



HES-3106-SE

**5 x 10/100/1000Base-T RJ45 + 1 x
100/1000Base-X Fiber L2 Managed CPE
Switch**

Network Management

User's Manual

Version 0.9

Revision History

Version	F/W	Date	Description
0.9	0.99.0G	2023/01/12	First release

Trademarks

CTS is a registered trademark of Connection Technology Systems Inc.

Contents are subject to revision without prior notice.

All other trademarks remain the property of their owners.

Copyright Statement

Copyright © Connection Technology Systems Inc.

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

FCC Warning

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult your local distributors or an experienced radio/TV technician for help.
- Shielded interface cables must be used in order to comply with emission limits.

Changes or modifications to the equipment, which are not approved by the party responsible for compliance, could affect the user's authority to operate the equipment.

Copyright © 2023 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 USA

40538 La Purissima Way,

Fremont, CA 94539, USA

Tel: +1-510-509-0304

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

E-mail: cts_us@ctsystem.com

Connection Technology Systems Japan

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

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

Tel: +81-6-6450-8890

E-mail: cts_japan@ctsystem.com

Connection Technology Systems NE AB

E A Rosengrens gata 31,

421 31 Västra Frölunda,

Sweden

E-mail: info@ctsystem.se

Connection Technology Systems Central Europe (COMPONET Handels GmbH)

Hirschstettner Straße 19-21/Stiege I

A-1220 Vienna, Austria

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

E-mail: cts_ce@ctsystem.com

CTS Connection Technology Systems DE GmbH

An den Bergen 17, 60437 Frankfurt am Main,

Germany

Tel: +491711051295

E-mail: cts_de@ctsystem.com

Connection Technology Systems India Private Limited

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

Uttarahalli, Talgatpura, Kanakpura MN

Rd, Bangalore, Karnataka, India, 560062

Table of Content

CTS Contact Information	4
1. INTRODUCTION	9
1.1 Management Options	9
1.2 Management Software	10
1.3 Management Preparations	11
2. Command Line Interface (CLI)	13
2.1 Remote Management – Telnet/SSH	13
2.2 Navigating CLI	14
2.2.1 General Commands.....	14
2.2.2 Quick Keys.....	14
2.2.3 Command Format.....	15
2.2.4 Login Username & Password	16
2.3 User Mode.....	18
2.3.1 Ping Command	18
2.3.2 Traceroute Command.....	19
2.4 Privileged Mode.....	19
2.4.1 Copy-cfg Command	20
2.4.2 Firmware Command	21
2.4.3 Ping Command	22
2.4.4 Reload Command.....	22
2.4.5 Traceroute Command	22
2.4.6 Write Command	23
2.4.7 Configure Command.....	23
2.4.8 Show Command	23
2.5 Configuration Mode	26
2.5.1 Entering Interface Numbers.....	26
2.5.2 No Command.....	27
2.5.3 Show Command	27
2.5.4 CATV Command	29
2.5.5 Event-record Command.....	29
2.5.6 IP Command.....	29
2.5.7 IPv6 Command	35
2.5.8 LLDP Command	37
2.5.9 Loop Detection Command	39
2.5.10 LED Command	40

2.5.11 MAC Command.....	40
2.5.12 Management Command	43
2.5.13 Mirror Command	44
2.5.14 NTP Command	45
2.5.15 QoS Command	46
2.5.16 Security Command	50
2.5.17 SNMP-Server Command	52
2.5.18 Switch Command.....	57
2.5.19 Switch-info Command.....	57
2.5.20 Syslog Command.....	59
2.5.21 Terminal Command.....	60
2.5.22 Transceiver Command.....	60
2.5.23 User Command.....	66
2.5.24 VLAN Command.....	68
2.5.24.1 Port-Based VLAN.....	69
2.5.24.2 802.1Q VLAN	69
2.5.24.3 Introduction to Q-in-Q (ISP Mode).....	71
2.5.25 Interface Command	76
2.5.26 Show interface statistics Command	79
2.5.27 Show Transceiver Command.....	80
2.5.28 Show running-config & start-up-config & default-config Command.....	80
3. SNMP NETWORK MANAGEMENT	82
4. WEB MANAGEMENT.....	83
4.1 System Setup.....	85
4.1.1 System Information	86
4.1.2 IP Setup	88
4.1.3 IP Source Binding	91
4.1.4 Time Server Setup	92
4.1.5 Syslog Configuration.....	93
4.2 Port Management.....	94
4.2.1 Port Setup & Status.....	95
4.2.2 Port Traffic Statistics	97
4.2.3 Port Packet Error Statistics	98
4.2.4 Port Packet Analysis Statistics	99
4.2.5 Port Mirroring	100
4.3 VLAN Setup.....	102
4.3.1 VLAN Mode	103

4.3.2 Port Based VLAN.....	104
4.3.3 IEEE 802.1q Tag VLAN.....	106
4.3.3.1 Trunk VLAN Setup	109
4.3.3.2 VLAN Interface	110
4.3.3.3 VLAN Table	112
4.4 MAC Address Management	113
4.4.1 MAC Table Learning	114
4.4.2 MAC Address Table	115
4.5 QoS Setup.....	117
4.5.1 QoS Priority	118
4.5.2 QoS Remarking	121
4.5.3 QoS Rate Limit.....	123
4.6 Multicast	124
4.6.1 IGMP/MLD Snooping	124
4.6.1.1 IGMP/MLD Setup	126
4.6.1.2 IGMP/MLD VLAN Setup.....	127
4.6.1.3 IGMP Snooping Status.....	128
4.6.1.4 IGMP Group Table	129
4.6.1.5 MLD Snooping Status	130
4.6.1.6 MLD Group Table.....	131
4.7 Security Setup	132
4.7.1 DHCP Snooping.....	133
4.7.1.1 DHCP Snooping Setup.....	133
4.7.1.2 DHCP Option 82 / DHCPv6 Option 37 Setup	134
4.7.1.3 DHCP Snooping Table	137
4.7.2 Port Isolation.....	138
4.7.3 Storm Control.....	139
4.7.4 Loop Detection.....	141
4.8 LLDP	143
4.8.1 LLDP Setup.....	144
4.8.2 LLDP Status	145
4.9 Maintenance.....	146
4.9.1 CPU & Memory Statistics.....	147
4.9.2 Ping.....	149
4.9.3 Event Log.....	150
4.9.4 Transceiver Information	153
4.9.4.1 Transceiver Info.....	154

4.9.4.2 Transceiver State	155
4.9.4.3 Transceiver Threshold Configuration	156
4.10 Management	159
4.10.1 Management Access Setup	161
4.10.2 User Authentication.....	162
4.10.3 SNMP	166
4.10.3.1 SNMPv3 USM User.....	166
4.10.3.2 Device Community	169
4.10.3.3 Trap Destination	171
4.10.3.4 Trap Setup.....	172
4.10.4 LED Control Setup	173
4.10.5 Firmware upgrade.....	174
4.10.5.1 Configuration Backup/Restore via HTTP.....	174
4.10.5.2 Firmware Upgrade via HTTP.....	175
4.10.5.3 Configuration Backup/Restore via FTP/TFTP	176
4.10.5.4 Firmware Upgrade via FTP/TFTP	177
4.10.6 Load Factory Settings.....	178
4.10.7 Save Configuration	179
4.10.8 Reset System.....	180
APPENDIX A: FreeRADIUS Readme.....	181
APPENDIX B: Set Up DHCP Auto-Provisioning.....	183

1. INTRODUCTION

Thank you for using the 5-port 10/100/1000Base-T plus 1-port 100/1000Base-X Ethernet 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 10/100/1000Base-TX 8-pin RJ-45 ports located at the front panel of the Managed Switch. Direct RJ-45 LAN cable connection between a PC and the Managed Switch is required for Web Management.

1.2 Management Software

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

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

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.

1000Base-X / 100Base-FX Transceiver

Transceivers are used in optical data communication applications, which interface 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.

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.

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

10/100/1000Base-T RJ-45 Auto-MDI/MDIX ports are located at the front of the Managed Switch. These RJ-45 ports allow user to connect their traditional copper-based Ethernet/Fast Ethernet devices to the network. All these ports support auto-negotiation and MDI/MDIX auto-crossover, i.e. either crossover or straight through CAT-5 UTP or STP cable may be used.

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 <i>enable</i> command	Switch#	disable, exit, logout
Configuration mode	From Privileged mode, enter the <i>config</i> or <i>configure</i> 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.

	field. Enter the subnet mask.
[port]	Enter one port number. See Section 2.5.25 for detailed explanations.
[port_list]	Enter a range of port numbers or several discontinuous port numbers. See Section 2.5.25 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 <u>1</u> 0 Switch(config)#qos dscp-map <u>10</u> 3 Example 2: specifying three values (separated by commas) Switch(config)#qos 802.1p-map <u>1,3</u> 0 Switch(config)#qos dscp-map <u>10,13,15</u> 3 Example 3: specifying a range of values (separated by a hyphen) Switch(config)#qos 802.1p-map <u>1-3</u> 0 Switch(config)#qos dscp-map <u>10-15</u> 3

2.2.4 Login Username & Password

Default Login

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

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

Privileged Mode Password

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

Forgot Your Login Username & Password

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

2.3 User Mode

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

Command	Description
exit	Quit the User mode or close the terminal connection.
help	Display a list of available commands in User mode.
history	Display the command history.
logout	Logout from the Managed Switch.
ping	Test whether a specified network device or host is reachable or not.
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 1-65500] [-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 1-65500]	Enter the packet size that would be sent. The allowable packet size is from 1 to 65500 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.
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.

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

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

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

5. Restore the Managed Switch back to default settings but keep the entire data of event log.

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

6. Restore the Managed Switch back to default settings but keep both of the IP configurations and the entire data of event log.

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

2.4.2 Firmware Command

To upgrade firmware via TFTP or FTP server.

Command	Parameter	Description
Switch# firmware upgrade ftp [A.B.C.D A:B:C:D:E:F:G:H] [file name] [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 very important for network administrators to get information about the device, receive outputs to verify a command’s configurations or troubleshoot a network configuration error. It can be used in Privileged or Configuration mode. The following describes different uses of “show” command.

1. Display system information

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

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

System Object ID: Display the predefined System OID.

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

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

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

DHCP/DHCPv6 Vendor ID: Vendor Class Identifier. Enter the user-defined DHCP vendor ID, up to 55 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.

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.

WAN Transceiver Type: The information about the WAN transceiver type.

WAN Transceiver Vendor: Vendor name of the WAN transceiver.

WAN Transceiver PN: Vendor PN of the WAN transceiver.

***CATV RF Status:** View-only field that shows whether RF TV is ready or not.

***CATV RF Module:** Turn on or off the RF TV Output. (only configurable for models with a CATV RF module)

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

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

Up Time: Display the up time since last restarting.

Local Time: Display the local time of the system.

2. Display or verify currently-configured settings

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

3. Display interface information or statistics

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

4. Show default, running and startup configurations

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

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
catv	Enable or disable the CATV RF module, and view whether the CATV RF module is ready or not.
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.
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.
mirror	Set up target port for mirroring.
ntp	Set up required configurations for Network Time Protocol.
qos	Set up the priority of packets within the Managed Switch.
security	Configure broadcast, unknown multicast, unknown unicast storm control settings.
snmp-server	Create a new SNMP community and trap destination and specify the trap types.
switch	Set up acceptable frame size and address learning, etc.
switch-info	Edit the system information.
syslog	Set up required configurations for Syslog server.
terminal	Set up Terminal functions.
transceiver	Configure the transceiver monitored items’ parameters and view the current value of each item.
user	Create a new user account.
vlan	Set up VLAN mode and VLAN configuration.
no	Disable a command or reset it back to its default setting.
interface	Select a single interface or a range of interfaces.
show	Show a list of commands or show the current setting of each listed command.

2.5.1 Entering Interface Numbers

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

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

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

2.5.2 No Command

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

2.5.3 Show Command

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

1. Display system information

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

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

System Object ID: Display the predefined System OID.

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

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

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

DHCP/DHCPv6 Vendor ID: Vendor Class Identifier. Enter the user-defined DHCP vendor ID, up to 55 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.

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.

WAN Transceiver Type: The information about the WAN transceiver type.

WAN Transceiver Vendor: Vendor name of the WAN transceiver.

WAN Transceiver PN: Vendor PN of the WAN transceiver.

***CATV RF Status:** View-only field that shows whether RF TV is ready or not.

***CATV RF Module:** Turn on or off the RF TV Output. (only configurable for models with a CATV RF module)

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

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

Up Time: Display the up time since last restarting.

Local Time: Display the local time of the system.

2. Display or verify currently-configured settings

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

3. Display interface information or statistics

Refer to "Show interface statistics command" and "Show transceiver information command" sections.

4. Show default, running and startup configurations

Refer to "show default-config copmmand", "show running-config command" and "show start-up-config command" sections.

2.5.4 CATV Command

Enable or disable the CATV RF module, and view whether the CATV RF module is ready or not. Please be noted that the commands below are available dependent upon the model at hand. The commands will not be applicable if the Managed Switch doesn't support a CATV RF module.

CATV command	Description
Switch(config)# catv	Enable CATV RF module.
No command	
Switch(config)# no catv	Disable CATV RF module.
Show command	
Switch(config)# show switch-info	Show current CATV RF module status.

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]	[A.B.C.D]	Enter the desired IP address for your Managed Switch.
[255.X.X.X] [A.B.C.D]	[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 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]	[1-4]	Specify DHCPv4/DHCPv6 server trust IPv4/IPv6 address number.
[1-4] ip-address [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 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".

3. 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.

4. Enable or disable IGMP/MLD snooping globally.

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

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

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

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

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

IGMP/MLD Snooping Command	Parameter	Description
Switch(config)# ip igmp snooping		Enable IGMP/MLD snooping. When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic. This is for IGMPv1, v2 and MLDv1 only.
Switch(config)# ip igmp snooping version-3		Enable IGMPv3/MLDv2 snooping. When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic. This is for IGMPv3 and MLDv2 only.
Switch(config)# ip igmp snooping flooding		Enable Unregistered IPMC Flooding function. Set forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic will flood when enabled. However, the traffic will be forwarded to router-ports only when disabled.
Switch(config)# ip igmp snooping immediate-leave		Enable immediate leave function.
Switch(config)# ip igmp snooping max-response-time [1-255]	[1-255] (Unit:1/10secs)	Specify the IGMP/MLD querier maximum response time. This determines the maximum amount of time can be allowed before sending an IGMP/MLD response report.
Switch(config)# ip igmp snooping query-interval [1-6000]	[1-6000]	Specify the query time interval of IGMP/MLD querier. This is used to set up the time interval between transmitting IGMP/MLD queries. (Range:1-6000 seconds)
Switch(config)# ip igmp snooping vlan [1-4094]	[1-4094]	Specify a VLAN ID. This enables IGMP/MLD Snooping for the specified VLAN.

Switch(config)# ip igmp snooping vlan [1-4094] query	[1-4094]	Enable a querier for the specified VLAN.
No command		
Switch(config)# no ip igmp snooping		Disable IGMP/MLD snooping function.
Switch(config)# no ip igmp snooping flooding		Disable Unregistered IPMC Flooding function. The traffic will be forwarded to router-ports only when disabled.
Switch(config)# no ip igmp snooping immediate-leave		Disable immediate leave function.
Switch(config)# no ip igmp snooping max-response-time		Reset the IGMP/MLD querier maximum response time back to the default.
Switch(config)# no ip igmp snooping query-interval		Reset the query time interval value back to the default. (100 seconds)
Switch(config)# no ip igmp snooping version-3		Disable IGMPv3/MLDv2 snooping.
Switch(config)# no ip igmp snooping vlan [1-4094]	[1-4094]	Disable IGMP/MLD snooping for the specified VLAN.
Switch(config)# no ip igmp snooping vlan [1-4094] query	[1-4094]	Disable a querier for the specified VLAN.
Show command		
Switch(config)# show ip igmp snooping		Show the current IGMP/MLD snooping configuration.
Switch(config)# show ip igmp snooping groups		Show IGMP snooping groups table.
Switch(config)# show ip igmp snooping status		Show IGMP Snooping status.
Switch(config)# show ip mld snooping groups		Show MLD snooping groups table.
Switch(config)# show ip mld snooping status		Show MLD Snooping status.

5. Set Up IP Source Binding Function.

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

		Binding list.
Show command		
Switch(config)# show ip source		Show IPv4/IPv6 Source configuration.

2.5.7 IPv6 Command

Brief Introduction to IPv6 Addressing

IPv6 addresses are 128 bits long and number about 3.4×10^{38} . IPv6 addresses are written in eight groups of four hexadecimal digits separated by colons, such as

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

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

Stateless Autoconfiguration

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

Autoconfigured address format

part	Subnet prefix	Interface identifier
bits	64	64

Link local address

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

Global address

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

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

DHCPv6

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

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

IPv6 command	Parameter	Description
Switch(config)# ipv6 address autoconfig		Configuration of IPv6 addresses using stateless autoconfiguration.
Switch(config)# ipv6 address dhcp auto		Configure DHCPv6 function into the auto mode.
Switch(config)# ipv6 address dhcp force		Configure DHCPv6 function into the forced mode.
Switch(config)# ipv6 address dhcp rapid-commit		Allow the two-message exchange for address assignment.
“ipv6 address dhcp” commands are functional only when autoconfiguration is enabled.		
Switch(config)# ipv6 address global	[A:B:C:D:E:F:G:H/10~128]	Specify switch IPv6 global address and prefix-length.
[A:B:C:D:E:F:G:H/10~128] [A:B:C:D:E:F:G:H]	[A:B:C:D:E:F:G:H]	Specify switch IPv6 default gateway IP address.
Switch(config)# ipv6 address link-local	[A:B:C:D:E:F:G:H/10~128]	Specify switch IPv6 link-local address and prefix-length.
[A:B:C:D:E:F:G:H/10~128]		
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.

2.5.8 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 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 hold-time		Reset the hold-time value back to the default. (120 seconds)
Switch(config)# no lldp interval		Reset the time interval value of sending updated LLDP packets back to the default.(5 seconds)
Switch(config)# no lldp packets		Reset the amount of packets that are sent in each discover back to the default.(1 packet)
Switch(config)# no lldp tlv-select capability		Disable Capability attribute to be sent.
Switch(config)# no lldp tlv-select management-address		Disable Management Address attribute to be sent.
Switch(config)# no lldp tlv-select port-description		Disable Port Description attribute to be sent.
Switch(config)# no lldp tlv-select system-description		Disable System Description attribute to be sent.
Switch(config)# no lldp tlv-select system-name		Disable System Name attribute to be sent.
Show command		
Switch# show lldp		Show LLDP settings.

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

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

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

2.5.9 Loop Detection Command

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

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

1. It blocks the relevant port to prevent broadcast storms, and send out SNMP trap to inform the network administrator. In other words, the system stops forwarding all the traffic via the looped port, 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 [0-1440]	[0-1440]	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 0 to 1440 minutes. The default setting is 0 minutes. "0" means "Disable".
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.
Examples of Loop Detection command		
Switch(config)# loop-detection unlock-interval 120		Set the Loop Detection unlock time interval to 120 minutes.

2.5.10 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.

2.5.11 MAC Command

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

MAC Command	Parameter	Description
Switch(config)# mac address-table aging-time [0-458s]	[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 static		Show the created static MAC addresses.
Switch(config)# show mac address-table static [mac vid port]	[mac vid port]	Show the created static MAC addresses sorted by specific option.
Switch(config)# show mac address-table vlan [vlan_id] [mac vid port]	[vlan_id]	Show the MAC addresses that belongs to the specified VLAN ID.
	[mac vid port]	Show the specified VLAN's MAC addresses sorted by specific option.
Switch(config)# show mac learning		Show MAC learning setting of each interface.
Switch(config)# show mac 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.

2.5.12 Management Command

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

Management Command	Parameter	Description
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 telnet timeout [1-1440]	[1-1440]	Disconnect the Managed Switch when telnet management is inactive for the specified period. The allowable value is from 1 to 1440 (minutes).
Switch(config)# management web		Enable Web management by the http method.
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 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 telnet timeout		Reset telnet timeout value back to the default (300 seconds).
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.

2.5.13 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_list] direction [tx rx both]	[port_list]	Specify the source port number(s) and TX/RX/both direction for port mirroring.
	[tx rx both]	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_list] direction [tx rx both]	[port_list]	Remove the source port number(s) and TX/RX/both direction from the port mirroring list.
	[tx rx both]	
Show command		
Switch(config)# show mirror		Show the current port mirroring configuration.
Switch(config-mirror-index)# show		Show the current configuration of the specified port mirroring.
Example of Mirror command		
Switch(config-mirror-3)# destination 8		The selected source ports' data will mirror to Port 8 in the port mirroring of Index No. 3.
Switch(config-mirror-3)# source 1-2 direction tx		Port 1 to 3's transmitting packets will mirror to the destination port in the port mirroring of Index No. 3.

