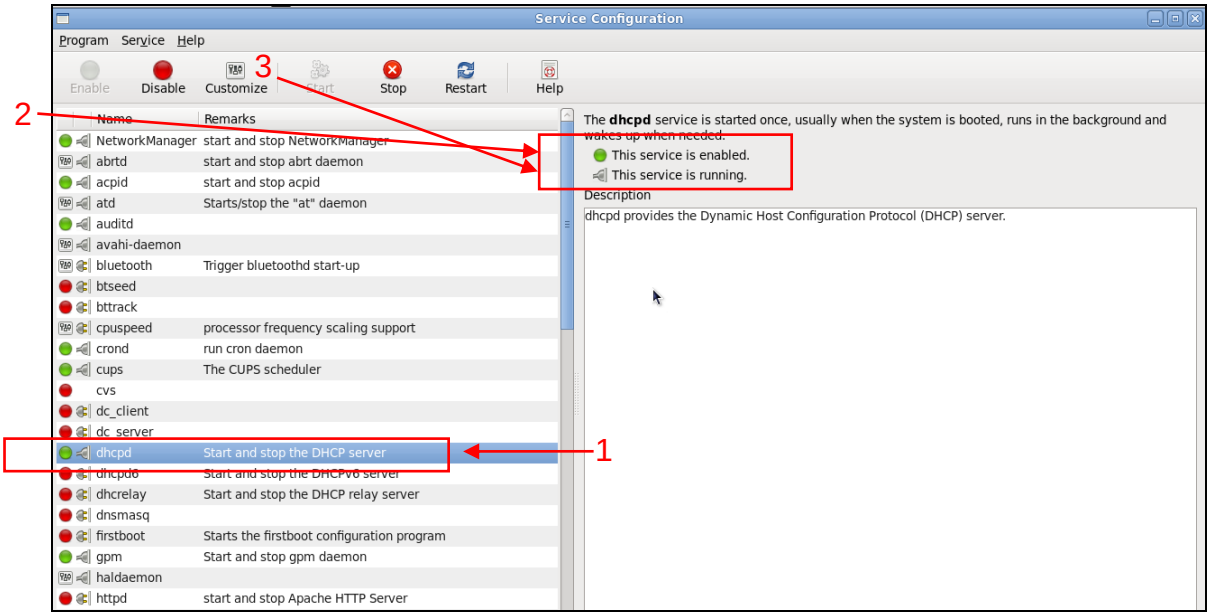
- **Copy dhcpd.conf to /etc/dhcp/ directory**



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

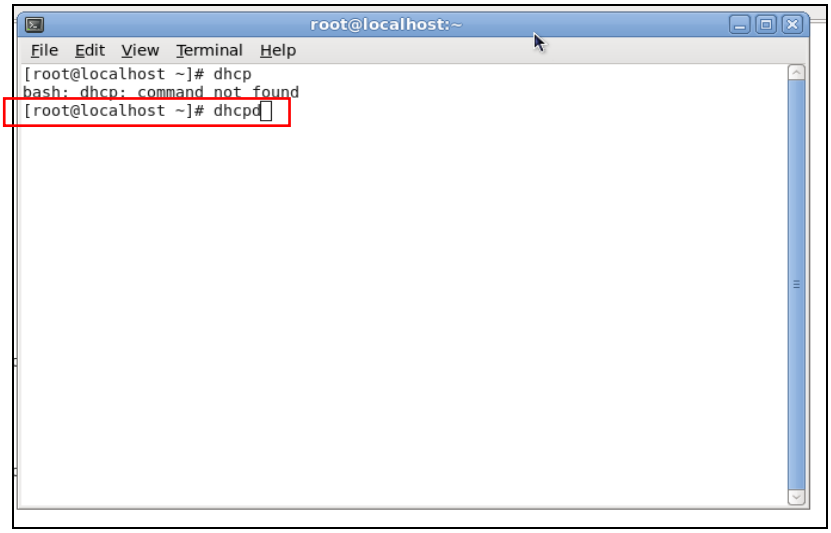
Please note that each vendor has their own way to define auto provisioning. Make sure to use the file provided by the vendor.

