



SRS-3106-4BT

**4 x 10/100/1000Base-T RJ-45
with IEEE 802.3af/at/bt PoE++ 90W Injector +
2 x 100/1000Base-X SFP
Managed Rugged PoE Switch**

SRS-3106

**4 x 10/100/1000Base-T RJ-45 +
2 x 100/1000Base-X SFP
Managed Rugged Switch**

Network Management

User's Manual

Version 1.0

Revision History

Version	F/W	Date	Description
1.0	1.00.00	2025/5/13	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 © 2025 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 R503, 1-23-13, Edobori,

Nishi-ku, Osaka 550-0002, Japan

Tel: +81-6-6450-8890

E-mail: cts_japan@ctsystem.com

Connection Technology Systems NE AB

E A Rosengrens gata 31,

421 31 Västra Frölunda,

Sweden

Tel: +46 31 22 19 80

E-mail: info@ctsystem.se

Connection Technology Systems CE GmbH

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

1100 Vienna

AUSTRIA

Tel: +43 1 343 9553 50

E-mail: cts_ce@ctsystem.com

Connection Technology Systems India Private Limited

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

Uttarahalli, Talgatpura, Kanakpura MN

Rd, Bangalore, Karnataka, India, 560062

E-mail: cts_in@ctsystem.com

Table of Content

1. INTRODUCTION	9
1.1 Management Options	9
1.2 Management Software	11
1.3 Management Preparations	12
2. Command Line Interface (CLI)	14
2.1 Using the Local Console.....	14
2.2 Remote Console Management - Telnet	15
2.3 Navigating CLI	15
2.3.1 General Commands.....	16
2.3.2 Quick Keys.....	16
2.3.3 Command Format.....	17
2.3.4 Login Username & Password	18
2.4 User Mode.....	19
2.4.1 Ping Command	19
2.4.2 Traceroute Command	19
2.5 Privileged Mode.....	21
2.5.1 Copy-cfg Command	21
2.5.2 Firmware Command	23
2.5.3 IP Command.....	23
2.5.4 Ping Command	23
2.5.5 Reload Command.....	24
2.5.6 Traceroute Command	24
2.5.7 Write Command	25
2.5.8 Configure Command.....	25
2.5.9 Show Command	26
2.6 Configuration Mode	28
2.6.1 Entering Interface Numbers	28
2.6.2 No Command.....	29
2.6.3 Show Command	29
2.6.4 Archive Command.....	31
2.6.5 Channel-group Command.....	32
2.6.6 Digital Input Command	35
2.6.7 Digital Output Command.....	35
2.6.8 Event Record	36
2.6.9 Fast Redundancy Command	37

2.6.10 IP Command	40
2.6.11 IPv6 Command	45
2.6.12 LLDP Command	47
2.6.13 Loop Detection Command	49
2.6.14 MAC Command	51
2.6.15 Management Command	54
2.6.16 Mirror Command	61
2.6.17 NTP Command	62
2.6.18 PoE Command	64
2.6.19 QoS Command	68
2.6.20 Security Command	78
2.6.21 Sfp Command	80
2.6.22 SNMP-Server Command	86
2.6.23 Spanning-tree Command	92
2.6.24 Switch Command	102
2.6.25 Switch-info Command	103
2.6.26 Syslog Command	106
2.6.27 Terminal Length Command	107
2.6.28 Time-range Command	108
2.6.29 User Command	111
2.6.30 VLAN Command	113
2.6.31 Interface Command	121
2.6.32 Show interface status Command	123
2.6.33 Show interface statistics Command	123
2.6.34 Show sfp Command	125
2.6.35 Show running-config & start-up-config & default-config Command	126
2.6.36 Show log Command	127
3. SNMP NETWORK MANAGEMENT	129
4. WEB MANAGEMENT	130
4.1 System Setup	133
4.1.1 Switch Information	134
4.1.2 IP Setup	136
4.1.3 IP Source Binding	139
4.1.4 Time Server Setup	140
4.1.5 Syslog Configuration	141
4.1.6 Time Range	142
4.2 Port Management	144