2.5.14 NTP Command

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

Show command	
Switch# show ntp	Show the current NTP time server configuration.
Switch(config)# show ntp	Show the current NTP time server configuration.
Examples of NTP command	
Switch(config)# ntp	Enable NTP function for the Managed Switch.
Switch(config)# ntp daylight-saving date	Enable the daylight saving function in date mode.
Switch(config)# ntp offset [100,12:00-101,12:00]	Daylight saving time date start from the 100 th day of the year to the 101 th day of the year.
Switch(config)# ntp server1 192.180.0.12	Set the primary NTP time server's IP address to 192.180.0.12.
Switch(config)# ntp server2 192.180.0.13	Set the secondary NTP time server's IP address to 192.180.0.13.
Switch(config)# ntp syn-interval 4	Set the synchronization interval to 4 hours.
Switch(config)# ntp time-zone 3	Set the time zone to GMT-8:00 Vancouver.

2.5.15 QoS Command

1. 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 “ <i>interface</i> ” command to assign a queue to the selected interfaces. 802.1p: Use “ <i>qos 802.1p-map</i> ” command to assign priority bits to a queue. dscp: Use “ <i>qos dscp-map</i> ” 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.
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]	<p>By default, "strict" queuing mode is used. If you want to use "weight" queuing mode, you need to disable "strict" mode.</p> <p>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.</p> <p>Weight mode: All queues have fair</p>

		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 remarking 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 remarking 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. <table border="1" data-bbox="869 766 1439 869"> <tr> <td>Priority Level</td> <td colspan="3">Low</td> <td>Normal</td> <td colspan="2">Medium</td> <td colspan="2">High</td> </tr> <tr> <td>802.1p Value</td> <td>0</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> <td>6</td> <td>7</td> </tr> </table>	Priority Level	Low			Normal	Medium		High		802.1p Value	0	1	2	3	4	5	6	7
Priority Level	Low			Normal	Medium		High													
802.1p Value	0	1	2	3	4	5	6	7												
	[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 Mbps]	[Kbps Mbps]	Specify the unit of the ingress rate limit between Kbps and Mbps.
Switch(config-if-PORT-PORT)# qos rate-limit egress		Enable QoS egress rate limit settings.
Switch(config-if-PORT-PORT)# qos rate-limit egress rate [500-1000000 1-	[500-1000000 1-	Specify the egress rate limit value. (Valid range is from 500-1000000 in

1000000 1-1000] Kbps/Mbps	1000] Kbps/Mbps	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)

2.5.16 Security Command

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

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)# security storm-protection		Globally enable the storm control function.
Switch(config-if-PORT-PORT)# security storm- protection broadcast [1-256k]	[1-256k]	Specify the maximum broadcast packets per second (pps). Any broadcast packets exceeding the specified threshold will then be dropped. The packet rates that can be specified are listed below: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k NOTE: To view a list of allowable values that can be specified you can

		press “spacebar” and then followed by “?”. For example, “Switch(config)# security storm-protection broadcast ?”
Switch(config-if-PORT-PORT)# security storm-protection unknown-multicast [1-256k]	[1-256k]	Specify the maximum unknown multicast packets per second (pps). Any unknown multicast packets exceeding the specified threshold will then be dropped. The packet rates that can be specified are listed below: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k NOTE: To view a list of allowable values that can be specified you can press “spacebar” and then followed by “?”. For example, “Switch(config)# security storm-protection multicast ?”
Switch(config-if-PORT-PORT)# security storm-protection unknown-unicast [1-256k]	[1-256k]	Specify the maximum unknown unicast packets per second (pps). Any unknown unicast packets exceeding the specified threshold will then be dropped. The packet rates that can be specified are listed below: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k NOTE: To view a list of allowable values that can be specified you can press “spacebar” and then followed by “?”. For example, “Switch(config)# security storm-protection unicast ?”
No command		
Switch(config)# no security storm-protection		Globally disable the storm control function.
Switch(config-if-PORT-PORT)# no security storm-protection broadcast		Disable broadcast storm control on the selected ports.
Switch(config-if-PORT-PORT)# no security storm-protection unknown-multicast		Disable unknown-multicast storm control on the selected ports.
Switch(config-if-PORT-PORT)# no security storm-protection unknown-unicast		Disable unknown-unicast storm control on the selected ports.
Examples of Security command		
Switch(config)# 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.

2.5.17 SNMP-Server Command

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

Snmp-server command	Parameter	Description
Switch(config)# snmp-server		Enable SNMP server function globally.
Switch(config)# snmp-server community [community]	[community]	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 alphanumeric characters can be accepted.
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 specified trap destination.
Switch(config-trap-ID)# destination [A.B.C.D A:B:C:D:E:F 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 specified 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 cold-start cpu-load port-link power-down transceiver-threshold warm-start]	[all auth-fail cold-start cpu-load port-link power-down transceiver-threshold warm-start]	<p>Specify a trap type that will be sent when a certain situation occurs.</p> <p>all: Enable all traps to be sent when corresponding events are triggered.</p> <p>auth-fail: A trap will be sent when any unauthorized user attempts to login.</p> <p>cold-start: A trap will be sent when the Managed Switch boots up.</p> <p>cpu-load: A trap will be sent when the CPU is overloaded.</p> <p>port-link: A trap will be sent when the link is up or down.</p> <p>power-down: A trap will be sent when the Managed Switch's power is down.</p> <p>transceiver-threshold: A trap will be sent when Temperature / Voltage/ Current / TX Power / RX Power of any transceivers is over the High value, under the Low value, or returning to the normal status from abnormal status.</p> <p>warm-start: A trap will be sent when the Managed Switch restarts.</p>
No command		
Switch(config)# no snmp-server trap-type [all auth-fail cold-start cpu-load port-link power-down transceiver-threshold warm-start]	[all auth-fail cold-start cpu-load port-link power-down transceiver-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. Up to 20 alphanumeric characters can be accepted.
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. Up to 20 alphanumeric characters can be accepted.
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.

2.5.18 Switch Command

Switch command	Parameter	Description
Switch(config)# switch mtu [1518-16367]	[1518-16367]	Specify the maximum frame size in bytes. The allowable MTU value is between 1518 and 16367 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.

2.5.19 Switch-info Command

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

Switch-info Command	Parameter	Description
Switch(config)# switch-info company-name [company_name]	[company_name]	Enter a company name, up to 55 alphanumeric characters, for this Managed Switch.
Switch(config)# switch-info cpu-loading-threshold [10-3000]	[10-3000] (Unit: 1/100)	Specify CPU loading threshold.
Switch(config)# switch-info dhcp-vendor-id [dhcp_vendor_id]	[dhcp_vendor_id]	Enter the user-defined DHCP vendor ID, and up to 55 alphanumeric characters can be accepted. Please make sure you have an exact DHCP Vendor ID with the value specified in "vendor-classes" in your dhcpd.conf file. For detailed information, see Appendix B .
Switch(config)# switch-info host-name [host_name]	[host_name]	Enter a new hostname, up to 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 system-contact [sys_contact]	[sys_contact]	Enter the contact information, up to 55 alphanumeric characters, for this Managed switch.
Switch(config)# switch-info system-location [sys_location]	[sys_location]	Enter a brief description of the Managed Switch location, up to 55 alphanumeric characters, for this Managed Switch. Like the name, the location is for reference only, for example, "13th Floor".

Switch(config)# switch-info system-name [sys_name]	[sys_name]	Enter a unique name, up to 55 alphanumeric characters, for this Managed Switch. Use a descriptive name to identify the Managed Switch in relation to your network, for example, "Backbone 1". This name is mainly used for reference only.
No command		
Switch(config)# no switch-info company-name		Reset the entered company name back to the default.
Switch(config)# no switch-info cpu-loading-threshold		Reset CPU loading threshold back to the default.
Switch(config)# no switch-info dhcp-vendor-id		Reset the entered DHCP vendor ID information back to the default.
Switch(config)# no switch-info host-name		Reset the hostname back to the default.
Switch(config)# no switch-info system-contact		Reset the entered system contact information back to the default.
Switch(config)# no switch-info system-location		Reset the entered system location information back to the default.
Switch(config)# no switch-info system-name		Reset the entered system name information back to the default.
Show command		
Switch(config)# show switch-info		Show the switch-related information including company name, system contact, system location, system name, model name, firmware version and so on.
Switch(config)# show switch-info cpu-mem-statistics		Show the current CPU & memory usage rate of the switch.
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@company.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 edgswitch10		Change the Managed Switch's hostname into "edgswitch10".

2.5.20 Syslog Command

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

2.5.21 Terminal 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.

2.5.22 Transceiver Command

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

You can decide one or all items to be shown at a time by assigning **All / Temperature / Voltage / Current / TX power / RX power** parameter upon your requirements.

Once this function of the specific transceiver 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 transceivers’ 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 transceiver status to prevent the disconnection and packets loss of any fiber ports from being taken place due to the occurrence of abnormal events.

Transceiver command	Parameter	Description
Switch(config)# transceiver threshold		Globally enable the alarm notification of temperature/voltage/current/TX power/RX power for transceivers of the Managed Swtich.
Switch(config)# transceiver threshold notification continuous-alarm		Enable the continuous alarm message sending function for transceivers’ temperature/voltage/current/TX power/RX power.
Switch(config)# transceiver threshold notification continuous-alarm interval [60-86400]	[60-86400]	Specify the continuous alarm interval for transceivers’ 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)# transceiver threshold notification interval [120-86400]	[120-86400]	Specify the time interval of sending transceivers' temperature/voltage/current/TX power/RX power alarm message in seconds.
No command		
Switch(config)# no transceiver threshold		Globally disable the alarm notification of temperature/voltage/current/TX power/RX power for transceivers of the Managed Swtich.
Switch(config)# no transceiver threshold notification continuous-alarm		Disable the continuous alarm message sending function for transceivers' temperature/voltage/current/TX power/RX power.
Switch(config)# no transceiver threshold notification continuous-alarm interval		Reset to default the continuous alarm interval for transceivers' temperature/voltage/current/TX power/RX power alarm message (120 seconds).
Switch(config)# no transceiver threshold notification interval		Reset the time interval of sending transceivers' temperature/voltage/current/TX power/RX power alarm message to default (600 seconds).
Show command		
Switch(config)# show transceiver threshold		Show transceiver threshold configuration, all transceivers' current temperature/voltage/current /TX power/RX power and their threshold information of these parameters.
Switch(config)# show transceiver threshold [port_list]	[port_list]	Show transceiver threshold configuration, the specific transceivers' current temperature/voltage/current/TX power/RX power and their threshold information of these parameters.
Switch(config)# show transceiver threshold current		Show transceiver threshold configuration, all transceivers' current and their threshold information of this parameter.
Switch(config)# show transceiver threshold current [port_list]	[port_list]	Show transceiver threshold configuration, the specific transceivers' current and their threshold information of this parameter.
Switch(config)# show transceiver threshold rx-power		Show transceiver threshold configuration, all transceivers' current RX power and their threshold information of this parameter.
Switch(config)# show transceiver threshold rx-power [port_list]	[port_list]	Show transceiver threshold configuration, the specific transceivers' current RX power and their threshold information of this parameter.
Switch(config)# show		Show transceiver threshold configuration,

transceiver threshold temperature		all transceivers' current temperature and their threshold information of this parameter.
Switch(config)# show transceiver threshold temperature [port_list]	[port_list]	Show transceiver threshold configuration, the specific transceivers' current temperature and their threshold information of this parameter.
Switch(config)# show transceiver threshold tx-power		Show transceiver threshold configuration, all transceivers' current TX power and their threshold information of this parameter.
Switch(config)# show transceiver threshold tx-power [port_list]	[port_list]	Show transceiver threshold configuration, the specific transceivers' current TX power and their threshold information of this parameter.
Switch(config)# show transceiver threshold voltage		Show transceiver threshold configuration, all transceivers' current voltage and their threshold information of this parameter.
Switch(config)# show transceiver threshold voltage [port_list]	[port_list]	Show transceiver threshold configuration, the specific transceivers' current voltage and their threshold information of this parameter.
Example of transceiver threshold command		
Switch(config)# transceiver threshold notification interval 300		Configure the time interval of sending transceivers' temperature/voltage/current/TX power/RX power alarm message as 300 seconds. If their transceiver 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)# transceiver threshold notification continuous-alarm interval 60		Configure the continuous alarm interval for transceivers' 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 transceiver threshold must be enabled beforehand for this to work properly.
Switch(config)# show transceiver threshold 6		Display Port 6 transceiver'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’ transceiver threshold function.

Transceiver 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)# transceiver threshold detect		Enable auto detect alarm and warning threshold for the selected port(s). Default value is enabled.
Switch(config-if-PORT-PORT)# transceiver threshold current [high low]	[high low]	Enable high/low current threshold for the selected port(s).
Switch(config-if-PORT-PORT)# transceiver threshold current [high low] value [0~1500]	[high low]	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).
	[0~1500]	
Switch(config-if-PORT-PORT)# transceiver threshold current [high low] value [alarm warning] [0~1500]	[high low]	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).
	[alarm warning]	
	[0~1500]	
Switch(config-if-PORT-PORT)# transceiver threshold rx-power [high low]	[high low]	Enable high/low RX power threshold for the selected port(s).
Switch(config-if-PORT-PORT)# transceiver threshold rx-power [high low] value [-400~100]	[high low]	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).
	[-400~100]	
Switch(config-if-PORT-PORT)# transceiver threshold rx-power [high low] value [alarm warning] [-400~100]	[high low]	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).
	[alarm warning]	
	[-400~100]	
Switch(config-if-PORT-PORT)# transceiver threshold temperature [high low]	[high low]	Enable high/low temperature threshold for the selected port(s).
Switch(config-if-PORT-PORT)# transceiver threshold temperature [high low] value [-400~1200]	[high low]	Specify the value for high/low alarm/warning temperature threshold for the selected port(s). This command can set high/low alarm and warning

	[-400~1200]	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)# transceiver threshold temperature [high low] value [alarm warning] [-400~1200]	[high low]	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).
	[alarm warning]	
	[-400~1200]	
Switch(config-if-PORT-PORT)# transceiver threshold tx-power [high low]	[high low]	Enable high/low TX power threshold for the selected port(s).
Switch(config-if-PORT-PORT)# transceiver threshold tx-power [high low] value [-300~100]	[high low]	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).
	[-300~100]	
Switch(config-if-PORT-PORT)# transceiver threshold tx-power [high low] value [alarm warning] [-300~100]	[high low]	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).
	[alarm warning]	
	[-300~100]	
Switch(config-if-PORT-PORT)# transceiver threshold voltage [high low]	[high low]	Enable high/low voltage threshold for the selected port(s).
Switch(config-if-PORT-PORT)# transceiver threshold voltage [high low] value [260~400]	[high low]	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).
	[260~400]	
Switch(config-if-PORT-PORT)# transceiver threshold voltage [high low] value [alarm warning] [260~400]	[high low]	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).
	[alarm warning]	
	[260~400]	
No command		
Switch(config-if-PORT-PORT)# no transceiver threshold detect		Disable auto detect alarm and warning threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no transceiver threshold current [high low]	[high low]	Disable high/low current threshold for the selected port(s).

Switch(config-if-PORT-PORT)# no transceiver 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 transceiver threshold current [high low] value [alarm warning]	[high low]	Respectively reset the high/low alarm or warning current threshold value to default.
	[alarm warning]	
Switch(config-if-PORT-PORT)# no transceiver threshold rx-power [high low]	[high low]	Disable high/low RX power threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no transceiver 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-PORT)# no transceiver threshold rx-power [high low] value [alarm warning]	[high low]	Respectively reset the high/low alarm or warning RX power threshold value to default.
	[alarm warning]	
Switch(config-if-PORT-PORT)# no transceiver threshold temperature [high low]	[high low]	Disable high/low temperature threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no transceiver 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 transceiver threshold temperature [high low] value [alarm warning]	[high low]	Respectively reset the high/low alarm or warning temperature threshold value to default.
	[alarm warning]	
Switch(config-if-PORT-PORT)# no transceiver threshold tx-power [high low]	[high low]	Disable high/low TX power threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no transceiver 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 transceiver threshold tx-power [high low] value [alarm warning]	[high low]	Respectively reset the high/low alarm or warning TX power threshold value to default.
	[alarm warning]	
Switch(config-if-PORT-PORT)# no transceiver threshold voltage [high low]	[high low]	Disable high/low voltage threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no transceiver 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 transceiver threshold voltage [high low]	[high low]	Respectively reset the high/low alarm or warning voltage threshold value to default.
	[alarm warning]	

value [alarm warning]	warning]	
Example of transceiver threshold & interface commands		
Switch(config-if-6)# transceiver threshold temperature high		Enable high temperature threshold for Port 6.
Switch(config-if-6)# transceiver threshold temperature high value 800		Configure both high alarm and warning temperature thresholds as 80 degrees Celsius for Port 6.
Switch(config-if-6)# transceiver threshold temperature low value warning -100		Configure low warning temperature threshold as -10 degrees Celsius for Port 6.

2.5.23 User Command

Create a new login account and set up RADIUS function.

1. Configure user login account.

User command	Parameter	Description
Switch(config)# user name [user_name]	[user_name]	Enter the new account's username. The authorized user login name is up to 20 alphanumeric characters. Only 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.
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 20 alphanumeric characters.
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. Set up RADIUS authentication function.

User command	Parameter	Description
Switch(config)# user radius		Enable RADIUS authentication function.
Switch(config)# user radius radius-port [1025-65535]	[1025-65535]	Specify the RADIUS port number.
Switch(config)# user radius retry-time [0-2]	[0-2]	Specify the number of retry times when the Switch gets no response from the RADIUS server.
Switch(config)# user radius secret [secret]	[secret]	Specify the secret key which is same as the one of the RADIUS server.

Switch(config)# user 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)# user radius server1 [A.B.C.D]	[A.B.C.D]	Specify the IP address of the 1 st RADIUS server.
Switch(config)# user radius server2 [A.B.C.D]	[A.B.C.D]	Specify the IP address of the 2 nd RADIUS server.
No command		
Switch(config)# no user radius		Disable RADIUS authentication function.
Switch(config)# no user radius radius-port		Set the RADIUS port number back to the default.
Switch(config)# no user radius retry-time		Set the number of retry times back to the default.
Switch(config)# no user radius secret		Set the secret key back to the default.
Switch(config)# no user radius secret-key-encryption		Disable encryption on RADIUS secret key.
Switch(config)# no user radius server1		Set the IP address of the 1 st RADIUS server back to the default.
Switch(config)# no user radius server2		Set the IP address of the 2 nd RADIUS server back to the default.
Show command		
Switch(config)# show user radius		Display the current RADIUS authentication setting.
User command example		
Switch(config)# user radius radius-port 1812		Set the RADIUS port number to 1812.
Switch(config)# user radius retry-time 2		Set the number of retry times to 2.
Switch(config)# user radius secret 1a2b3c		Set the secret key to 1a2b3c.
Switch(config)# user radius server1 172.1.1.2		Set the IP address of the 1 st RADIUS server to 172.1.1.2.

2.5.24 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.

2.5.24.1 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.

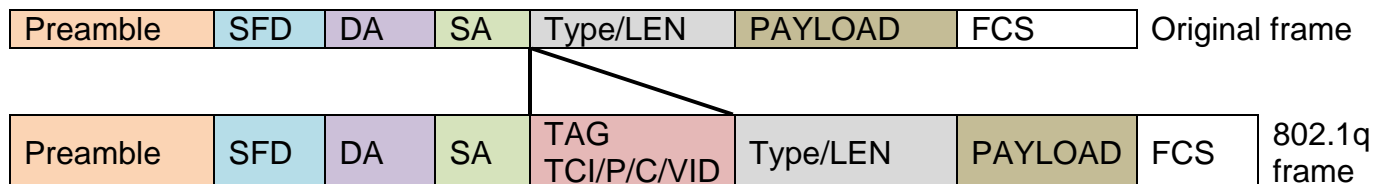
Since source addresses of the packets are listed in MAC address table of specific VLAN (except broadcast/multicast packets), in every VLAN the traffic between two ports will be two-way without restrictions.