- **Enable and run DHCP service**



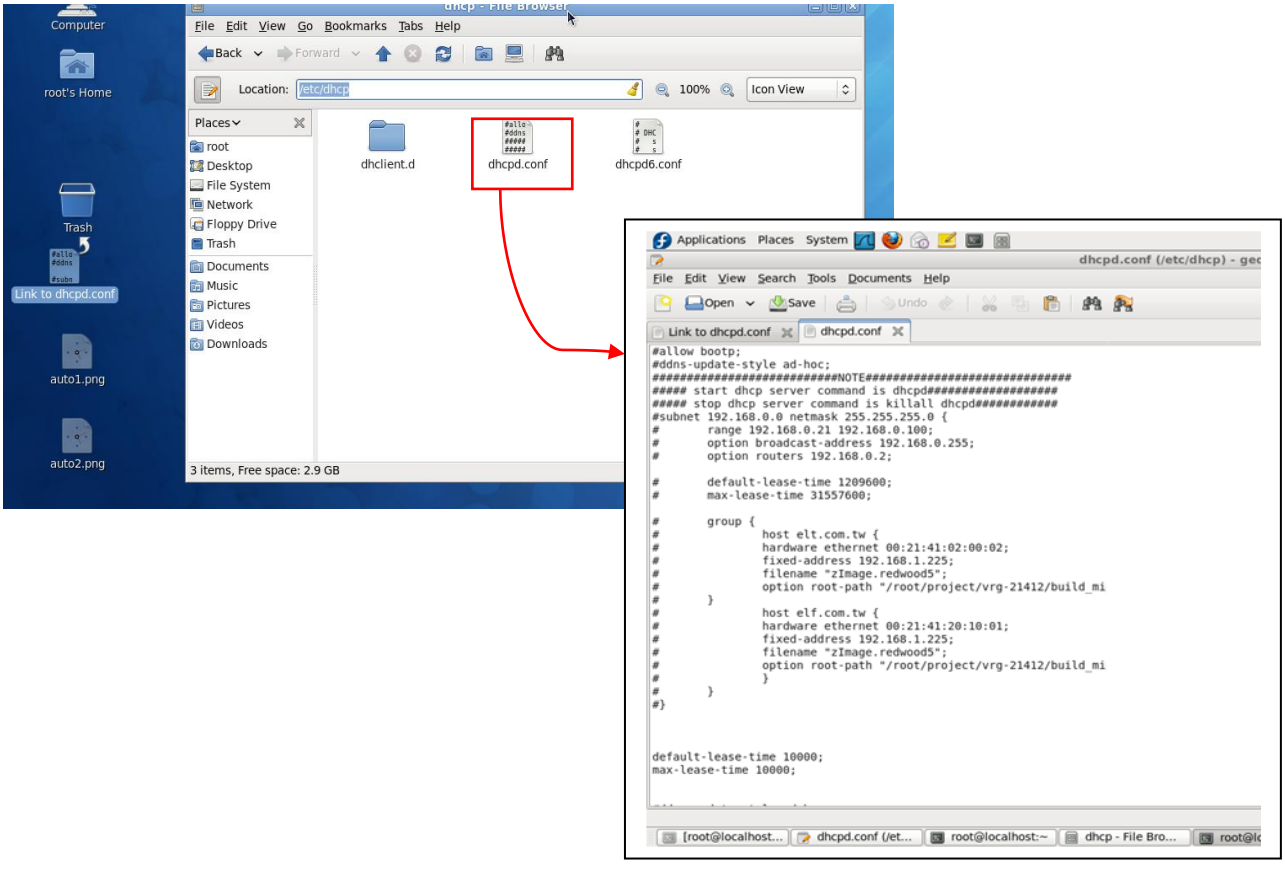
1. Choose dhcpd.
2. Enable DHCP service.
3. Start running DHCP service.