4.2.1 Port Setup & Status.....	145
4.2.2 Port Traffic Statistics	147
4.2.3 Port Packet Error Statistics	148
4.2.4 Port Packet Analysis Statistics	149
4.2.5 Port Mirroring	150
4.3 Link Aggregation.....	152
4.3.1 Distribution Rule.....	153
4.3.2 Static Port Trunking	153
4.4 VLAN Setup.....	155
4.4.1 VLAN Mode	156
4.4.2 Port Based VLAN.....	157
4.4.3 IEEE 802.1q VLAN	159
4.5 Rapid Spanning Tree	168
4.5.1 RSTP Switch Setup	169
4.5.2 RSTP Port Setup	170
4.5.3 RSTP Status	171
4.6 Fast Redundancy	173
4.6.1 Fast Redundancy Setup	174
4.6.2 Fast Redundancy Status.....	184
4.7 MAC Address Management.....	187
4.7.1 MAC Table Learning	188
4.7.2 MAC Address Table	189
4.8 QoS Setup.....	191
4.8.1 QoS Priority	192
4.8.2 QoS Remarking	194
4.8.3 QoS Rate Limit.....	196
4.9 Multicast	197
4.9.1 IGMP/MLD Snooping	197
4.10 Security Setup	205
4.10.1 DHCP Snooping Configuration	206
4.10.2 Port Isolation.....	207
4.10.3 Broadcast Storm Control.....	208
4.10.4 Loop Detection Configuration	209
4.11 LLDP.....	211
4.11.1 LLDP Setup.....	212
4.11.2 LLDP Status	213
4.12 Power over Ethernet.....	214

4.12.1 PoE Setup.....	215
4.12.2 PoE Status	218
4.13 Maintenance.....	220
4.13.1 CPU Loading	221
4.13.2 System Memory	223
4.13.3 CPU Temperature Status	224
4.13.4 Ping.....	227
4.13.5 Event Log.....	228
4.13.6 SFP Information	231
4.13.7 Digital Input.....	237
4.13.8 Digital Output	239
4.14 Management	242
4.14.1 Management Access Setup	244
4.14.2 User Account	246
4.14.3 RADIUS/TACACS+	248
4.14.4 Management Authentication	250
4.14.5 SNMP	252
4.14.6 Firmware Upgrade	260
4.14.7 Load Factory Settings	264
4.14.8 Auto-Backup Setup	265
4.14.9 Save Configuration	267
4.14.10 Reset System.....	267
APPENDIX A: FreeRADIUS Readme.....	268
APPENDIX B: Set Up DHCP Auto-Provisioning.....	270
APPENDIX C: VLAN Application Note.....	279
APPENDIX D: SFP/SFP+ Port Threshold	302

1. INTRODUCTION

Thank you for choosing the 4-port 10/100/1000M RJ-45 with IEEE 802.3af/at/bt 90W PoE injector and 2-port 100/1000M SFP Managed PoE Switch, or the 4-port 10/100/1000M RJ-45 and 2-port 100/1000M SFP Managed Switch, specifically designed for FTTx applications. The Managed Switch features a built-in management module, allowing users to configure and monitor its status locally or remotely.

This user manual provides instructions on configuring the Managed Switch via the command-line interface and web management. Readers should have a basic understanding of networking concepts and topologies to effectively utilize this manual and optimize the Managed Switch's performance.

1.1 Management Options

Switch management options available are listed below:

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

Local Console Management

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

Telnet Management

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

SNMP Management

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

Web Management

Web Management is done over the network and can be accessed via a standard web browser, such as Microsoft Internet Explorer. Once the Managed Switch is available on the network, you can login and monitor the status of it through a web browser remotely or locally. 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 SFP/SFP+ ports located on the front panel of the Managed Switch. A converter and direct RJ-45 LAN cable connection between a PC and the Managed Switch are required for Web Management.