2.5.24.2 802.1Q 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 :**

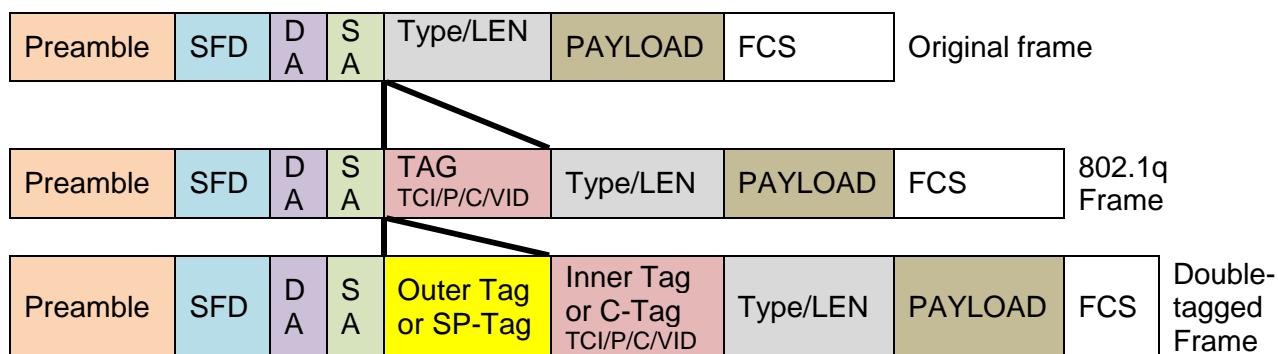
A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.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

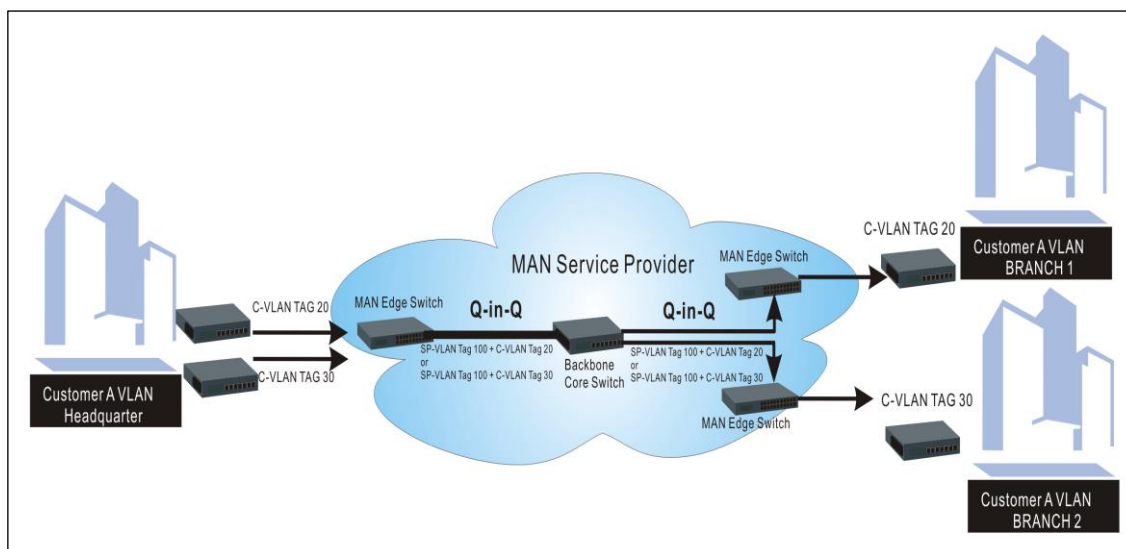
2.5.24.3 Introduction to Q-in-Q (ISP Mode)

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, maximum 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] include-cpu	[name]	Include CPU into any existing Port-Based VLAN.
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-priority [0-7]	[0-7]	Specify an 802.1p bit value for the service tag VID to prioritize different classes of traffic. Valid values are 0 through 7.
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 isp-mode		Disable ISP mode (IEEE 802.1Q double 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-		Reset the 802.1p bit for the service tag to

mode stag-priority		the default. Valid values are 0 through 7.
Switch(config)# no vlan isp-mode stag-ethertype		Reset the service tag's ethertype to the default.
Show command		
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-mod		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 demonstrate 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-vlan 30,40	Set port 3 to port 4's Trunk-VLAN ID (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.

2.5.25 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. Configure QoS rate limit.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# qos rate-limit ingress [0 32- 1000000]	[0 32- 1000000]kbps	Configure the ingress rate limit, from 32Kbps to 1000Mbps. 0:Disable
Switch(config-if-PORT-PORT)# qos rate-limit egress [0 32- 1000000]	[0 32- 1000000]kbps	Configure the egress rate limit, from 32Kbps to 1000Mbps. 0:Disable
No command		
Switch(config-if-PORT-PORT)# no qos rate-limit ingress		Disable QoS ingress rate limit setting.
Switch(config-if-PORT-PORT)# no qos rate-limit egress		Disable QoS egress rate limit setting.

7. 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.

8. Set up port speed.

Command	Parameter	Description
Switch(config-if-PORT- PORT)# speed [1000 100 10]	[1000 100 10]	Configure the port speed as 1000Mbps, 100Mbps or 10Mbps. Note: Speed can only be configured when auto-negotiation is disabled.
No command		
Switch(config-if-PORT- PORT)# no speed		Reset the port speed setting back to the default.

9. Set up VLAN parameters per port.

Command	Parameter	Description
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 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 port. (Tagged and untagged) Note : When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.
Switch(config-if-PORT-PORT)# vlan port-based [name]	[name]	Set the selected ports to any existing port-based VLAN.
No command		
Switch(config-if-PORT-PORT)# no vlan isp-mode isp-port		Reset the selected ports to non-ISP ports (the default setting).
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan access-vlan		Reset the selected ports' PVID back to the default setting.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the specified trunk VLAN ID from the selected ports.
Switch(config-if-PORT-PORT)# no vlan dot1q-vlan mode		Reset the selected ports' 802.1q VLAN mode back to the default setting (Access Mode).
Switch(config-if-PORT-PORT)# no vlan port-based [name]	[name]	Remove the selected ports from the specified port-based VLAN.

2.5.26 Show interface statistics Command

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

Command	Parameters	Description
Switch(config)# show interface		Show the overall interface configuration.
Switch(config)# show interface [port_list]	[port_list]	Show interface configuration of the selected port(s).
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 port(s).
Switch(config)# show interface statistics clear		Clear all statistics counters.
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 port(s).
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 port(s).
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 port(s).
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 port(s).

2.5.27 Show Transceiver Command

Detailed information on the transceivers in use can be viewed by issuing this command.

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

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

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

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

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.

Welcome: admin

System Setup » Switch Information

Company Name	Connection Technology Systems		
System Object ID	.13.6.1.4.1.9304.100.31066		
System Contact	info@ctsystem.com		
System Name	HES-3106B-SE-DR		
System Location	18F-6, No. 79, Sec. 1, Xintai 5th Rd., Xizhi Dist., Taiwan		
DHCPv4/DHCPv6 Vendor ID	HES-3106B-SE-DR		
Model Name	HES-3106B-SE-DR		
Host Name	HES-3106B-SE-DR		
Current Boot Image	Image-1		
Configured Boot Image	Image-1		
Image-1 Version	0.99.0F		
Image-2 Version	0.99.0F		
M/B Version	A01		
WAN Transceiver Type	100/1000M 10KM		
WAN Transceiver Vendor	CTS-INC	WAN Transceiver PN	CTS-W2A-10KM-DR
CATV RF Status	N/A	CATV RF Module	Disabled
Serial Number	ABBCCDEF0000000	Date Code	20220606
Up Time	0 day 00:22:35	Local Time	Not Available

Ok Reset

There are 11 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.
- **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 5 options within this folder will be displayed as follows.

The screenshot displays the 'System Setup' web interface. On the left is a navigation menu with 'System Setup' expanded to show 'Switch Information', 'IP Setup', 'IP Source Binding', 'Time Server Setup', and 'Syslog Setup'. The main content area is titled 'System Setup > Switch Information' and contains a form with the following fields:

Company Name	Connection Technology Systems		
System Object ID	.1.3.6.1.4.1.9304.100.31066		
System Contact	info@ctsystem.com		
System Name	HES-3106B-SE-DR		
System Location	18F-6, No. 79, Sec. 1, Xintai 5th Rd., Xizhi Dist., Taiwan		
DHCPv4/DHCPv6 Vendor ID	HES-3106B-SE-DR		
Model Name	HES-3106B-SE-DR		
Host Name	HES-3106B-SE-DR		
Current Boot Image	Image-1		
Configured Boot Image	Image-1		
Image-1 Version	0.99.0F		
Image-2 Version	0.99.0F		
M/B Version	A01		
WAN Transceiver Type	100/1000M 10KM		
WAN Transceiver Vendor	CTS-INC	WAN Transceiver PN	CTS-W2A-10KM-DR
CATV RF Status	N/A	CATV RF Module	Disabled
Serial Number	ABBCEDEF0000000	Date Code	20220606
Up Time	0 day 00:09:17	Local Time	Not Available

At the bottom of the form are two buttons: 'Ok' and 'Reset'.

1. **Switch Information:** Name the Managed Switch, specify the location and check the current version of information
2. **IP Setup:** Set up the required IP configuration of the Managed Switch.
3. **IP Source Binding:** Set up the IP address for source binding.
4. **Time Server Setup:** Set up the time server's configuration.
5. **Syslog Setup:** Set up the Mal-attempt Log server's configuration.

4.1.1 System Information

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

System Setup » Switch Information			
Company Name	Connection Technology Systems		
System Object ID	.1.3.6.1.4.1.9304.100.31066		
System Contact	info@ctsystem.com		
System Name	HES-3106B-SE-DR		
System Location	18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan		
DHCPv4/DHCPv6 Vendor ID	HES-3106B-SE-DR		
Model Name	HES-3106B-SE-DR		
Host Name	HES-3106B-SE-DR		
Current Boot Image	Image-1		
Configured Boot Image	Image-1		
Image-1 Version	0.99.0F		
Image-2 Version	0.99.0F		
M/B Version	A01		
WAN Transceiver Type	100/1000M 10KM		
WAN Transceiver Vendor	CTS-INC	WAN Transceiver PN	CTS-W2A-10KM-DR
CATV RF Status	N/A	CATV RF Module	Disabled ▾
Serial Number	ABBCCDEF0000000	Date Code	20220606
Up Time	0 day 00:09:17	Local Time	Not Available

Ok Reset

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

System Object ID: Display the predefined System OID.

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

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

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

DHCP/DHCPv6 Vendor ID: Vendor Class Identifier. Enter the user-defined DHCP vendor ID, up to 55 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.

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.

WAN Transceiver Type: The information about the WAN transceiver type.

WAN Transceiver Vendor: Vendor name of the WAN transceiver.

WAN Transceiver PN: Vendor PN of the WAN transceiver.

***CATV RF Status:** View-only field that shows whether RF TV is ready or not.

***CATV RF Module:** Turn on or off the RF TV Output. (only configurable for models with a CATV RF module)

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.

The screenshot shows the 'System Setup >> IP Setup' page. On the left is a navigation menu with 'System Setup' expanded to show 'IP Setup'. The main content area is divided into two sections: IPv4 and IPv6.

IPv4 Section:

- Enable IPv4: Enabled (dropdown)
- MAC Address: 00:06:19:98:76:54
- Configuration Type: Manual (dropdown)
- Current State: (empty)
- IPv4 Address: 192.168.0.150 (input field) | 192.168.0.150 (Current State)
- Subnet Mask: 255.255.255.0 (input field) | 255.255.255.0 (Current State)
- Gateway: 0.0.0.0 (input field) | 0.0.0.0 (Current State)

IPv6 Section:

- Enable IPv6: Disabled (dropdown)
- Auto-configuration: Enabled (dropdown)
- Current State: (empty)
- IPv6 Link-local Address/Prefix Length: fe80::206:19ff:fe98:7654/64 (input field) | ::/0 (Current State)
- IPv6 Global Address/Prefix Length: ::/64 (input field)
- IPv6 Gateway: :: (input field)
- DHCPv6: Enable force mode (dropdown)
- Rapid Commit:
- DHCPv6 Unique Identifier (DUID): (input field)

At the bottom are 'Ok' and 'Reset' buttons.

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.

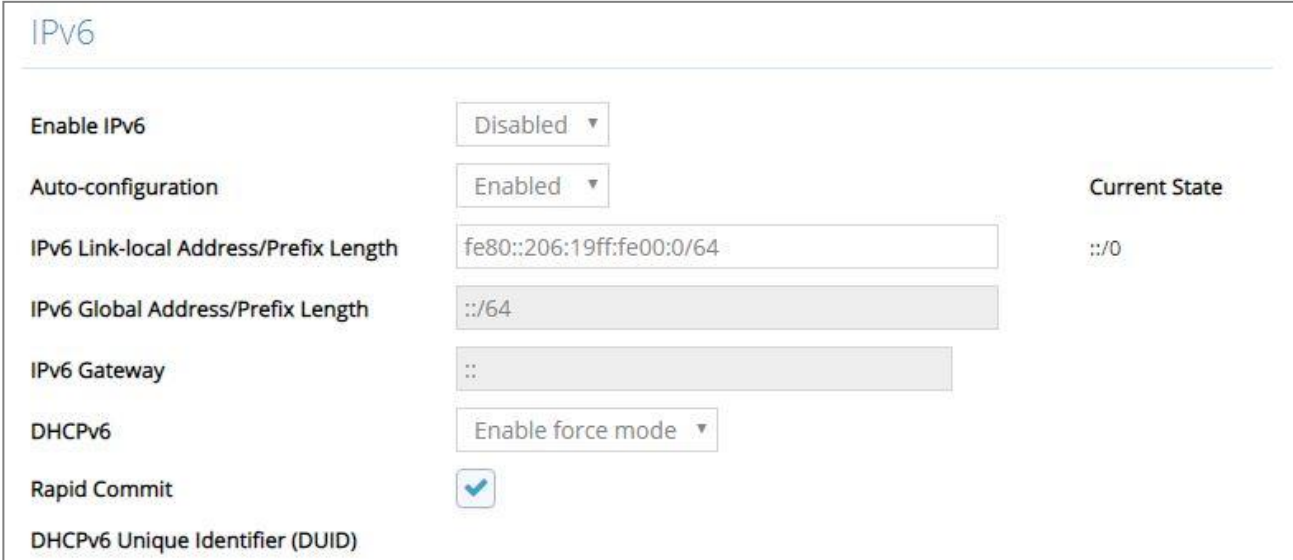
IPv4 Address: Enter the unique IP address of this Managed Switch. You can use the default IP address or specify a new one when the situation of address duplication occurs or the address does not match up with your network. (The default factory setting is 192.168.0.1.)

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.



The screenshot shows the IPv6 configuration page. At the top, the title 'IPv6' is displayed. Below it, there are several configuration options:

- Enable IPv6:** A dropdown menu set to 'Disabled'.
- Auto-configuration:** A dropdown menu set to 'Enabled'. To its right, the text 'Current State' is visible.
- IPv6 Link-local Address/Prefix Length:** A text input field containing 'fe80::206:19ff:fe00:0/64'. To its right, the text 'Current State' is followed by '::/0'.
- IPv6 Global Address/Prefix Length:** A text input field containing '::/64'.
- IPv6 Gateway:** A text input field containing '::'.
- DHCPv6:** A dropdown menu set to 'Enable force mode'.
- Rapid Commit:** A checkbox that is checked.
- DHCPv6 Unique Identifier (DUID):** A text input field that is currently empty.

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.

Index	State	IPv4/IPv6 Address
1	Disabled	0.0.0.0
2	Disabled	0.0.0.0
3	Disabled	0.0.0.0
4	Disabled	0.0.0.0
5	Disabled	0.0.0.0

Ok Reset

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

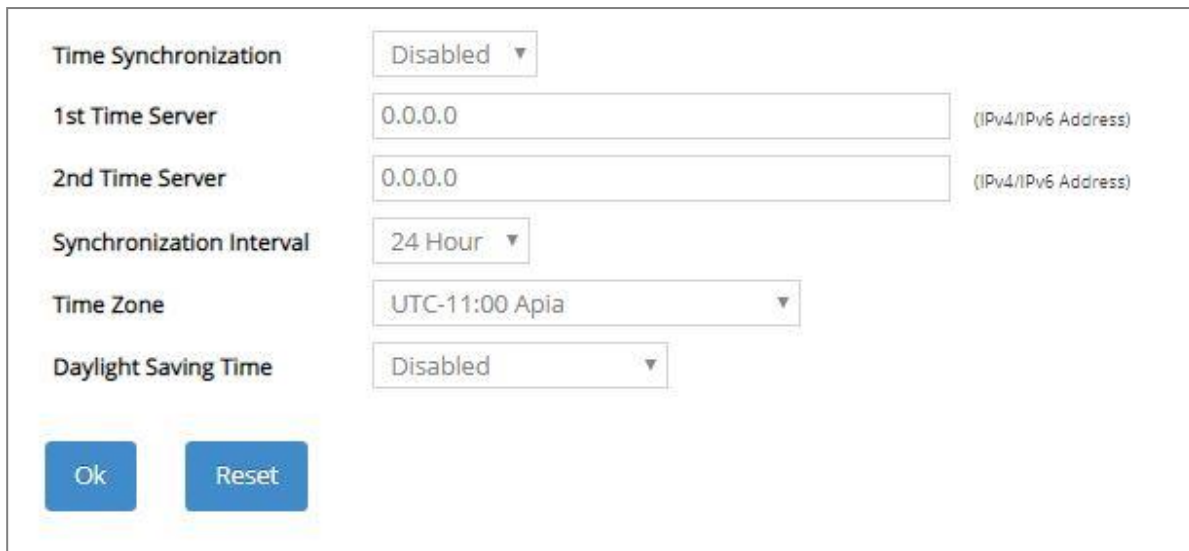
State: Disable or enable the assigned IP address to reach the management.

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	Disabled	
1st Time Server	0.0.0.0	(IPv4/IPv6 Address)
2nd Time Server	0.0.0.0	(IPv4/IPv6 Address)
Synchronization Interval	24 Hour	
Time Zone	UTC-11:00 Apia	
Daylight Saving Time	Disabled	

Ok Reset

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

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

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

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

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

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

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

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

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

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

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

4.1.5 Syslog Configuration

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

The screenshot shows the 'Log Server' configuration page. It includes the following fields and options:

- Log Server:** A dropdown menu currently set to 'Disabled'.
- SNTP Status:** A text field set to 'Disabled'.
- Facility:** A dropdown menu currently set to 'Local 0'.
- 1st Log Server:** A text input field containing '0.0.0.0' with a placeholder '(IPv4/IPv6 Address)'.
- 2nd Log Server:** A text input field containing '0.0.0.0' with a placeholder '(IPv4/IPv6 Address)'.
- 3rd Log Server:** A text input field containing '0.0.0.0' with a placeholder '(IPv4/IPv6 Address)'.

Below the log server fields is the 'Logging Type' section, which includes:

- Terminal History:** A dropdown menu currently set to 'Disabled'.

At the bottom of the page are two blue buttons: 'Ok' and 'Reset'.

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

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

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

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

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

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

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

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

4.2 Port Management

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

The screenshot displays the 'Port Management' configuration page. The breadcrumb trail is 'Port Management > Port Setup & Status'. The 'Maximum Frame Size' is set to 16367 Bytes (1518-16367). A 'Quick Select' dropdown is set to '1,2,3-6'. The main table lists the following port configurations:

Select	Port	Port State			Description	Preferred Media Type	Port Type	Speed			Flow Control	MAC Address
		Enable	State	Reason				State	Speed	Duplex		
<input type="checkbox"/>	All	<input type="checkbox"/>	--	--				--			<input type="checkbox"/>	--
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Up	--		Copper	Auto-Negotiation	1000 Mbps / Full	1000Mbps	Full	<input type="checkbox"/>	00:06:19:98:76:55
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Down	Link Down		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:98:76:56
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Down	Link Down		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:98:76:57
<input type="checkbox"/>	4	<input checked="" type="checkbox"/>	Down	Link Down		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:98:76:58
<input type="checkbox"/>	5	<input checked="" type="checkbox"/>	Down	Link Down		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:98:76:59
<input type="checkbox"/>	6	<input checked="" type="checkbox"/>	Down	Link Down		Fiber	Auto-Negotiation	--	Auto-Sense	Full	<input type="checkbox"/>	00:06:19:98:76:5A

Buttons for 'Ok' and 'Reset' are located at the bottom left of the table area.

- 1. Port Setup & Status:** Set up frame size, enable/disable port state & flow control, and view current port media type, port state, etc.
- 2. Port Traffic Statistics:** View each port's frames and bytes received or sent, utilization, etc.
- 3. Port Packet Error Statistics:** View each port's traffic condition of error packets, e.g. CRC, fragment, Jabber, etc.
- 4. Port Packet Analysis Statistics:** View each port's traffic analysis of packets, e.g. RX/TX frames of Multicast and Broadcast, etc.
- 5. Port Mirroring:** Set up TX/RX source port(s) to mirror to the destination port for the traffic monitoring.