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



Step 3. Modify dhcpd.conf file

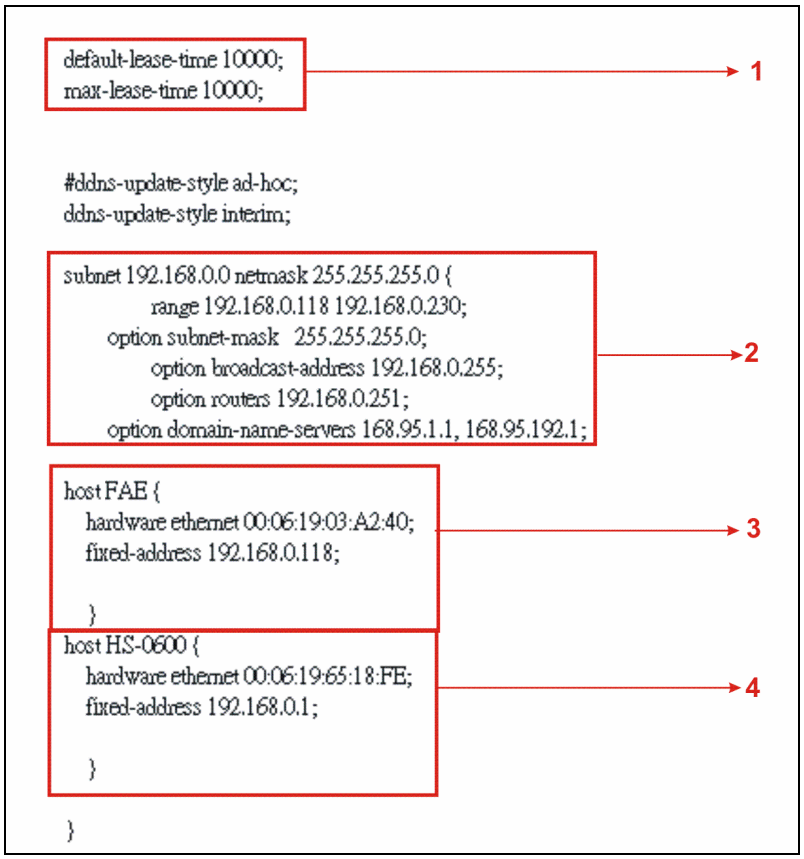
- **Open dhcpd.conf file in /etc/dhcp/ directory**



Double-click dhcpd.conf placed in /etc/dhcp/ directory to open it.

- **Modify dhcpd.conf file**

The following marked areas in dhcpd.conf file can be modified with values that work with your networking environment.



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

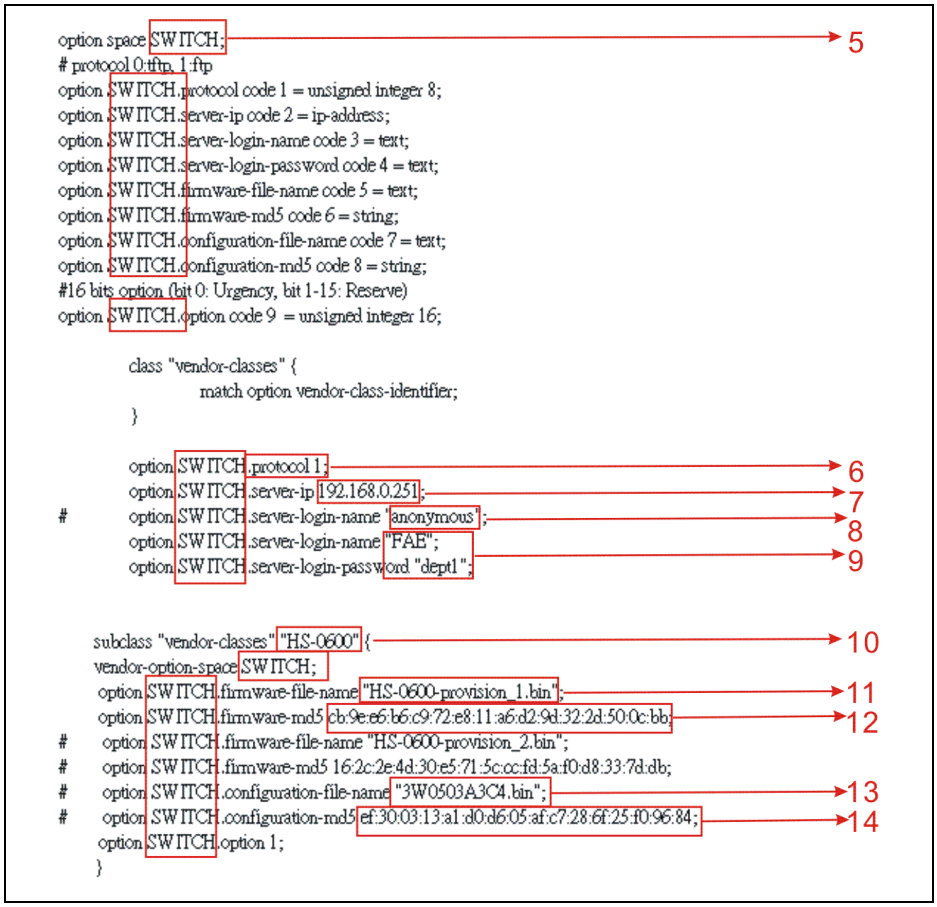
   Default lease time: If a client does not request a specific IP lease time, the server will assign a default lease time value.

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

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

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

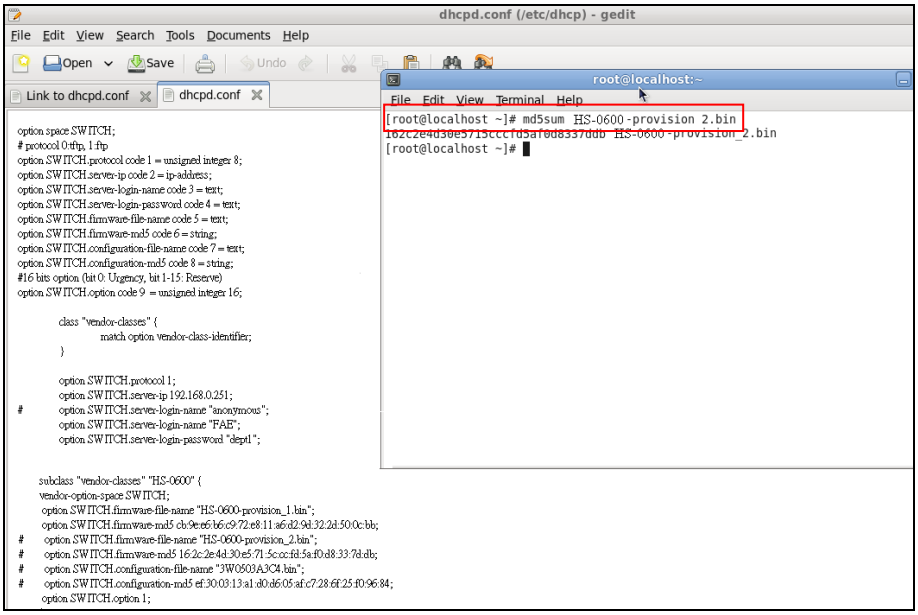
4. Map a host's MAC address to a fixed IP address. Use the same format to create multiple MAC-to-IP address bindings.