4.2.1 Port Setup & Status

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

Maximum Frame Size Bytes (1518-16367) Quick Select

Select	Port	Port State			Description	Preferred Media Type	Port Type	Speed			Flow Control	MAC Address
		Enable	State	Reason				State	Speed	Duplex		
<input type="checkbox"/>	All	<input type="checkbox"/>	--	--				--			<input type="checkbox"/>	--
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Up	--		Copper	Auto-Negotiation	1000 Mbps / Full	1000Mbps	Full	<input type="checkbox"/>	00:06:19:98:76:55
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Down	Link Down		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:98:76:56
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Down	Link Down		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:98:76:57
<input type="checkbox"/>	4	<input checked="" type="checkbox"/>	Down	Link Down		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:98:76:58
<input type="checkbox"/>	5	<input checked="" type="checkbox"/>	Down	Link Down		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:98:76:59
<input type="checkbox"/>	6	<input checked="" type="checkbox"/>	Down	Link Down		Fiber	Auto-Negotiation	--	Auto-Sense	Full	<input type="checkbox"/>	00:06:19:98:76:5A

Maximum Frame Size: Specify the maximum frame size between 1518 and 16367 bytes. The default maximum frame size is 16367 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, 3-7) in the **Quick Select** field located at the top-right corner of the Port Setup & Status table, the specified port(s) will be checked immediately when pressing the **Select** button in back of it. The new settings configured in the row of **All** port will be applied to these checked ports.

Port: The number of the port.

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

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

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

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

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

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

State of Port in Speed field: View-only field that shows the current operation speed of ports, which can be 10Mbps/100Mbps/1000Mbps in copper port(s) 1-5 and 100Mbps/1000Mbps in the fiber port 6, and the current operation duplex mode of the port, either Full or Half.

Speed of Port in Speed field: When you select "Manual" as port type, you can further specify the transmission speed (10Mbps/100Mbps/1000Mbps) of copper port(s) 1-5 and (auto-sense/100Mbps/1000Mbps) of the fiber port 6. When you select "Auto-Negotiation" as port type for fiber port(s), the transmission speed is 1000Mbps.

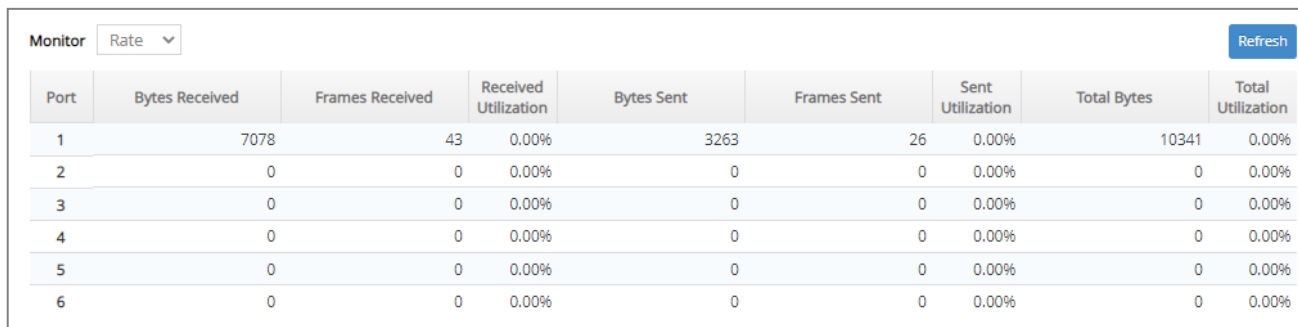
Duplex of Port in Speed field: In fiber ports, only the full-duplex operation mode is allowed.

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	7078	43	0.00%	3263	26	0.00%	10341	0.00%
2	0	0	0.00%	0	0	0.00%	0	0.00%
3	0	0	0.00%	0	0	0.00%	0	0.00%
4	0	0	0.00%	0	0	0.00%	0	0.00%
5	0	0	0.00%	0	0	0.00%	0	0.00%
6	0	0	0.00%	0	0	0.00%	0	0.00%

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.

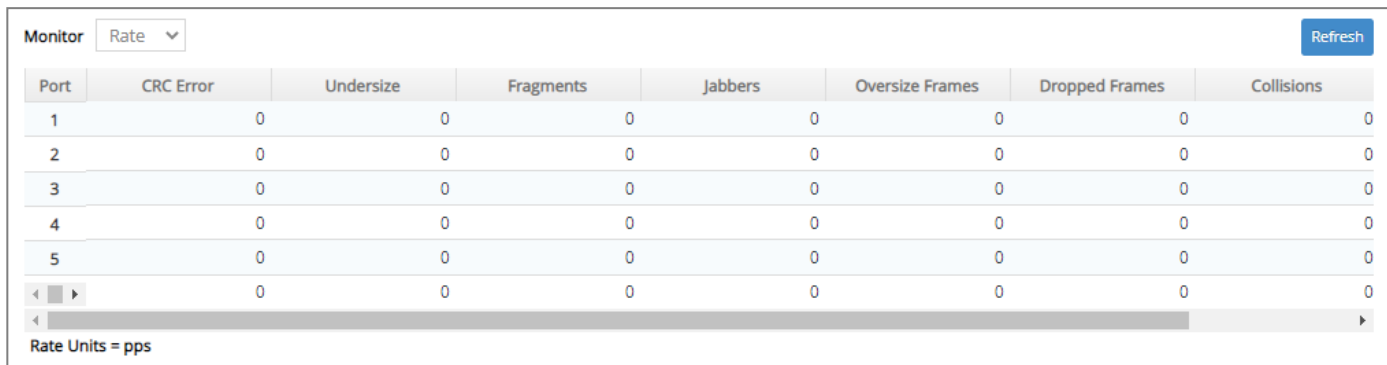
Refresh: Click **Refresh** to update the latest port traffic statistics.

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.



Port	CRC Error	Undersize	Fragments	Jabbers	Oversize Frames	Dropped Frames	Collisions
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
< >	0	0	0	0	0	0	0

Rate Units = pps

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

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

RX Undersize: Undersize frames received.

RX Fragments: Fragments frames received.

RX Jabbers: Jabber frames received.

RX Oversize Frames: Oversize frames received.

RX Dropped Frames: Drop frames received.

TX Collisions: Each port’s Collision frames.

TX Dropped Frames: Drop frames sent.

Total Errors: Total error frames received.

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

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

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

4.2.4 Port Packet Analysis Statistics

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

Packet Statistics	Port 1 Clear		Port 2 Clear		Port 3 Clear		Port 4 Clear		Port 5 Clear		Port 6 Clear	
	Rate	Event	Rate	Event	Rate	Event	Rate	Event	Rate	Event	Rate	Event
Frames 64 Bytes	8	26913	0	0	0	0	0	0	0	0	0	2018
Frames 65-127 Bytes	0	16767	0	0	0	0	0	0	0	0	0	3355
Frames 128-255 Bytes	0	4436	0	0	0	0	0	0	0	0	0	287
Frames 256-511 Bytes	0	706	0	0	0	0	0	0	0	0	0	2
Frames 512-1023 Bytes	0	5504	0	0	0	0	0	0	0	0	0	1136
Frames 1024-1518 Bytes	0	16307	0	0	0	0	0	0	0	0	0	403
Frames 1519-Max Bytes	0	0	0	0	0	0	0	0	0	0	0	0
Rx Multicast Frames	0	8171	0	0	0	0	0	0	0	0	0	0
Tx Multicast Frames	0	0	0	0	0	0	0	0	0	0	0	2489
Rx Broadcast Frames	0	1280	0	0	0	0	0	0	0	0	0	0
Tx Broadcast Frames	0	0	0	0	0	0	0	0	0	0	0	398

Rate Units = pps

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

RX Frames 64 Bytes: 64 bytes frames received.

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

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

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

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

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

RX Frames 1519-Max Bytes: Over 1519 bytes frames received.

RX Multicast Frames: Good multicast frames received.

TX Multicast Frames: Good multicast packets sent.

RX Broadcast Frames: Good broadcast frames received.

TX Broadcast Frames: Good broadcast packets sent.

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

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

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

4.2.5 Port Mirroring

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

Note !!
Port Isolation and Port Mirroring can not be enabled at the same time.
When you enable Port Isolation, Port Mirroring is automatically disabled and vice versa.
Tx/Rx source port must be the same interface if you are to specify both.
Tx/Rx source port can only accept one interface.

Port Mirroring

Occupied/Max Entry: 0/1

Index	Enabled	Source Port		Destination Port	Action
		Tx	Rx		

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

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

Occupied/Max Entry: View-only field.

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

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

Occupied/Max Entry: 0/1



Index	Enabled	Source Port		Destination Port	Action
		Tx	Rx		

Enabled: Enable or disable the specific port mirroring.


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

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

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

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

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

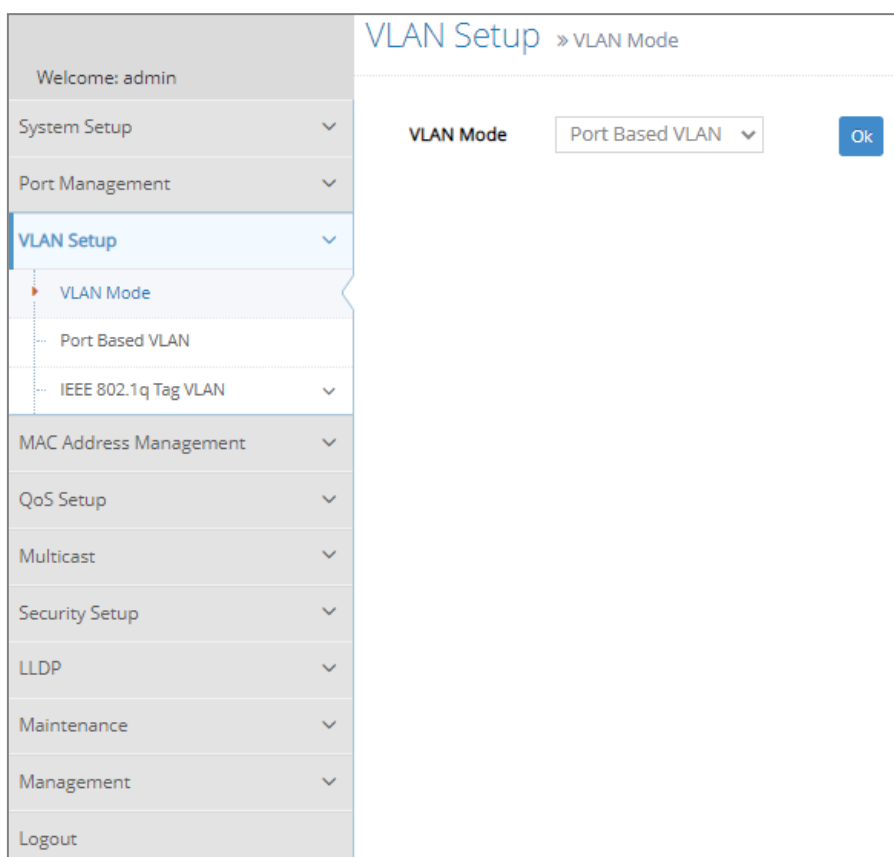
Click the  icon to remove a specified port mirroring entry and its settings from the port mirroring table. Or click **Batch Delete** to remove a number of /all port mirrorings at a time by clicking on the checkbox belonging to the corresponding port mirroring in the **Action** field and then click **Delete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

4.3 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.



The screenshot shows a configuration window with a label "VLAN Mode" on the left. To its right is a dropdown menu with the text "IEEE 802.1q VLAN" and a downward arrow. Further to the right is a blue button with the text "Ok".

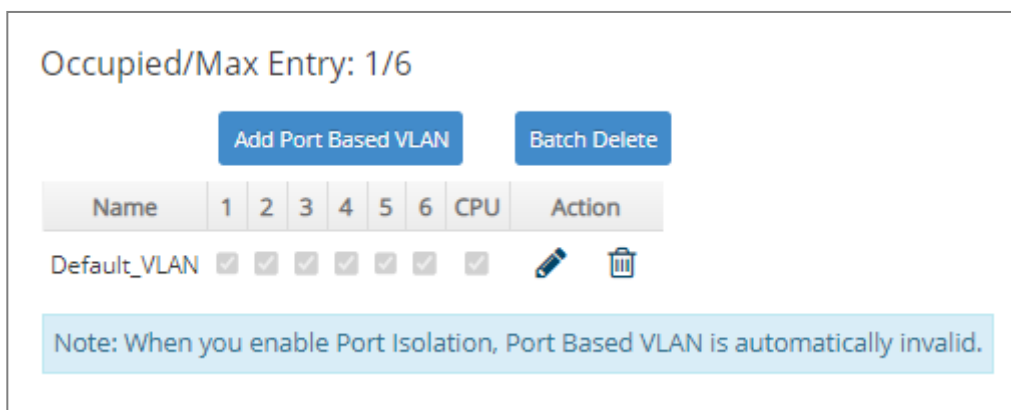
VLAN Mode: Specify **Port Based VLAN** or **IEEE 802.1q Tag VLAN** from the pull-down menu. The Managed Switch will run VLAN accordingly to the mode that which you decide on. You can then go to Port Based VLAN or IEEE 802.1q VLAN web pages to configure in depth.

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.

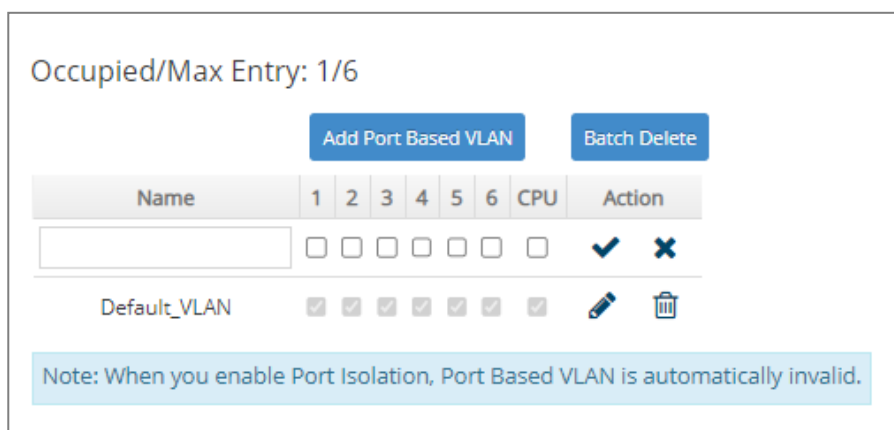


Since source addresses of the packets are listed in MAC address table of specific VLAN (except broadcast/multicast packets), in every VLAN the traffic between two ports will be two-way without restrictions.

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 6.

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

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

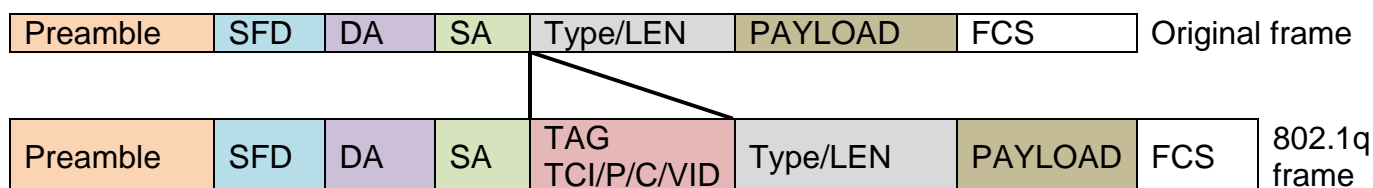
Click  when the settings are completed, this new Port-Based VLAN will be listed on the Port-Based VLAN table, or click  to cancel the settings.

4.3.3 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.

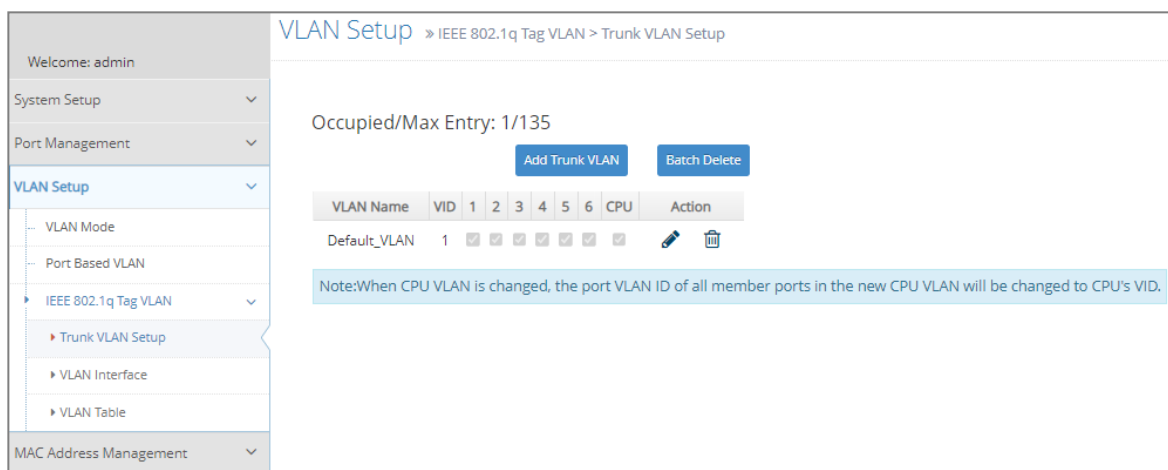
- Trunk Native Mode :

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

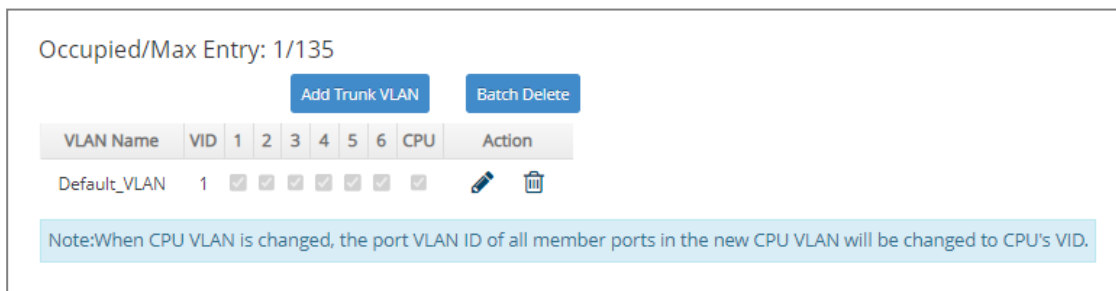
The following screen page appears when you choose the option **IEEE 802.1q Tag VLAN** mode from the **VLAN Setup** menu.



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

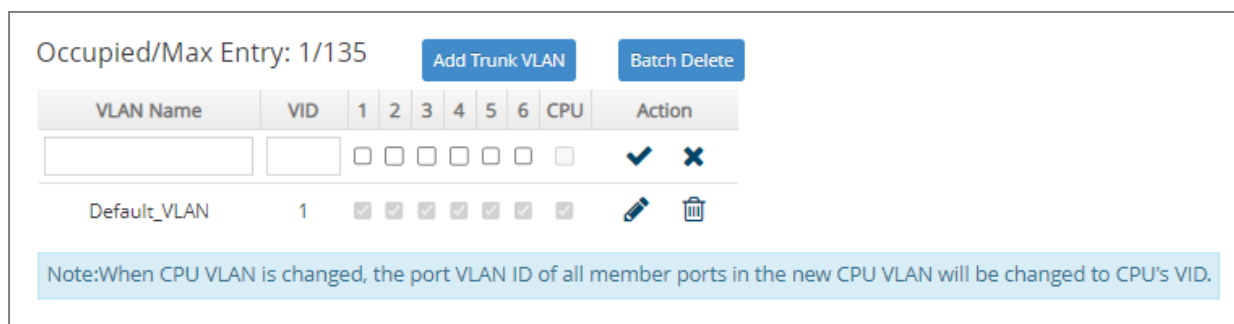
The following screen page appears if you choose **Trunk VLAN Setup** function.



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 135.

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.