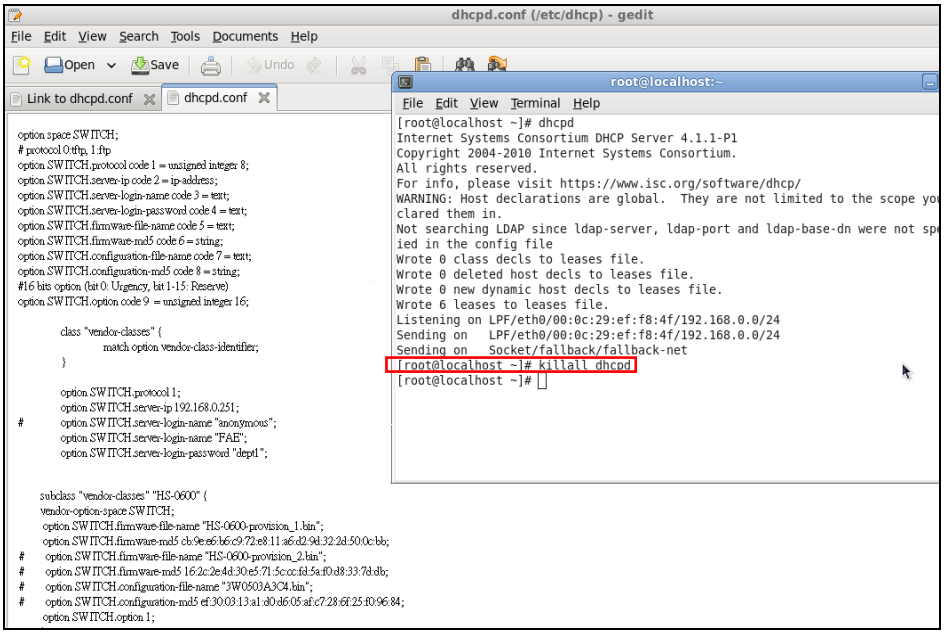
5. This value is configurable and can be defined by users.
6. Specify the protocol used (Protocol 1: FTP; Protocol 0: TFTP).
7. Specify the FTP or TFTP IP address.
8. Login TFTP server anonymously (TFTP does not require a login name and password).
9. Specify FTP Server login name and password.
10. Specify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

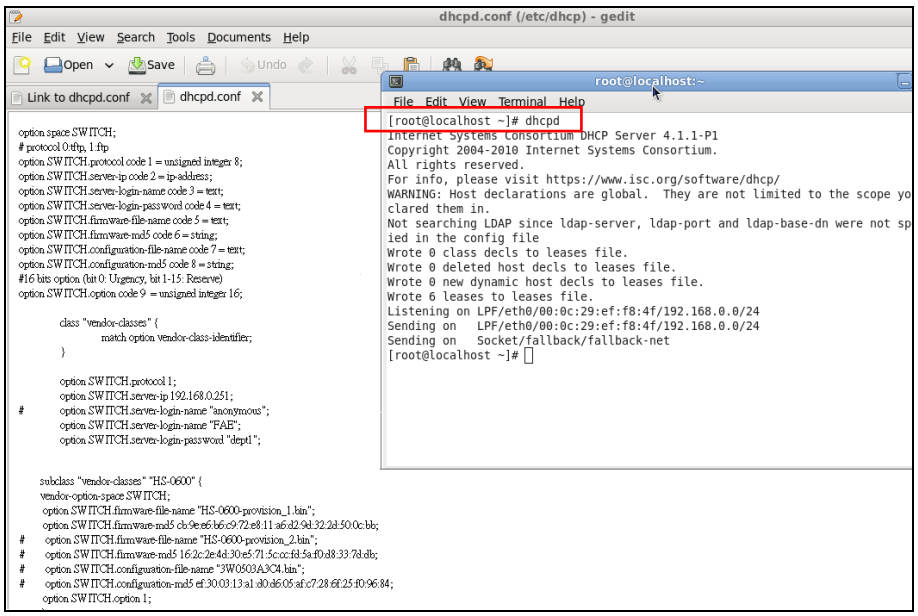
NOTE 1: *The text beginning with a pound sign (#) will be ignored by the DHCP server. For example, in the figure shown above, firmware-file-name "HS-0600-provision_2.bin" and firmware-md5 (line 5 & 6 from the bottom) will be ignored. If you want DHCP server to process these two lines, remove pound signs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