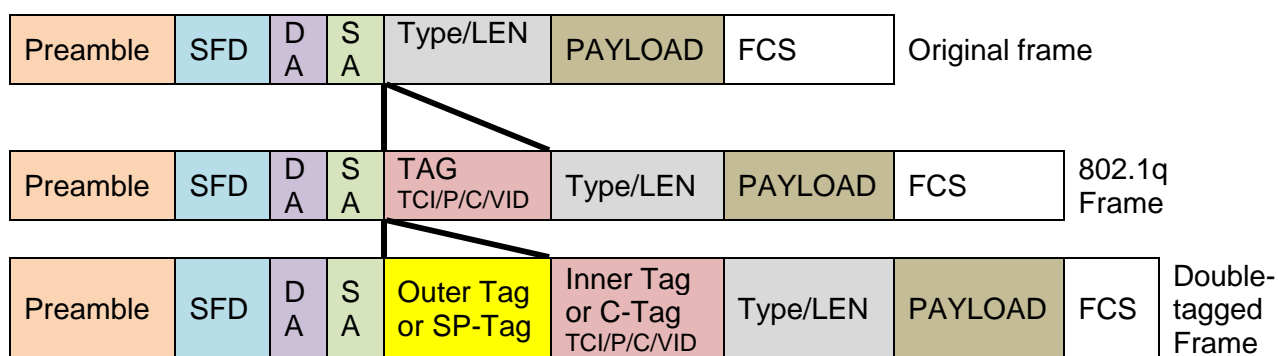
Click  when the settings are completed, this new 802.1q VLAN will be listed on the IEEE 802.1q Tag VLAN Setup table, or click  to cancel the settings.

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.

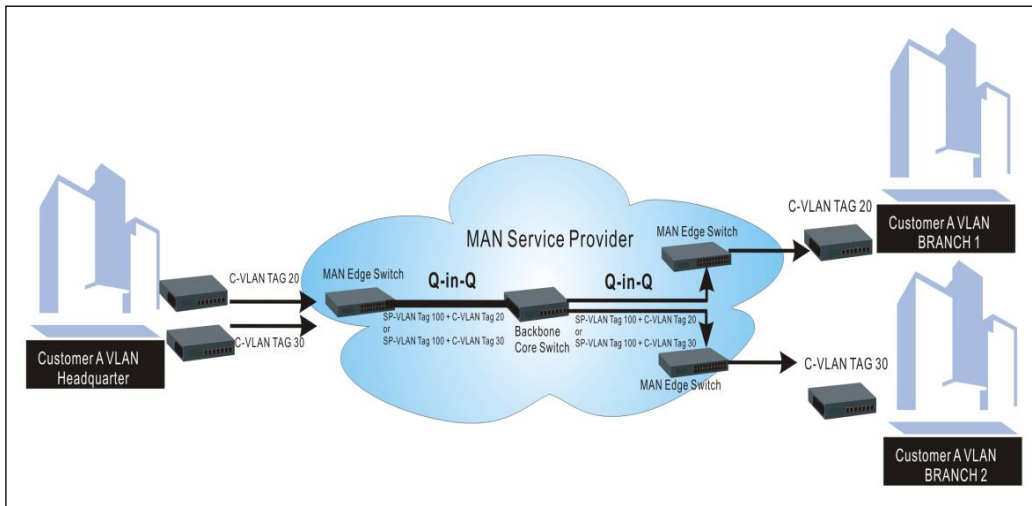
Introduction to Q-in-Q (ISP Mode)

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 (1-4094)

ISP Mode

Stag VID (1-4094)

Stag Priority (0-7)

Stag EtherType 0x (0000-FFFF)

Select	Port	Mode	PVID	Trunk-VLAN	ISP Port
<input type="checkbox"/>	All	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="checkbox"/>
<input type="checkbox"/>	1	ACCESS	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="checkbox"/>
<input type="checkbox"/>	2	ACCESS	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	ACCESS	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	ACCESS	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	ACCESS	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	ACCESS	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="checkbox"/>

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.

Stag Priority: Specify an 802.1p bit value for the service tag VID to prioritize different classes of traffic. Valid values are 0 through 7.

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).

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 configuring, 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.

U: Untagged T: Tagged V: Member -: Not Member								
VLAN Name	VID	1	2	3	4	5	6	CPU
Default_VLAN	1	U	U	U	U	U	U	V

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.

MAC Address Management > MAC Table Learning

Welcome: admin

System Setup

Port Management

VLAN Setup

MAC Address Management

MAC Table Learning

MAC Address Table

QoS Setup

MAC Address Aging Time Secs (0-458)

MAC Address Learning Per Port Select All

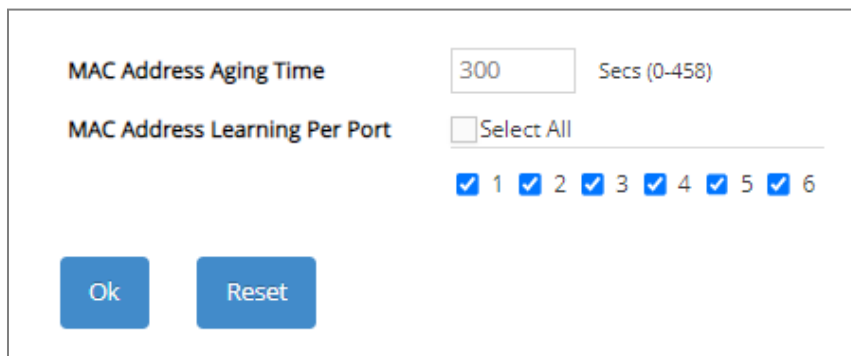
1 2 3 4 5 6

Ok Reset

- 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.



The screenshot displays a configuration window with the following elements:

- MAC Address Aging Time:** A text input field containing the value "300" and a label "Secs (0-458)".
- MAC Address Learning Per Port:** A section containing a "Select All" checkbox and six individual checkboxes labeled "1" through "6". All checkboxes are checked.
- Buttons:** Two blue buttons labeled "Ok" and "Reset" are positioned at the bottom left of the window.

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.

Capacity	Free	Used	Dynamic	Static	Internal
16384	16384	0	0	0	0

Clear All **Clear by Port List** 1,2,3-7

MAC Address Filter Condition

Type: All

MAC: All AA:BB:CC:DD:EE:FF Mask: FF:FF:FF:FF:FF:FF

VLAN: All 1 (1-4094)

Port List: All 1,2,3-7

Sort by: Port

Search

MAC Address 0 Entries

Index	Type	MAC Address	VID	Port	Add to Static
-------	------	-------------	-----	------	---------------

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

- 1. Capacity:** The maximum number of the MAC address entries allowed to be kept on the Managed Switch.
- 2. Free:** The available number of the MAC address entries still allowed to be kept on the Managed Switch.
- 3. Used:** The number of the MAC address entries already kept on the Managed Switch.
- 4. Dynamic:** The number of the dynamic MAC addresses entries already kept on the Managed Switch.
- 5. Static:** The number of the static MAC addresses entries already kept on the Managed Switch.
- 6. Internal:** The MAC address of the Managed Switch.

The table that sits at the very bottom of the page is composed of the MAC addresses that are automatically learned from each port of Managed Switch or manually created by the users. Click **Clear All** to clear all dynamic MAC addresses in the MAC address table. Or click **Clear by Port List** to clear the dynamic MAC addresses for the specified port(s).

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

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

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

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

3. **VLAN:** Select **All**, **Include**, or **Exclude** to determine the filtering behavior, and specify the VLAN ID to be filtered with.
4. **Port List:** Select **All**, **Include**, or **Exclude** to determine the filtering behavior, and specify the port to be filtered with.
5. **Sort by:** Select **Port**, **MAC**, or **VLAN** to determine the arrangement of the MAC address entries displayed in the table. Each option is described below:

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

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

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

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

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

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

4.5 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.

The screenshot displays the 'QoS Setup' configuration page. The sidebar menu on the left includes 'Welcome: admin', 'System Setup', 'Port Management', 'VLAN Setup', 'MAC Address Management', 'QoS Setup' (highlighted), 'QoS Priority', 'QoS Remarking', 'QoS Rate Limit', 'Multicast', and 'Security Setup'. The main content area is titled 'QoS Setup » QoS Priority' and contains the following settings:

- QoS Priority**
- Priority Mode:** Disable (dropdown menu)
- Queue Mode:** Strict (dropdown menu)
- User Priority**

Port	1	2	3	4	5	6	CPU
Priority	0	0	0	0	0	0	0

At the bottom of the page, there are two buttons: 'Ok' and 'Reset'.

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.

Port	1	2	3	4	5	6	CPU
Priority	0	0	0	0	0	0	0

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.

Disabled: Disable QoS.

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

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

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

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

Queue Weight	Q0 1	: Q1 2	: Q2 4	: Q3 8	: Q4 16	: Q5 32	: Q6 64	: Q7 127	(1-127)
--------------	------	--------	--------	--------	---------	---------	---------	----------	---------

Port to Queue Mapping: Assign a priority level to interfaces to prioritize network traffic. The higher the number is, the higher the priority.

Port to Queue Mapping

Port	1	2	3	4	5	6	CPU
Queue	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾

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

802.1p to Queue Mapping

802.1p	0	1	2	3	4	5	6	7
Queue	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾

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.

DSCP to Queue Mapping

DSCP Value List (e.g. 1,2,3-7) Queue

DSCP	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Queue	Q0 ▾	Q5 ▾	Q5 ▾	Q5 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾
DSCP	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Queue	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾
DSCP	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
Queue	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾
DSCP	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
Queue	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾	Q0 ▾

User Priority:

User Priority

Port	1	2	3	4	5	6	CPU
Priority	0	0	0	0	0	0	0

There are eight priority levels that you can choose to classify data packets. Specify one of the

listed options for CoS (Class of Service) priority tag values. The default value is “0”.

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

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

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.

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

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

Ok Reset

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.

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

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.

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

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.

		Ingress			Egress		
Select	Port	Enabled	Rate (500-1000000 Kbits/Sec)	Unit	Enabled	Rate (500-1000000 Kbits/Sec)	Unit
<input checked="" type="checkbox"/>	All	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	1	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>	500	Kbps
<input type="checkbox"/>	2	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>	500	Kbps
<input type="checkbox"/>	3	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>	500	Kbps
<input type="checkbox"/>	4	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>	500	Kbps
<input type="checkbox"/>	5	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>	500	Kbps
<input type="checkbox"/>	6	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>	500	Kbps

Quick Select: 1,2,3-6

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

Port: The number of each port.

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

Rate in Ingress/Egress field: Specify the transmitting rate limit of the inbound and outbound bandwidth. Valid range is from 500 ~1000000 in unit of Kbps or 1~1000 in unit of Mbps.

Unit in Ingress/Egress field: Either Kbps or Mbps can be selected 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.

The screenshot shows a network management interface with a sidebar on the left and a main configuration area on the right. The sidebar contains a menu with the following items: System Setup, Port Management, VLAN Setup, MAC Address Management, QoS Setup, Multicast, IGMP/MLD Snooping, IGMP/MLD Setup, IGMP/MLD VLAN Setup, IGMP Snooping Status, IGMP Group Table, MLD Snooping Status, and MLD Group Table. The 'Multicast' folder is expanded, and 'IGMP/MLD Setup' is selected. The main configuration area is titled 'Multicast > IGMP/MLD Snooping > IGMP/MLD Setup'. It contains the following settings: IGMP/MLD Snooping (Disabled), IGMPv3/MLDv2 Snooping (Disabled), Unregistered IPMC Flooding (Disabled), Query Interval (125 Secs (1-6000)), Query Response Interval (100 1/10 Secs (1-255)), Fast Leave (Disabled), and Router Port (Select All). Below these settings are radio buttons for ports 1 through 6. A blue error message box states: 'Query interval must be greater than Query Response interval.' At the bottom of the configuration area are 'Ok' and 'Reset' buttons.

1. **IGMP/MLD Setup:** To enable or disable IGMP/MLD Snooping, IGMPv3/MLDv2 Snooping, Unregistered IPMC Flooding and set up router ports.
2. **IGMP/MLD VLAN Setup:** To set up the ability of IGMP/MLD snooping and querying with VLAN.
3. **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 ▾

IGMPv3/MLDv2 Snooping ▾

Unregistered IPMC Flooding ▾

Query Interval Secs (1-6000)

Query Response Interval 1/10 Secs (1-255)

Fast Leave ▾

Router Port Select All

1 2 3 4 5 6

Query interval must be greater than Query Response interval.

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

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

Unregistered IPMC Flooding: Set forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic will flood when enabled. However, the traffic will be forwarded to router-ports only when disabled.

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

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

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

Router Port: When ports are connected to the IGMP administrative routers, they should be checked. Or directly input the port number (e.g.1, 2, 3-7) in the **Quick Select** field and then press the **Select** button, the specified port(s) will be checked immediately. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

4.6.1.2 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 functions of IGMP Snooping and Querying in VLAN(s) appears.

Select	VID	VLAN Name	Snooping	Querying
<input type="checkbox"/>	All	--	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	1	Default_VLAN	Disabled <input type="text"/>	Disabled <input type="text"/>

VID: VID of the specific VLAN. And VID marked * stands that it is a MVR VLAN ID.

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

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

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

4.6.1.3 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. And VLAN ID marked * stands that it is a MVR VLAN ID.

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

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

Querier: The state of IGMP querier in the VLAN.

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

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

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

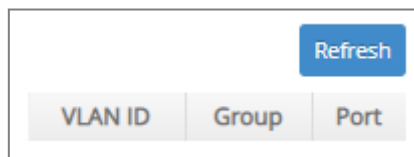
v2 Reports: The total amount of received IGMP Version 2 reports (packets).

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

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

4.6.1.4 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.



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

VLAN ID: VID of the specific VLAN. And VLAN ID marked * stands that it is a MVR VLAN ID.

Group: The multicast IP address of IGMP querier.

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

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.



The screenshot shows a web interface for MLD Snooping Status. At the top right, there is a blue button labeled "Refresh". Below it is a table with the following headers: "VLAN ID", "Querier", "Queries Transmitted", "Queries Received", "v1 Reports", "v2 Reports", and "Done".

VLAN ID	Querier	Queries Transmitted	Queries Received	v1 Reports	v2 Reports	Done
---------	---------	---------------------	------------------	------------	------------	------

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

VLAN ID: VID of the specific VLAN. And VLAN ID marked * stands that it is a MVR VLAN ID.

Querier: The state of MLD querier in the VLAN.

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

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

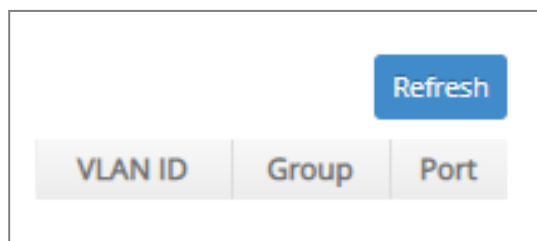
v1 Reports: The total amount of received MLD Version 1 reports (packets).

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

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

4.6.1.6 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.



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

VLAN ID: VID of the specific VLAN. And VLAN ID marked * stands that it is a MVR VLAN ID.

Group: The multicast IP address of MLD querier.

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

4.7 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

The screenshot shows the 'Security Setup' configuration page for DHCP Snooping. The left sidebar contains a navigation menu with the following items: System Setup, Port Management, VLAN Setup, MAC Address Management, QoS Setup, Multicast, Security Setup (highlighted), DHCP Snooping (expanded), Port Isolation, Storm Control, Loop Detection, LLDP, Maintenance, and Management. The main content area is titled 'Security Setup » DHCP Snooping » DHCP Snooping Setup'. It features the following settings:

- DHCPv4/DHCPv6 Snooping:** Disabled (dropdown)
- Default DHCP Initiated Time:** 4 (text input) Secs (0-9999)
- Default DHCP Leased Time:** 86400 (text input) Secs (180-259200)
- DHCP Server Trust Port:** Select All, with checkboxes for ports 1, 2, 3, 4, 5, and 6.
- DHCP Server Trust IP:** DHCP Server Trust IP State: Disabled (dropdown)
- IPv4/IPv6 Address-1:** 0.0.0.0 (text input)
- IPv4/IPv6 Address-2:** 0.0.0.0 (text input)
- IPv4/IPv6 Address-3:** 0.0.0.0 (text input)
- IPv4/IPv6 Address-4:** 0.0.0.0 (text input)

At the bottom of the configuration area are 'Ok' and 'Reset' buttons.

- 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: Disabled

Default DHCP Initiated Time: 4 Secs (0-9999)

Default DHCP Leased Time: 86400 Secs (180-259200)

DHCP Server Trust Port: Select All

1 2 3 4 5 6

DHCP Server Trust IP

DHCP Server Trust IP State: Disabled

IPv4/IPv6 Address-1: 0.0.0.0

IPv4/IPv6 Address-2: 0.0.0.0

IPv4/IPv6 Address-3: 0.0.0.0

IPv4/IPv6 Address-4: 0.0.0.0

Ok Reset

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

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

4.7.1.2 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.

Select	Port	Opt82 / Opt37		Circuit-ID		
		Enabled	Trust Port	Enabled	Formatted	Contents
<input type="checkbox"/>	All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Remote-ID

Remote-ID Enable

Remote-ID Formatted

Remote-ID

Current Remote-ID 00:06:19:98:76:54

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 configuring, 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
<input checked="" type="checkbox"/>	All	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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 mechanisms 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.



Index	Port		VID	IP Address		Client MAC Address	Time Left
	Client	Server		Client	Server		

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 address is obtained from.

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

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

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

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

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

4.7.2 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 invalid automatically. Also note that "Port Isolation" function is not "Private VLAN" function.

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

Note: "Port Isolation" function is not "Private VLAN" function.

When you enable Port Isolation, Port Based VLAN is automatically invalid.

Port Isolation Enable: Disabled

Uplink Port: Select All

1 2 3 4 5 6

Ok Reset

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.

Select	Port	Unknown Unicast Rate	Unknown Multicast Rate	Broadcast Rate
<input type="checkbox"/>	All	<input type="text"/> pps	<input type="text"/> pps	<input type="text"/> pps
<input type="checkbox"/>	1	Off pps	Off pps	Off pps
<input type="checkbox"/>	2	Off pps	Off pps	Off pps
<input type="checkbox"/>	3	Off pps	Off pps	Off pps
<input type="checkbox"/>	4	Off pps	Off pps	Off pps
<input type="checkbox"/>	5	Off pps	Off pps	Off pps
<input type="checkbox"/>	6	Off pps	Off pps	Off pps

Ok Reset

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 configuring, 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

Looped Port Unlock-interval Mins (1-1440)

Current Status Update

Select	Port	Enabled	Status	Unlock
<input type="checkbox"/>	All	<input type="checkbox"/>	--	<input type="button" value="Unlock"/>
<input type="checkbox"/>	1	<input type="checkbox"/>	Unlocked	<input type="button" value="Unlock"/>
<input type="checkbox"/>	2	<input type="checkbox"/>	Unlocked	<input type="button" value="Unlock"/>
<input type="checkbox"/>	3	<input type="checkbox"/>	Unlocked	<input type="button" value="Unlock"/>
<input type="checkbox"/>	4	<input type="checkbox"/>	Unlocked	<input type="button" value="Unlock"/>
<input type="checkbox"/>	5	<input type="checkbox"/>	Unlocked	<input type="button" value="Unlock"/>
<input type="checkbox"/>	6	<input type="checkbox"/>	Unlocked	<input type="button" value="Unlock"/>

Loop Detection Enable: Check to enable 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 un-blocks the looped port if it does not receive any loop-detection packet during the configured unlock-interval. The unlock-interval can be set from 1 to 1440 minutes. The default setting is 1440 minutes.

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

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 configuring, click on the **Ok** button to have the setup in effect.

Port: The number of each port.

Enabled: Click on the checkbox of the corresponding port No. to enable the Loop Detection function on the specific port(s).

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

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

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.

The screenshot shows the LLDP Setup configuration page. On the left is a navigation menu with the following items: Welcome: admin, System Setup, Port Management, VLAN Setup, MAC Address Management, QoS Setup, Multicast, Security Setup, LLDP (selected), LLDP Setup, LLDP Status, Maintenance, Management, and Logout. The main content area is titled 'LLDP » LLDP Setup' and contains the following sections:

- State:** A dropdown menu set to 'Enabled'.
- Receiver Hold-Time (TTL):** A text input field containing '120' with the unit 'Secs (1-3600)'.
- Sending LLDP Packet Interval:** A text input field containing '5' with the unit 'Secs (1-180)'.
- Sending LLDP Packets Per Discover:** A text input field containing '1' with the unit 'Packet (1-16)'.
- Selection of LLDP TLVs to Send:** A list of TLV types with checkboxes, all of which are checked:
 - Port Description
 - System Name
 - System Description
 - System Capabilities
 - Management Address
- LLDP Port Configuration:** A section with a 'Select All' checkbox and radio buttons for ports 1 through 6.
- Buttons:** 'Ok' and 'Reset' buttons at the bottom.

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.

The screenshot shows the LLDP Setup configuration page. It is organized into three main sections:

- Global Settings:**
 - State:** A dropdown menu set to "Enabled".
 - Receiver Hold-Time (TTL):** A text input field containing "120" with the unit "Secs (1-3600)".
 - Sending LLDP Packet Interval:** A text input field containing "5" with the unit "Secs (1-180)".
 - Sending LLDP Packets Per Discover:** A text input field containing "1" with the unit "Packet (1-16)".
- Selection of LLDP TLVs to Send:** A list of five items, each with a checked checkbox:
 - Port Description
 - System Name
 - System Description
 - System Capabilities
 - Management Address
- LLDP Port Configuration:**
 - A "Select All" checkbox.
 - Individual checkboxes for ports 1, 2, 3, 4, 5, and 6.

At the bottom of the form are two buttons: "Ok" and "Reset".

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.

Port	Chassis ID	Remote Port	System Name	Port Description	System Capabilities	Management1 Address	Management2 Address	Management3 Address	Management4 Address	Management5 Address
1										
2										
3										
4										
5										
6										

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 4 options within this folder will be displayed for your selection.

The screenshot shows the 'Maintenance' page with a sidebar menu on the left and a main content area on the right. The sidebar menu includes: Welcome: admin, System Setup, Port Management, VLAN Setup, MAC Address Management, QoS Setup, Multicast, Security Setup, LLDP, Maintenance (selected), CPU & Memory Statistics, Ping, Event Log, Transceiver Information, Management, and Logout. The main content area is titled 'Maintenance > CPU & Memory Statistics'. It features a 'Refresh Page Interval' of 10 seconds, with 'Start Auto Update', 'Stop Auto Update', and 'Update' buttons. Below this is a 'CPU Loading Threshold' of 300 (1/100). The 'CPU Statistics' section shows: CPU Usage (%) at 6.93, Load Averages - 1 min at 8.12, Load Averages - 5 min at 7.95, and Load Averages - 15 min at 7.95. The 'Memory Statistics (KByte)' section shows: Total Memory at 122352, Memory Use at 36696, Memory Free at 85656, Memory Buffers at 340, and Memory Cached at 20672. At the bottom of the statistics are 'Ok' and 'Reset' buttons.

- 1. CPU & Memory Statistics:** Manually or automatically update statistics of CPU & Memory and view them.
- 2. 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.
- 3. 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.
- 4. Transceiver Information:** View the current WAN transceiver information, e.g. speed, Vendor Name, Vendor S/N, etc. WAN transceiver state shows current DMI (Diagnostic monitoring interface) temperature, voltage, TX Bias, etc.

4.9.1 CPU & Memory Statistics

CPU & Memory Statistics is to manually or automatically update statistics of CPU and Memory. Select the option **CPU & Memory Statistics** from the **Maintenance** menu and then the following screen page appears.

Refresh Page Interval	<input type="text" value="10"/>	Secs (1-300)
<input type="button" value="Start Auto Update"/> <input type="button" value="Stop Auto Update"/> <input type="button" value="Update"/>		
CPU Loading Threshold	<input type="text" value="300"/>	1/100
CPU Statistics		
CPU Usage (%)	4.95	
Load Averages - 1 min	7.82	
Load Averages - 5 min	8.02	
Load Averages - 15 min	7.84	
Memory Statistics (KByte)		
Total Memory	57336	
Memory Use	25360	
Memory Free	31976	
Memory Buffers	1492	
Memory Cached	8824	
<input type="button" value="Ok"/> <input type="button" value="Reset"/>		

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

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

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

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

CPU Loading Threshold: Specify a value for the CPU loading threshold. Valid range: 1-300 (Unit: 1/100).

Every three seconds the system will capture the value of **Load Averages - 15 min** and use it to compare against the specified value of **CPU Loading Threshold** (850 as the default value). The

trap-sending behavior will correspond to this comparison result and follow the pattern described below:

- A one-off CPU Loading **alarm trap** will be sent once the captured value of Load Averages – 15 min is **higher** than the threshold, with no follow-up alarm traps if the next captured value **still stays above** the threshold.
(However, when the value falls lower than the threshold, a **normal** trap will then be sent.)
- A one-off CPU Loading **normal trap** will be sent once the captured value of Load Averages – 15 min is **lower** than the threshold, with no follow-up normal traps if the next captured value **still stays below** the threshold.
(However, when the value is above the threshold, an **alarm** trap will then be sent.)

CPU Usage (%): The percentage of current CPU usage of the system.

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 1/5/15 minute(s).*

Load Averages – 1 min: The average of both running and waiting threads for the past 1 minute.

Load Averages – 5 min: The average of both running and waiting threads for the past 5 minutes.

Load Averages – 15 min: The average of both running and waiting threads for the past 15 minutes.

Total Memory: It shows the entire memory in kilobytes.

Memory Use: The memory in kilobytes that is in use.

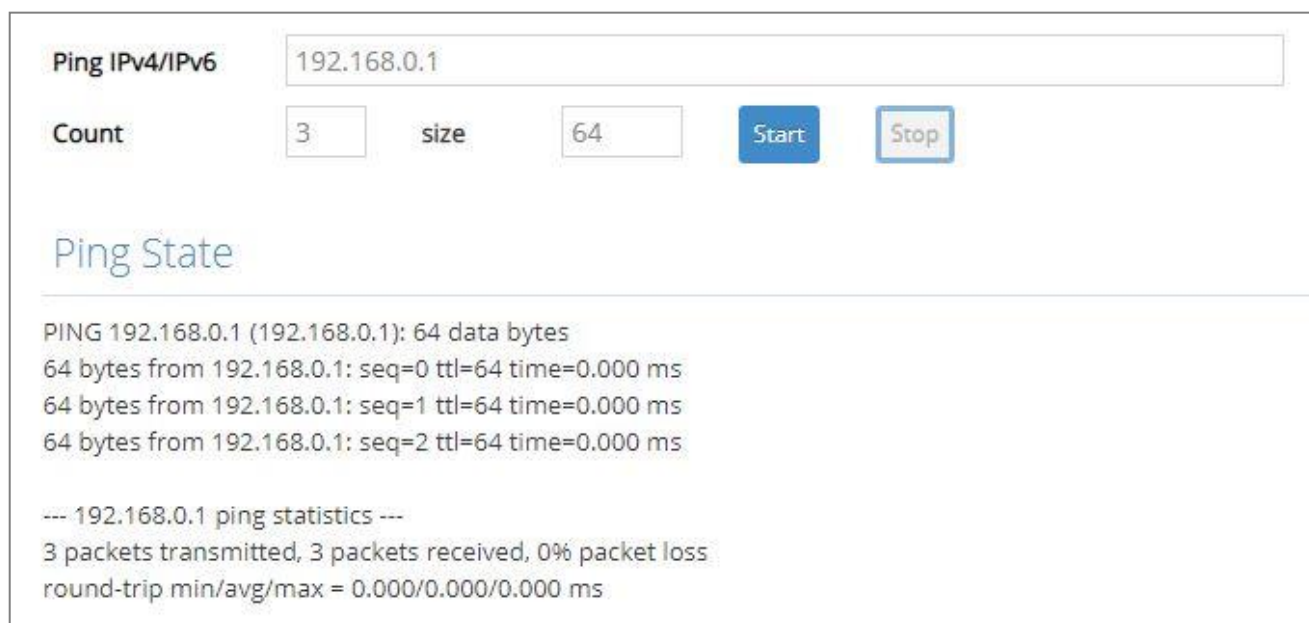
Memory Free: The memory in kilobytes that is idle.

Memory Buffers: The memory in kilobytes temporarily stored in a buffer area. Buffer allows the computer to be able to focus on other matters after it writes up the data in the buffer; as oppose to constantly focus on the data until the device is done.

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

4.9.2 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.



The screenshot shows a web interface for configuring and running a ping test. At the top, there is a form with the following fields and controls:

- Ping IPv4/IPv6:** A text input field containing the IP address `192.168.0.1`.
- Count:** A numeric input field containing the value `3`.
- size:** A text label followed by a numeric input field containing the value `64`.
- Start:** A blue button to initiate the ping test.
- Stop:** A light blue button to stop the ping test.

Below the form, the **Ping State** section displays the results of the test:

```
PING 192.168.0.1 (192.168.0.1): 64 data bytes
64 bytes from 192.168.0.1: seq=0 ttl=64 time=0.000 ms
64 bytes from 192.168.0.1: seq=1 ttl=64 time=0.000 ms
64 bytes from 192.168.0.1: seq=2 ttl=64 time=0.000 ms

--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms
```

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.

4.9.3 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.

The screenshot shows the 'Event Record' configuration page. It is divided into three sections: 'Event Record', 'Display Sequence', and 'Filter'.
1. **Event Record**: A dropdown menu is set to 'Disabled', and there is an 'Ok' button.
2. **Display Sequence**: A dropdown menu is set to 'Newest to oldest'. Below it, 'Start from index' is 500 and 'with' is 500 entries per page. Navigation buttons include 'First', 'Previous', 'Page 1', 'Next', and 'Last'.
3. **Filter**: 'Time Policy' is 'All Time', 'Time Range' is 'Up Time', and 'Item Policy' is 'Display All'. There is a 'Select' button for 'Item List', 'Item Selected' is 'None', and 'Search' and 'Clear All' buttons.

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.

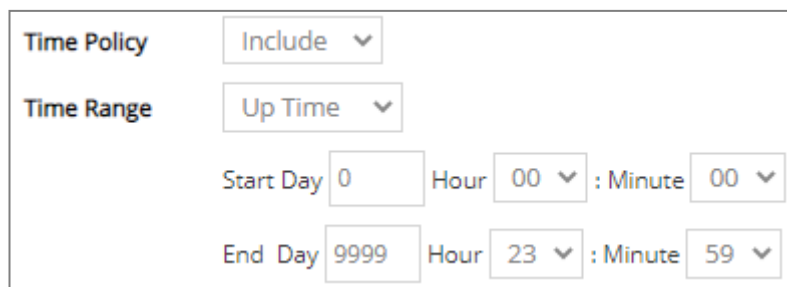
1. Select **Newest to oldest** or **Oldest to newest** to specify the arrangement of the event log display.
2. Set **Start from index** as a particular event index. Any event of which the index is smaller than the specified index will not be displayed if you specify the arrangement of **Oldest to newest**;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

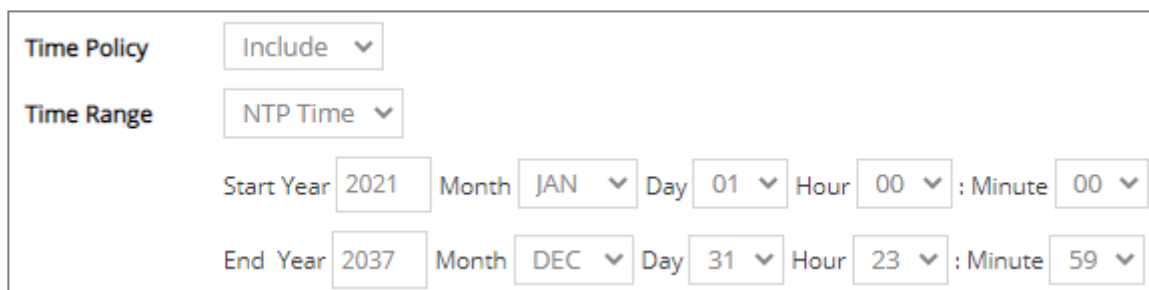
Filter: Configure each filter setting to customize the display of the event log table.

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.



The screenshot shows a filter configuration box. The 'Time Policy' dropdown is set to 'Include'. The 'Time Range' dropdown is set to 'Up Time'. Below these, there are two rows of time selection controls. The first row is for the 'Start' time, with 'Start Day' set to '0', 'Hour' set to '00', and 'Minute' set to '00'. The second row is for the 'End' time, with 'End Day' set to '9999', 'Hour' set to '23', and 'Minute' set to '59'.

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.



The screenshot shows a filter configuration box. The 'Time Policy' dropdown is set to 'Include'. The 'Time Range' dropdown is set to 'NTP Time'. Below these, there are two rows of time selection controls. The first row is for the 'Start' time, with 'Start Year' set to '2021', 'Month' set to 'JAN', 'Day' set to '01', 'Hour' set to '00', and 'Minute' set to '00'. The second row is for the 'End' time, with 'End Year' set to '2037', 'Month' set to 'DEC', 'Day' set to '31', 'Hour' set to '23', and 'Minute' set to '59'.

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.

Item List Select

Display Log Item List Select All Quick Select (e.g.: 1,2,3-6) Select

<input type="checkbox"/> 1. Information	<input type="checkbox"/> 2. Warning	<input type="checkbox"/> 3. Error
<input type="checkbox"/> 4. CLI disconnected	<input type="checkbox"/> 5. Code start	<input type="checkbox"/> 6. CPU over loading
<input type="checkbox"/> 7. DHCP snooping	<input type="checkbox"/> 8. Link down	<input type="checkbox"/> 9. Link up
<input type="checkbox"/> 10. Login	<input type="checkbox"/> 11. Login failed	<input type="checkbox"/> 12. Logout
<input type="checkbox"/> 13. Loop detection	<input type="checkbox"/> 14. SFP RX power OK	<input type="checkbox"/> 15. SFP RX power overheat
<input type="checkbox"/> 16. SFP RX power too low	<input type="checkbox"/> 17. SFP temperature ok	<input type="checkbox"/> 18. SFP temperature overheat
<input type="checkbox"/> 19. SFP temperature too low	<input type="checkbox"/> 20. SFP TX power ok	<input type="checkbox"/> 21. SFP TX power overheat
<input type="checkbox"/> 22. SFP TX power too low	<input type="checkbox"/> 23. SFP voltage ok	<input type="checkbox"/> 24. SFP voltage overheat
<input type="checkbox"/> 25. SFP voltage too low	<input type="checkbox"/> 26. System voltage warning	<input type="checkbox"/> 27. Update failed
<input type="checkbox"/> 28. Warn start		

Ok

Item Selected: None

Search Clear All

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.

4.9.4 Transceiver Information

Select the option **Transceiver Information** from the **Maintenance** menu and then three functions, including **Transceiver Info**, **Transceiver State**, and **Transceiver Threshold Configuration** within this subfolder will be displayed.

Welcome: admin

Maintenance » Transceiver Information > Transceiver Info

Refresh

Port	Speed	Distance	Vendor Name	Vendor PN	Vendor SN
6	100/1000Mbps	10 km	CTS-INC	CTS-W2A-10KM-DR	N/A

System Setup

Port Management

VLAN Setup

MAC Address Management

QoS Setup

Multicast

Security Setup

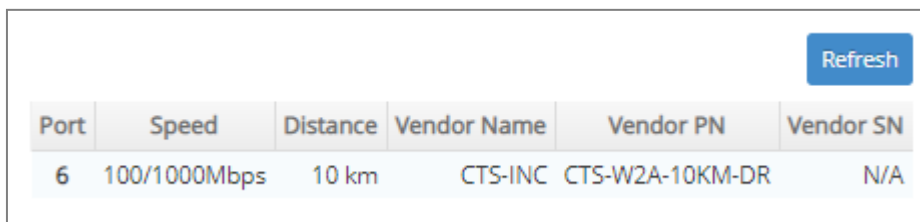
LLDP

Maintenance

- ... CPU & Memory Statistics
- ... Ping
- ... Event Log
- ▶ Transceiver Information
 - ▶ Transceiver Info
 - ▶ Transceiver State
 - ▶ Transceiver Threshold Configuration

4.9.4.1 Transceiver Info

Transceiver Info displays WAN 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 **Transceiver Info** function.



Port	Speed	Distance	Vendor Name	Vendor PN	Vendor SN
6	100/1000Mbps	10 km	CTS-INC	CTS-W2A-10KM-DR	N/A

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.

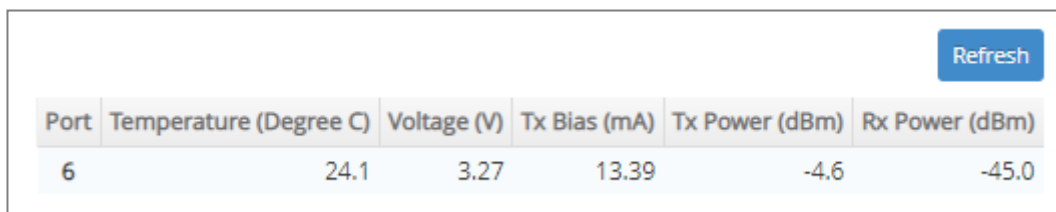
Vendor Name: Vendor name of the transceiver.

Vendor PN: Vendor PN of the transceiver.

Vendor SN: Vendor SN of the transceiver.

4.9.4.2 Transceiver State

Transceiver State displays WAN transceiver information e.g. the currently detected temperature, voltage, TX Bias, etc. The following screen page appears if you choose **Transceiver State** function.



The screenshot shows a user interface for 'Transceiver State'. It features a table with six columns: Port, Temperature (Degree C), Voltage (V), Tx Bias (mA), Tx Power (dBm), and Rx Power (dBm). The table contains one row of data for Port 6. A blue 'Refresh' button is located in the top right corner of the interface.

Port	Temperature (Degree C)	Voltage (V)	Tx Bias (mA)	Tx Power (dBm)	Rx Power (dBm)
6	24.1	3.27	13.39	-4.6	-45.0

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 Transceiver Threshold Configuration

Transceiver Threshold Configuration function not only displays the WAN transceiver current temperature, voltage, current, TX power and RX power information but is capable of detecting whether the WAN transceiver is at normal status or not.

In the display of the above WAN traceiver 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 requiriements.

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 WAN 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 WAN 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 **Transceiver Threshold Configuration** function.

Select	Port	Auto Detect	Temperature Threshold (-40.0 - 120.0 °C)						Voltage Threshold (2.60 - 4.00 V)							
			Current	High			Low			Current	High			Low		
				Enable	Alarm	warning	Enable	Alarm	warning		Enable	Alarm	warning	Enable	Alarm	warning
<input type="checkbox"/>	All	<input type="checkbox"/>	--	<input type="checkbox"/>	0.0	0.0	<input type="checkbox"/>	0.0	0.0	--	<input type="checkbox"/>	0.00	0.00	<input type="checkbox"/>	0.00	0.00
<input type="checkbox"/>	6	<input checked="" type="checkbox"/>	24.1	<input type="checkbox"/>	100.0	95.0	<input type="checkbox"/>	-50.0	-45.0	3.27	<input type="checkbox"/>	3.70	3.65	<input type="checkbox"/>	2.90	2.95

Transceiver Threshold Enable: Globally enable or disable the alarm notification of temperature/current/ voltage/TX power/RX power for the WAN transceiver of the Managed Switch.

Threshold Interval for Notification: Specify the time interval of sending WAN transceiver 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 WAN transceiver 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 WAN transceiver 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 WAN transceiver 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 the WAN transceiver 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: 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 configuring, click on the **Ok** button to have the setup in effect.

Port: The port number of the WAN transceiver.

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 WAN transceiver supports and follows the full SFF-8472. The 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 the WAN transceiver doesn't support the full SFF-8472 or customer doesn't trust the threshold value from the WAN transceiver (SFF-8472).

Current status of Temperature/Voltage/Current/TX power/RX power Threshold parameter: Display the WAN transceiver 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 WAN transceiver alarm/warning notification of temperature /voltage/current/TX power/RX power.

High/Low Value of Temperature Threshold Alarm/Warning parameter: Specify the WAN transceiver 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 the WAN transceiver 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 the WAN transceiver 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 the WAN transceiver 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 the WAN transceiver 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 Management

In order to do the firmware upgrade, load the factory default settings, etc. for the Managed Switch, please click the folder **Management** from the **Main Menu** and then 8 options will be displayed for your selection.