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



- **Restart DHCP service**





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

Step 4. Backup a Configuration File

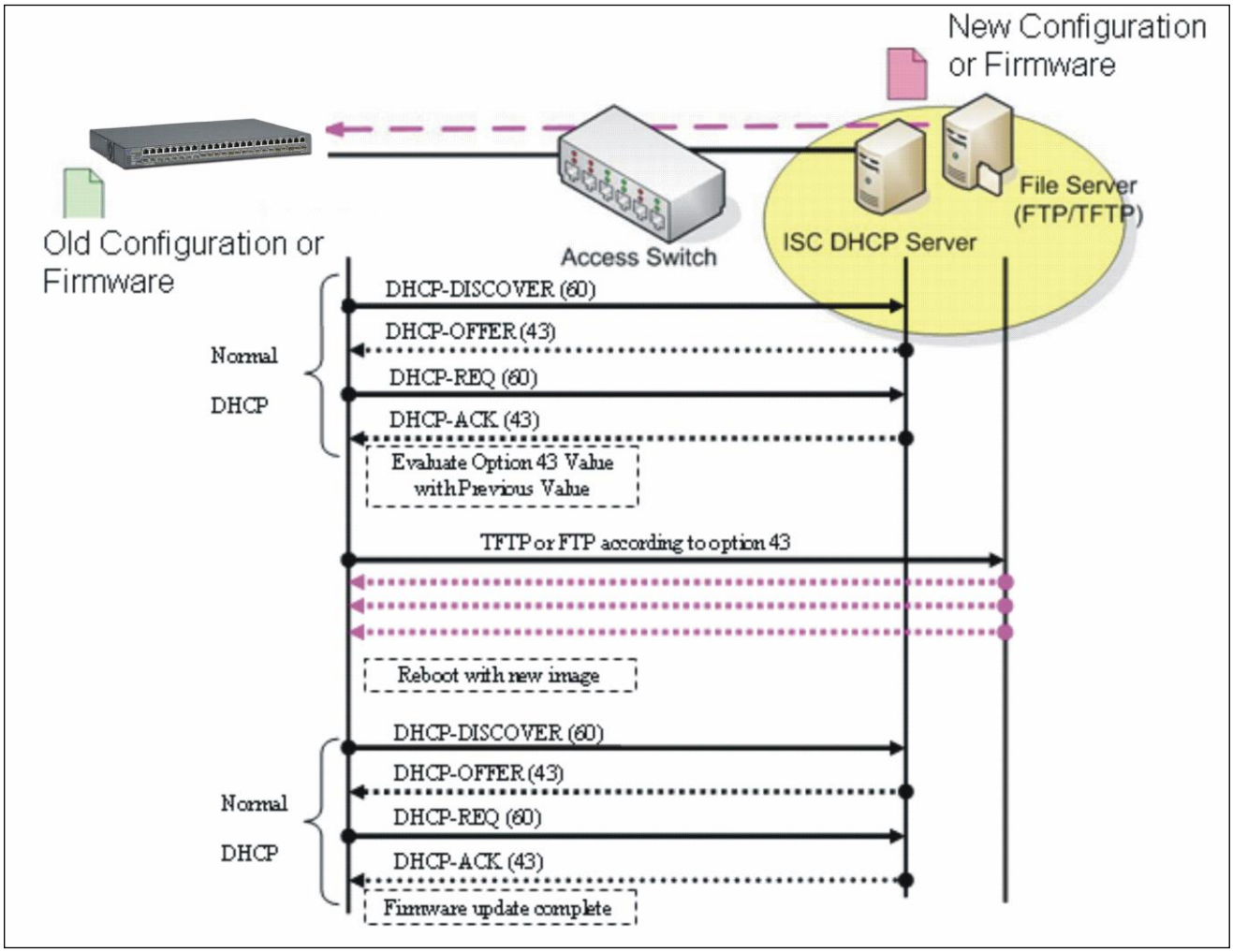
Before preparing a configuration file in TFTP/FTP Server, make sure the device generating the configuration file is set to **“Get IP address from DHCP”** assignment. This is because that DHCP Auto-provisioning is running under DHCP mode, so if the configuration file is uploaded by the network type other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

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

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

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

B. Auto-Provisioning Process

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

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