The screenshot shows the 'Management' configuration page. The left sidebar contains a menu with the following items: System Setup, Port Management, VLAN Setup, MAC Address Management, QoS Setup, Multicast, Security Setup, LLDP, Maintenance, Management (selected), Management Access Setup (expanded), User Authentication, SNMP, LED Control Setup, Firmware Upgrade, Load Factory Settings, Save Configuration, and Reset System. The main content area is titled 'Management » Management Access Setup' and contains the following settings:

Telnet Service	Enabled	▼
SSH Service	Disabled	▼
SNMP Service	Enabled	▼
Web Service	Enabled	▼
Telnet Port	23	(1-65535)
Telnet Time Out	300	(1-1440) Unit Seconds ▼
Web Time Out	20	Mins (1-1440)

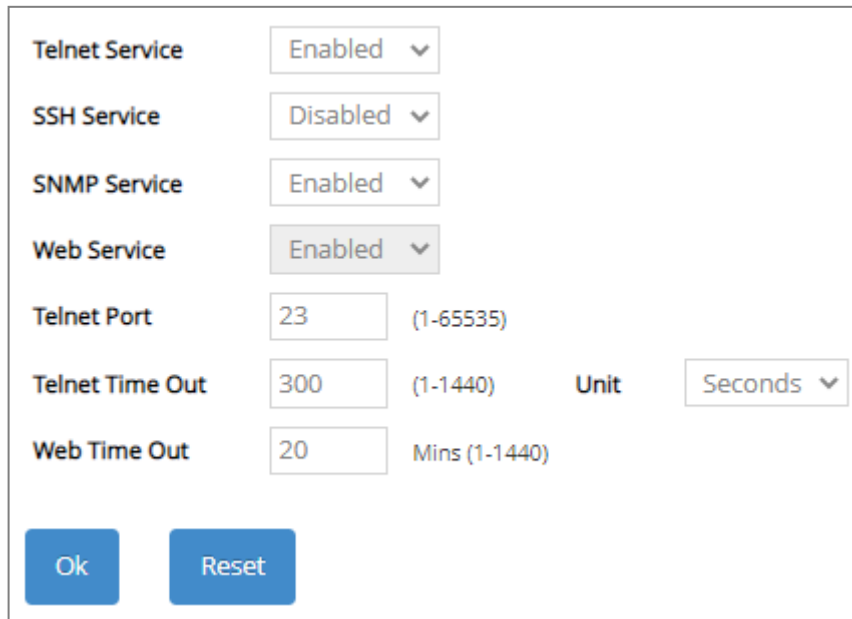
At the bottom of the configuration area are two buttons: 'Ok' and 'Reset'.

- 1. Management Access Setup:** Enable or disable the specified network services
- 2. User Authentication:** View the registered user list, add a new user or remove an existing user and set up RADIUS authentication.
- 3. 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.
- 4. LED Control Setup:** Toggle between the on and off state of the LED status light.
- 5. Firmware Upgrade:** This allows users to update the latest firmware, save current configuration or restore previous configuration to the Managed Switch.
- 6. Load Factory Settings:** Load Factory Setting will reset the configuration including or excluding the IP and Gateway addresses of the Managed Switch back to the factory default settings.

7. **Save Configuration:** Save all changes to the system.
8. **Reset System:** Reset the Managed Switch.

4.10.1 Management Access Setup

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



Telnet Service	Enabled	▼
SSH Service	Disabled	▼
SNMP Service	Enabled	▼
Web Service	Enabled	▼
Telnet Port	23	(1-65535)
Telnet Time Out	300	(1-1440)
Web Time Out	20	Mins (1-1440)

Unit: Seconds ▼

Ok Reset

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. It is a view-only field.

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

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

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

4.10.2 User Authentication

To prevent any unauthorized operations, only registered users are allowed to operate the Managed Switch. Users who would like to operate the Managed Switch need to create a user account first.

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

Account State	Privilege Level	User Name	Description	Action
Enabled	Administrator	admin		

Password Encryption: Pull down the menu of **Password Encryption** to select one method to secure the password against potential malicious attacks.

Disabled: Disable the password encryption function. Select **Disabled** 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.

To configure RADIUS authentication, click the **RADIUS Configuration** button. The following screen page will show up.

Authentication

Authentication: Select RADIUS to enable the RADIUS server authentication method against which a user accessing the Managed Switch can be authenticated. Or, select **Disabled** to use no authentication at all.

Authentication: RADIUS

RADIUS

Note!!

1. If Password Encryption is already specified as AES-128, any later changes on the function setting will result in each configured secret key being set to empty.
2. Once the secret key is set to empty, if applicable, you will have to manually reset each one to its original secret key.

Secret Key Encryption: Disabled

RADIUS Secret Key: default

RADIUS Port: 1812 (1025-65535)

RADIUS Retry Times: 0

1st RADIUS Server IPv4/IPv6 Address: 0.0.0.0

2nd RADIUS Server IPv4/IPv6 Address: 0.0.0.0

Ok Reset

Secret Key Encryption: Pull down the menu of **Secret Key Encryption** to select one method to secure the secret key against potential malicious attacks.

Disabled: Disable the secret key encryption function. Select **Disabled** 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.

RADIUS 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.

RADIUS Port: The RADIUS service port on the RADIUS server. Valid values are 1025 through 65535.

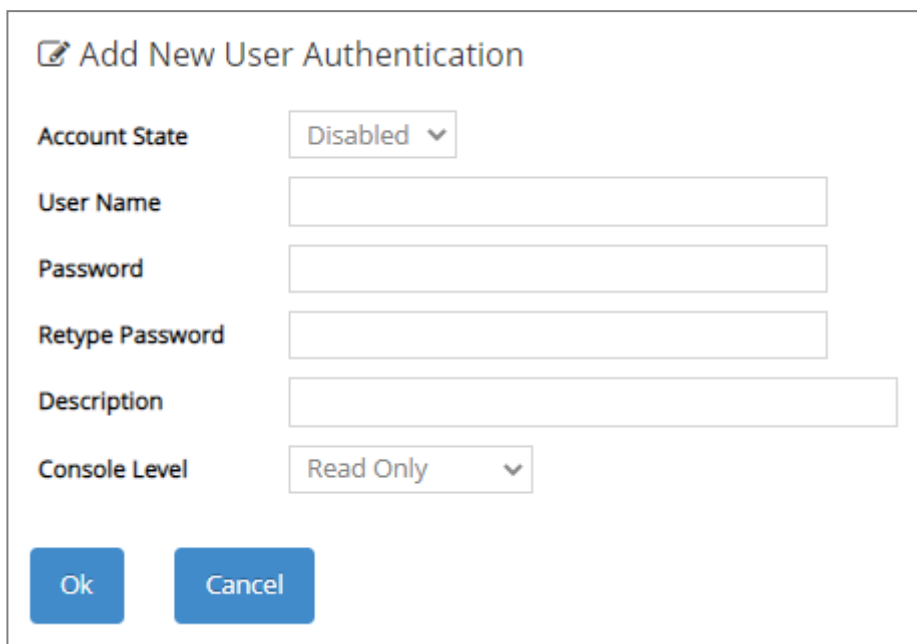
RADIUS Retry Times: The maximum number of attempts to reconnect if the RADIUS server is not reachable. Valid values are 0 through 3.

1st RADIUS Server IPv4/IPv6 IP: The 1st IPv4/IPv6 address of the RADIUS server. Up to 2 servers can be configured as the RADIUS authentication server.

2nd RADIUS Server IPv4/IPv6 IP: The 2nd IPv4/IPv6 address of the RADIUS server. Up to 2 servers can be configured as the RADIUS authentication server.

NOTE: For FreeRADIUS server setup, please refer to [APPENDIX A](#) for the creation of CTS vendor-specific dictionary and modification of the configuration files.

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



Account State: Enable or disable this user account.

User Name: Specify the authorized user login name. Up to 20 alphanumeric characters can be accepted.

Password: Enter the desired user password. Up to 20 alphanumeric characters can be accepted.

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

Description: Enter a unique description for this user. Up to 35 alphanumeric characters can be accepted. This is mainly used for reference only.


Console Level: Select the desired privilege level for the management operation from the pull-down menu. Three operation levels of privilege are available in Managed Switch:

Administrator: Own the full-access right. The user can maintain user account as well as system information, load the factory default settings, and so on.

Read & Write: Own the partial-access right. The user is unable to modify user account and system information, do the firmware upgrade, load the factory default settings, and set up auto-backup.

Read Only: Allow to view only.

Click the  icon to modify the settings of a registered user you specify.

Click the  icon to remove the selected registered user account from the user list. Or click **Batch Delete** to remove a number of /all user accounts at a time by clicking on the checkbox belonging to the corresponding user in the **Action** field and then click **Delete Select Item**, the selected user(s) will be deleted immediately. To cancel this batch delete, please click **Cancel Batch Delete** to cancel the selection.

NOTE:

1. To prevent incautious operations, users cannot delete their own account, modify their own user name and change their own account state.
 2. The acquired password from backup config file is not applicable for user login on CLI/Web interface.
 3. We strongly recommend not to alter off-line Auth Method setting in backup configure file.
 4. If Auth-Method is enabled and do firmware downgrade, users must reset default config.
-

4.10.3 SNMP

Select the option **SNMP** from the **Management** menu and then four functions, including SNMPv3 USM User, Device Community, Trap Destination and Trap Setup will be displayed for your selection.

4.10.3.1 SNMPv3 USM User

Simple Network Management Protocol Version 3, SNMPv3 in short, features stronger security mechanism, including authentication and encryption that helps ensure that the message is from a valid source and scramble the content of a packet, to prevent from being learned by an unauthorized source. The following screen page appears if you choose **SNMPv3 USM User** function.

Account State	SNMP Level	User Name	Authentication	Private	Action
Enabled	Administrator	admin	None	None	

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.

Edit SNMPv3 USM User

Account State: Enable

User Name: admin

Authentication: None

Private: None

SNMP Level: Administrator

Ok Cancel

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

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

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

None: Disable authentication function. Select “None” from the pull-down menu to disable it.

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

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

Authentication-Password: Specify the passwords if “MD5” or “SHA” is chosen. Up to 20 characters can be accepted.

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

None: Disable Private function. Select “None” from the pull-down menu to disable it.

DES (Data Encryption Standard): An algorithm to encrypt critical information such as message text message signatures, etc. Select “DES” from the pull-down menu to enable it.

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.

4.10.3.2 Device Community

The following screen page appears if you choose **Device Community** function.



Account State	SNMP Level	Community	Description	Action
Enabled	Read and Write	public	Default_Account	 
Enabled	Administrator	admin	Default_Account	 

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	SNMP Level	Community	Description	Action
Disabled ▾	Read Only ▾			 
Enabled	Read and Write	public	Default_Account	 
Enabled	Administrator	admin	Default_Account	 



Account State: Enable or disable this Community Account.


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


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

Community: Specify the authorized SNMP community name, up to 20 alphanumeric characters.

Description: Enter a unique description for this community name. Up to 35 alphanumeric characters can be accepted. This is mainly for reference only.

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

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

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

4.10.3.3 Trap Destination

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

Index	State	Destination IP	Community
1	Disabled ▾	0.0.0.0	
2	Disabled ▾	0.0.0.0	
3	Disabled ▾	0.0.0.0	

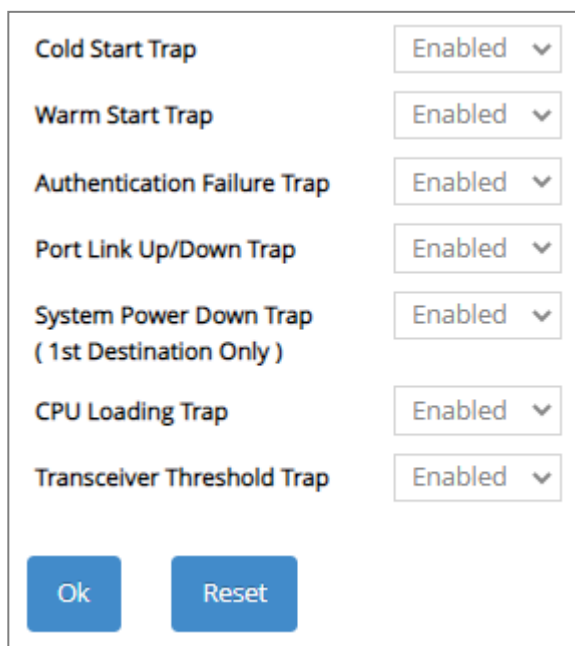
State: Enable or disable the function of sending trap to the specified destination.

Destination IP: Enter the specific IPv4/IPv6 address of the network management system that will receive the trap.

Community: Enter the description for the specified trap destination.

4.10.3.4 Trap Setup

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



Cold Start Trap	Enabled ▾
Warm Start Trap	Enabled ▾
Authentication Failure Trap	Enabled ▾
Port Link Up/Down Trap	Enabled ▾
System Power Down Trap (1st Destination Only)	Enabled ▾
CPU Loading Trap	Enabled ▾
Transceiver Threshold Trap	Enabled ▾

Ok Reset

Cold Start Trap: Enable or disable the Managed Switch to send a trap when the Managed Switch is turned on.

Warm Start Trap: Enable or disable the Managed Switch to send a trap when the Managed Switch restarts.

Authentication Failure Trap: Enable or disable the Managed Switch to send authentication failure trap after any unauthorized users attempt to login.

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

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

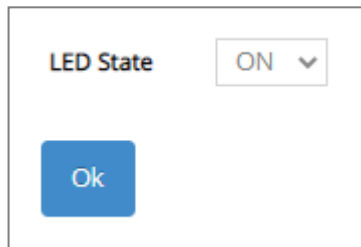
CPU Loading Trap: Enable or disable the Managed Switch to send a trap when the CPU is overloaded.

Transceiver Threshold Trap: Enable or disable Managed Switch to send a trap when Temperature/ Voltage/Current/TX Power/RX Power of any WAN transceiver is over the **High** value, under the **Low** value, or returning to the normal status from abnormal status.

4.10.4 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.

4.10.5 Firmware upgrade

The Managed Switch offers three methods, including HTTP, FTP and TFTP to back up/restore the configuration and update the firmware. To do this, please select the option **Firmware Upgrade** from the **Management** menu and then the following screen page appears.

Protocol: HTTP (dropdown menu open showing TFTP, FTP, HTTP)

File Type: Configuration (dropdown menu)

Config Type: Running-config (dropdown menu)

Select File: Choose File No file chosen

Update Backup

Transmitting State

4.10.5.1 Configuration Backup/Restore via HTTP

To back up or restore the configuration via HTTP, just pull down the **Protocol** menu and select **HTTP**. Also configure the type of file as “**Configuration**” to process. The related parameter description is as below.

Protocol: HTTP (dropdown menu)

File Type: Configuration (dropdown menu)

Config Type: Running-config (dropdown menu)

Select File: Choose File No file chosen

Update Backup

Transmitting State

Config Type: There are three types of the configuration file: Running-config, Default-config and Start-up-config.

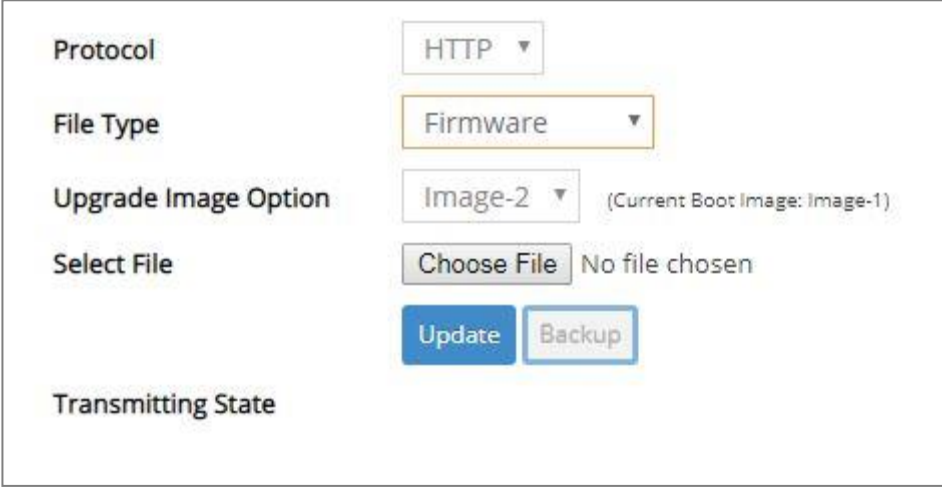
- **Running-config:** Back up the data you're processing.
- **Default-config:** Back up the data same as the factory default settings.
- **Start-up-config:** Back up the data same as last saved data.

Backup: Click **Backup** to begin download the configuration file to your PC.

Select File: Click **Choose File** to select the designated data and then click **Update** to restore the configuration.

4.10.5.2 Firmware Upgrade via HTTP

To update the firmware via HTTP, just pull down the **Protocol** menu and select **HTTP**. Also configure the type of file as “**Firmware**” to process. The related parameter description is as below.



The screenshot shows a web interface for firmware upgrade. It contains the following elements:

- Protocol:** A dropdown menu with "HTTP" selected.
- File Type:** A dropdown menu with "Firmware" selected.
- Upgrade Image Option:** A dropdown menu with "Image-2" selected. To its right, it says "(Current Boot Image: Image-1)".
- Select File:** A "Choose File" button followed by the text "No file chosen".
- Buttons:** Two buttons, "Update" (blue) and "Backup" (light blue), are positioned below the "Select File" section.
- Transmitting State:** A label at the bottom left of the form area.

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

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

4.10.5.3 Configuration Backup/Restore via FTP/TFTP

The Managed Switch has both built-in TFTP and FTP clients. Users may back up or restore the configuration via FTP/TFTP. Just pull down the **Protocol** menu and select **FTP** or **TFTP**, also configure the type of file as “**Configuration**” to process. The related parameter description is as below.

The screenshot shows a web-based configuration interface for backup/restore operations. It features several dropdown menus and text input fields. The 'Protocol' dropdown is set to 'FTP', 'File Type' is 'Configuration', and 'Config Type' is 'Running-config'. Below these are four text input fields: 'Server IPv4/IPv6 Address', 'User Name', 'Password', and 'File Location'. At the bottom of the form are two blue buttons labeled 'Update' and 'Backup'. Below the buttons is a label 'Transmitting State'.

Protocol: Select the preferred protocol, either FTP or TFTP.

Config Type: Choose the type of the configuration file that will be saved or restored among “Running-config”, “Default-config” or “Start-up-config”.

Server IPv4/IPv6 Address: Enter the specific IPv4/IPv6 address of the FTP/TFTP file server.

User Name (for FTP only): Enter the specific username to access the FTP file server.

Password (for FTP only): Enter the specific password to access the FTP file server.

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

Click **Backup** to start the download process and receive files from the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind the user.

Click **Update** to start the upload process and transmit files to the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind users.

4.10.5.4 Firmware Upgrade via FTP/TFTP

The Managed Switch has both built-in TFTP and FTP clients. Users may update the firmware via FTP/TFTP. Just pull down the **Protocol** menu and select **FTP** or **TFTP**, also configure the type of file as **“Firmware”** to process. The related parameter description is as below.

The screenshot shows a web-based configuration interface for firmware upgrade. It contains the following elements:

- Protocol:** A dropdown menu with 'FTP' selected.
- File Type:** A dropdown menu with 'Firmware' selected.
- Upgrade Image Option:** A dropdown menu with 'Image-2' selected. To its right, it says '(Current Boot Image: Image-1)'. Below this is a long text input field.
- Server IPv4/IPv6 Address:** A text input field.
- User Name:** A text input field.
- Password:** A text input field.
- File Location:** A long text input field.
- Buttons:** Two buttons labeled 'Update' and 'Backup'.
- Transmitting State:** A label at the bottom left of the form area.

Protocol: Select the preferred protocol, either FTP or TFTP.

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

Server IPv4/IPv6 Address: Enter the specific IPv4/IPv6 address of the FTP/TFTP file server.

User Name (for FTP only): Enter the specific username to access the FTP file server.

Password (for FTP only): Enter the specific password to access the FTP file server.

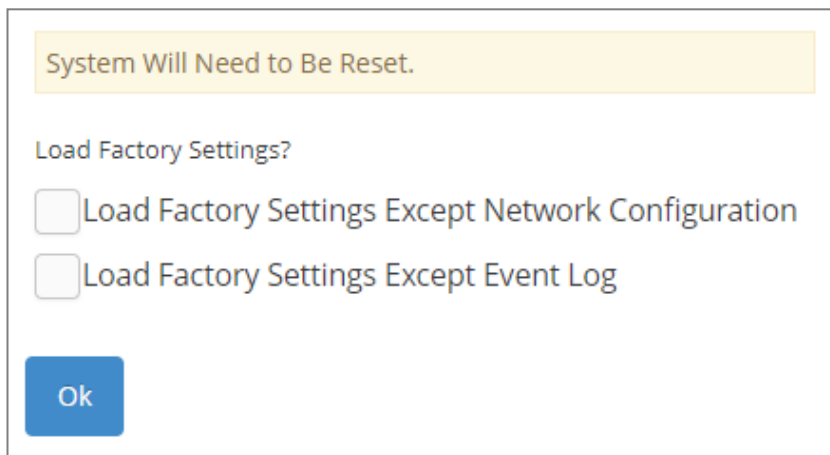
File Location: Enter the specific path and filename within the FTP/TFTP file server.

Click **Update** to start the upload process and transmit files to the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind users.

4.10.6 Load Factory Settings

Load Factory Settings will set all the configurations of the Managed Switch back to the factory default settings, including the IP and Gateway address. **Load Factory Setting** is useful when network administrators would like to re-configure the system. A system reset is required to make all changes effective after Load Factory Setting.

Select the option **Load Factory Settings** from the **Management** menu and then the following screen page appears.



The screenshot shows a dialog box with a yellow header bar containing the text "System Will Need to Be Reset." Below the header, the text "Load Factory Settings?" is displayed. There are two radio button options: "Load Factory Settings Except Network Configuration" and "Load Factory Settings Except Event Log". At the bottom left of the dialog box is a blue button labeled "Ok".

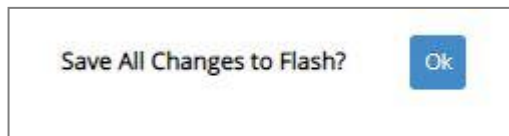
Load Factory Settings Except Network Configuration: It will set all the configurations of the Managed Switch back to the factory default settings. However, IP and Gateway addresses will not restore to the factory default. It is very useful when network administrators need to re-configure the system "REMOTELY"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

4.10.7 Save Configuration

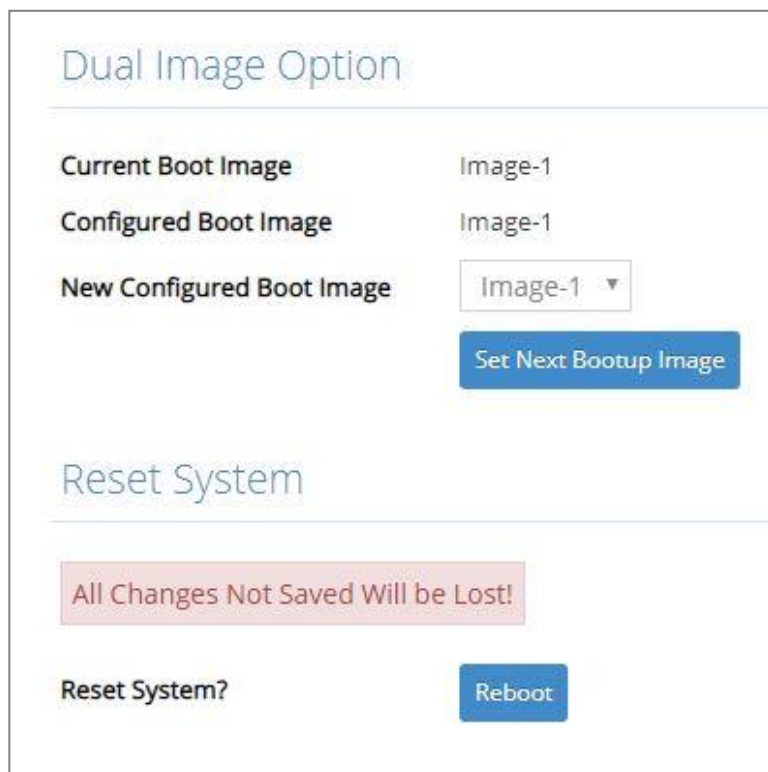
In order to save the configuration permanently, users need to save configuration first before resetting the Managed Switch. Select the option **Save Configuration** from the **Management** menu and then the following screen page appears.



Click **OK** to save the configuration. Alternatively, you can also press the **Save** quick button located on the top-right side of the webpage, which has the same function as Save Configuration.

4.10.8 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.



The screenshot shows a web interface with two main sections. The top section, titled "Dual Image Option", contains three rows of configuration fields. The first row shows "Current Boot Image" set to "Image-1". The second row shows "Configured Boot Image" set to "Image-1". The third row shows "New Configured Boot Image" with a dropdown menu currently displaying "Image-1". Below these fields is a blue button labeled "Set Next Bootup Image". The bottom section, titled "Reset System", features a pink warning box that reads "All Changes Not Saved Will be Lost!". Below the warning is a "Reset System?" label and a blue "Reboot" button.

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

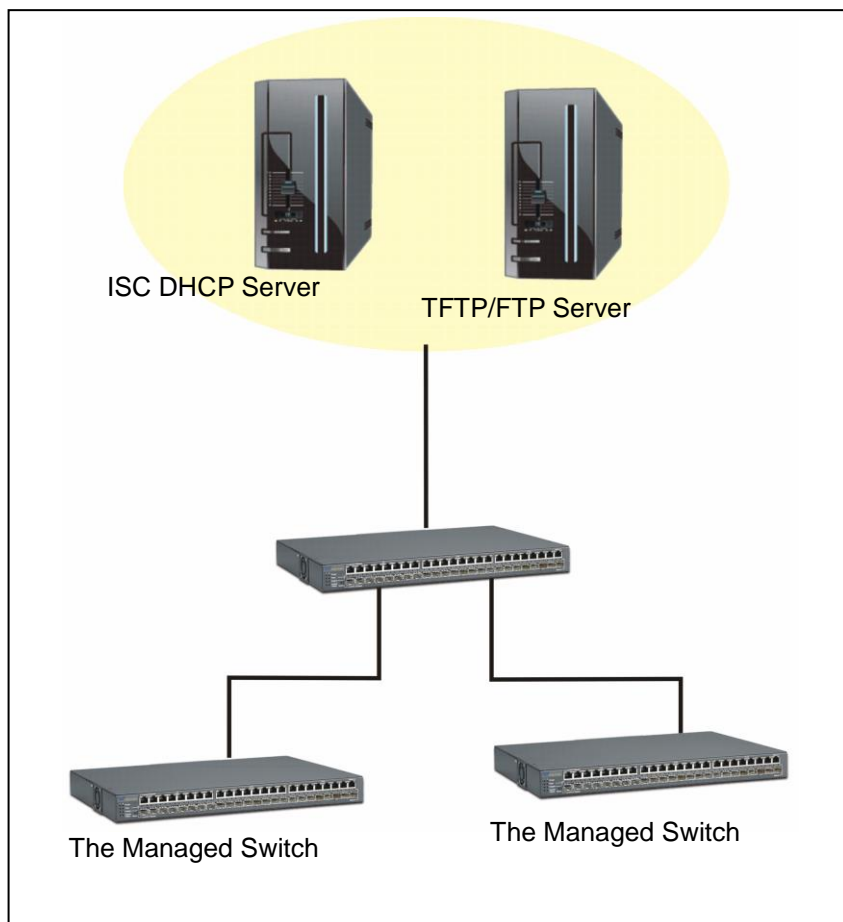
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the Managed Switch that you purchased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

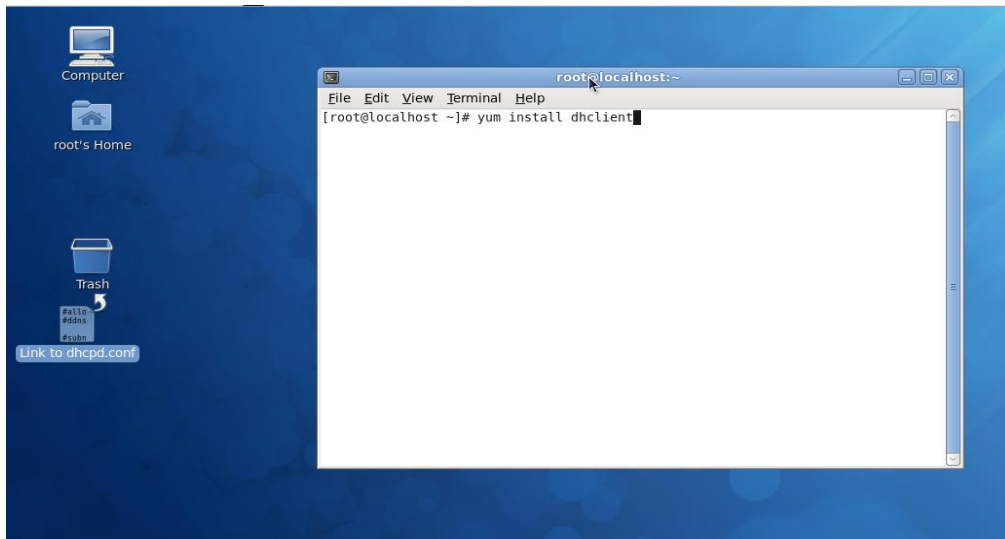
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Topology Example

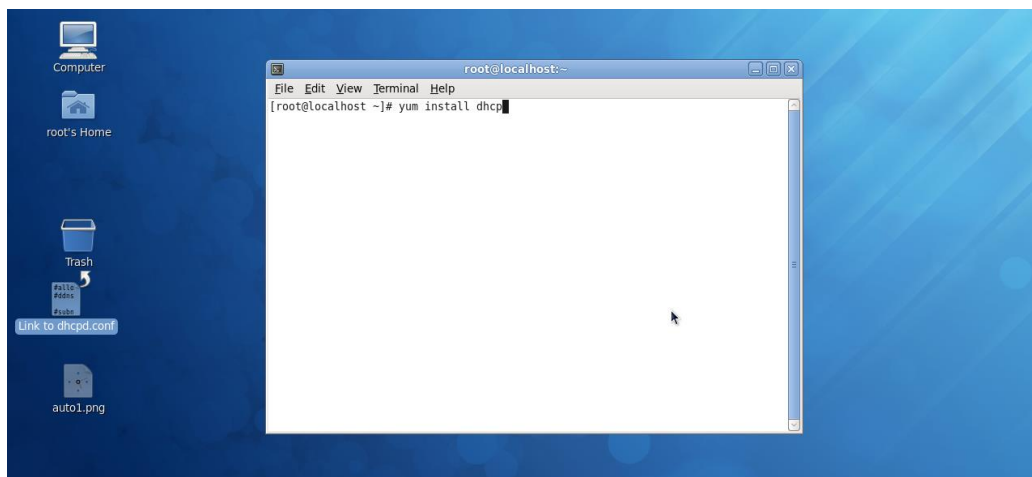
Step 2. Set up Auto Provision Server

● Update DHCP Client



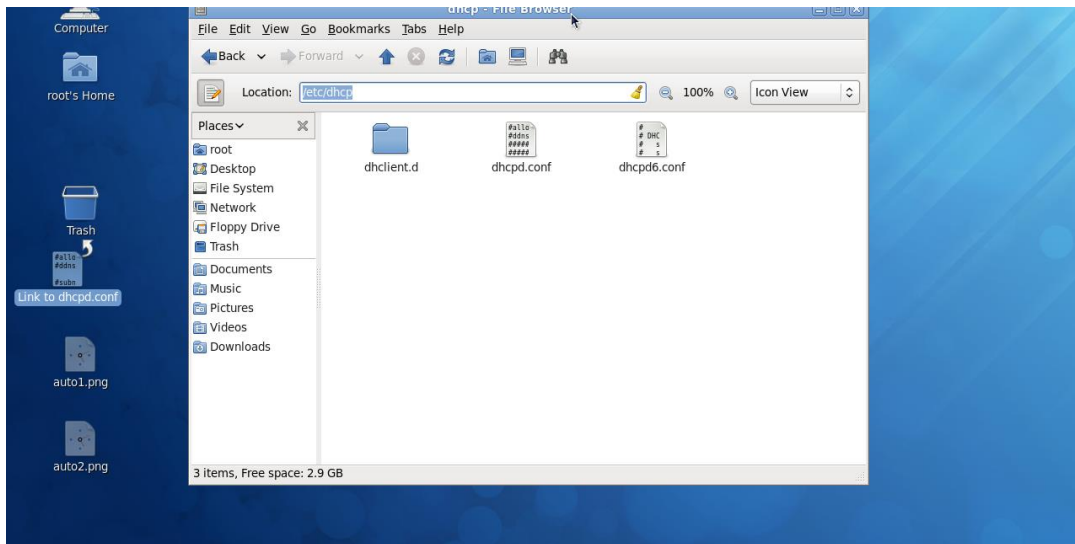
Linux Fedora 12 supports “yum” function by default. First of all, update DHCP client function by issuing “yum install dhclient” command.

● Install DHCP Server



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

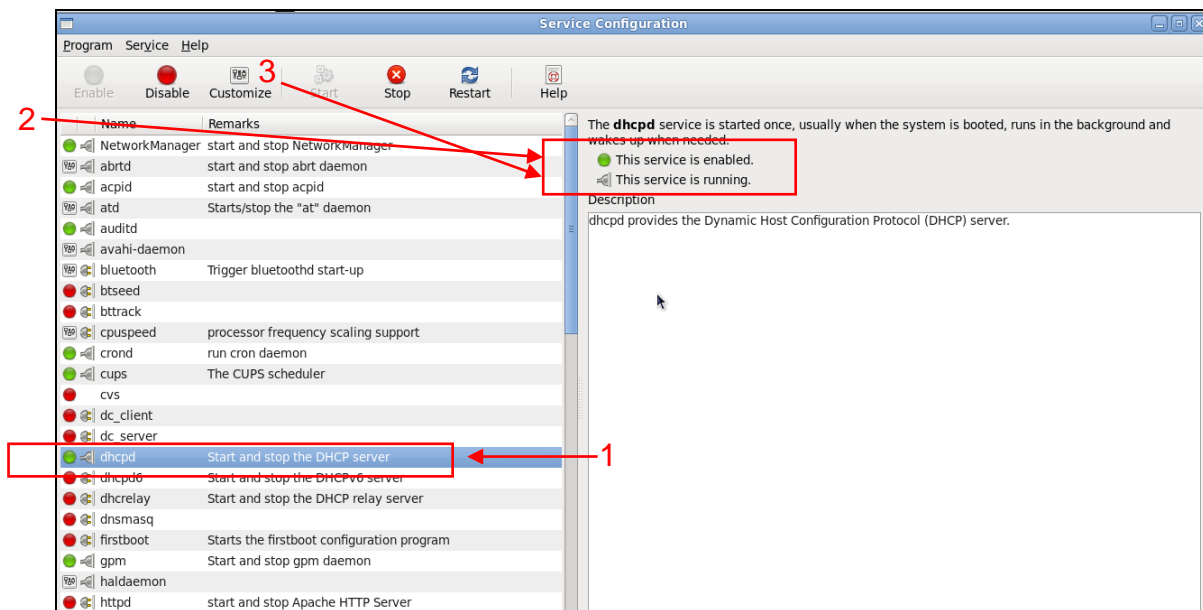
● Copy dhcpd.conf to /etc/dhcp/ directory



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

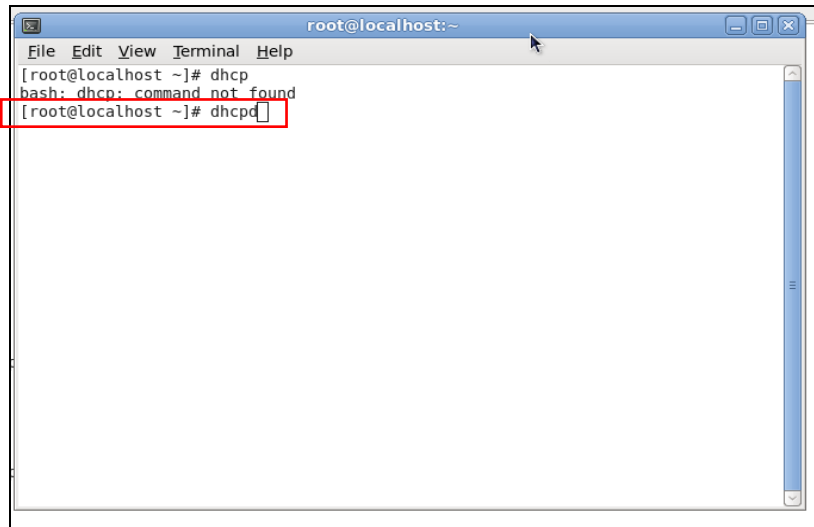
Please note that each vendor has their own way to define auto provisioning. Make sure to use the file provided by the vendor.

● Enable and run DHCP service



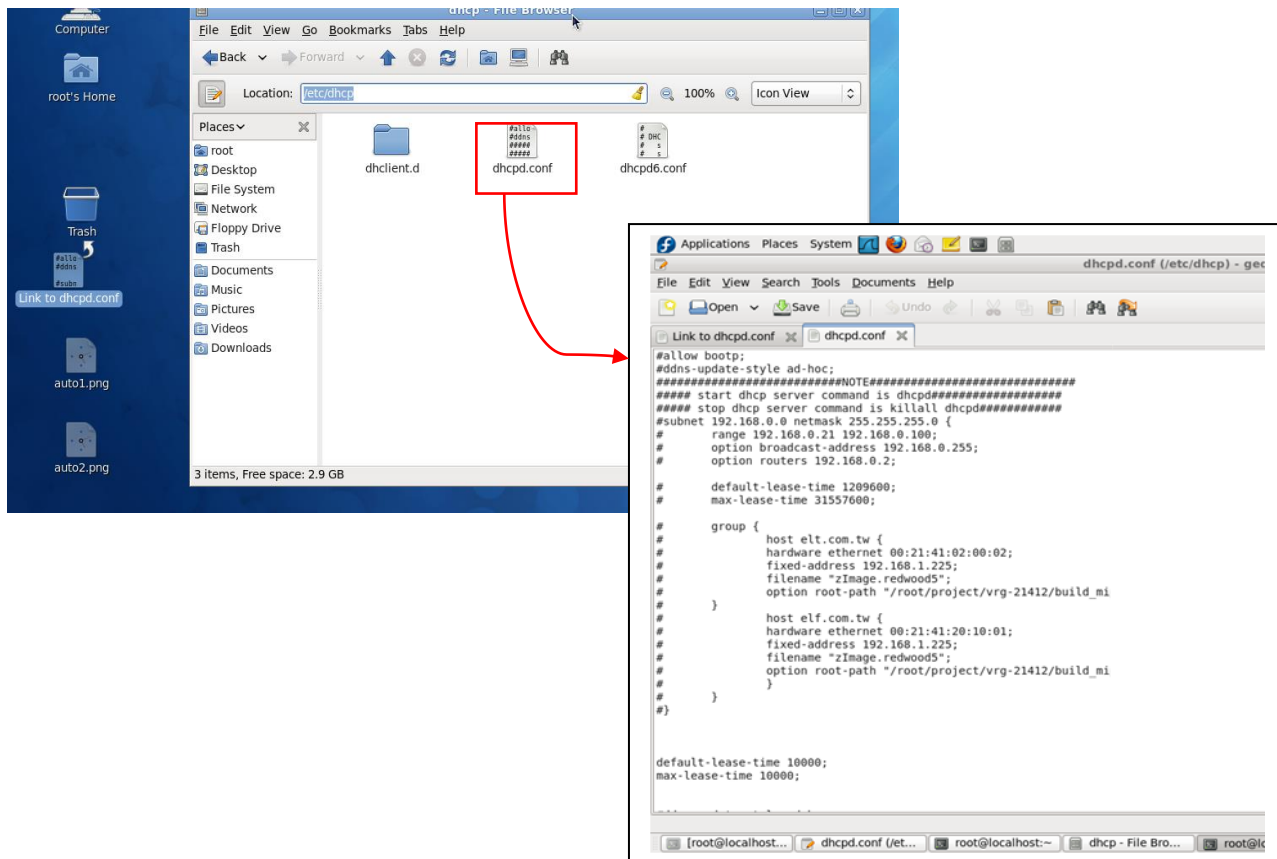
1. Choose dhcpd.
2. Enable DHCP service.
3. Start running DHCP service.

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.

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

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

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

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

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

}
```

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

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

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

2. Define subnet, subnet mask, IP range, broadcast address, router address and DNS server address.
3. Map a host's MAC address to a fixed IP address.
4. Map a host's MAC address to a fixed IP address. Use the same format to create multiple MAC-to-IP address bindings.

```

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

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

option SWITCH.protocol 1;
option SWITCH.server-ip [192.168.0.251];
# option SWITCH.server-login-name "anonymous";
option SWITCH.server-login-name "FAE";
option SWITCH.server-login-password "depl";

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

```

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

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

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

```

root@localhost:~# md5sum HS-0600-provision_2.bin
162c2e4d30e5715cccf85a10d83378db:HS-0600-provision_2.bin
root@localhost ~#

```

● Restart DHCP service

```

root@localhost:~# dhcpd
Internet Systems Consortium DHCP Server 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
WARNING: Host declarations are global. They are not limited to the scope you
clared them in.
Not searching LDAP since ldap-server, ldap-port and ldap-base-dn were not sp
ied in the config file
Wrote 0 class decls to leases file.
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 6 leases to leases file.
Listening on LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on Socket/fallback/fallback-net
root@localhost ~# killall dhcpd
root@localhost ~#

```

```

root@localhost:~# dhcpd
Internet Systems Consortium DHCP Server 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
WARNING: Host declarations are global. They are not limited to the scope you
clared them in.
Not searching LDAP since ldap-server, ldap-port and ldap-base-dn were not sp
ied in the config file
Wrote 0 class decls to leases file.
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 6 leases to leases file.
Listening on LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on Socket/fallback/fallback-net
root@localhost ~#

```

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.