SSH Management

SSH Management supports encrypted data transfer to prevent the data from being “stolen” for remote management. You can use PuTTY, a free and open source terminal emulator application which can act as a client for the SSH, to gain access to the Managed Switch.

1.2 Management Software

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

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

Console Program

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

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

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

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

SNMP Management System

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

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

Web Browser Application

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

1.3 Management Preparations

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

Connecting the Managed Switch

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

10/100/1000MBase-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-5E UTP or STP cable may be used. As to NBase-T RJ-45 port can be plugged with CAT-5E/CAT.6/CAT-6A (22~24 AWG) or better cabling.

100/1000MBase-X SFP Port

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

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

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

RS-232 RJ-45 Port (Console Port)

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

IP Addresses

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

IP addresses are made up of two parts:

- The first part (for example 192.168.n.n) refers to network address that identifies the network where the device resides. Network addresses are assigned by three allocation organizations. Depending on your location, each allocation organization assigns a globally unique network number to each network which intends to connect to the Internet.
- The second part (for example n.n.0.1) identifies the device within the network. Assigning unique device numbers is your responsibility. If you are unsure of the IP addresses allocated to you, consult with the allocation organization where your IP addresses were obtained.

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

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

MIB for Network Management Systems

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

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

2. Command Line Interface (CLI)

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

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

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

2.1 Using the Local Console

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

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

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

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

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

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

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

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

2.2 Remote Console Management - Telnet

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

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

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

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

Step 2. Run Telnet

Step 3. Log into the Switch CLI

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

Only 5 active Telnet sessions can access the Managed Switch at the same time.

2.3 Navigating CLI

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

Command Mode	Access Method	Prompt Displayed	Exit Method
User mode	Login username & password	Switch>	logout, exit
Privileged mode	From User mode, enter the <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.

2.3.1 General Commands

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

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

2.3.2 Quick Keys

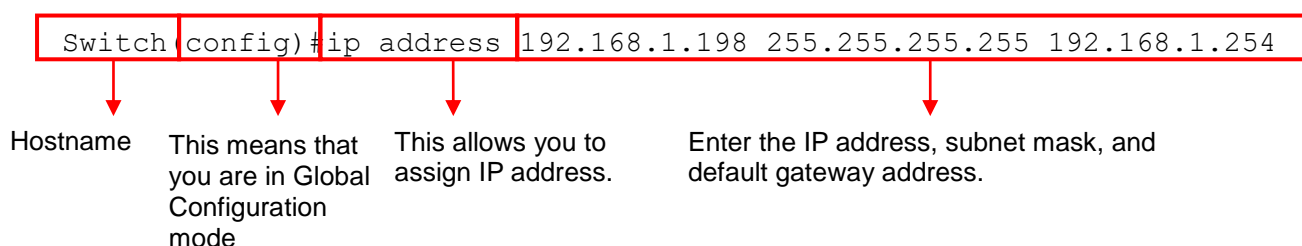
In CLI, there are several quick keys that you can use to perform several functions. The following table summarizes the most frequently used quick keys in CLI.

Keys	Purpose
tab	Enter an unfinished command and press “Tab” key to complete the command.
?	Press “?” key in each mode to get available commands.
Unfinished command followed by ?	<p>Enter an unfinished command or keyword and press “?” key to complete the command and get command syntax help.</p> <p>Example: List all available commands starting with the characters that you enter.</p> <pre>Switch#h? help Show available commands history Show history commands</pre>
A space followed by ?	Enter a command and then press Spacebar followed by a “?” key to view the next parameter.
Up arrow	Use Up arrow key to scroll through the previous entered commands, beginning with the most recent key-in commands.
Down arrow	Use Down arrow key to scroll through the previous entered commands, beginning with the commands that are entered first.

2.3.3 Command Format

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

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



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

Symbols	Brief Description
>	Currently, the device is in User mode.
#	Currently, the device is in Privileged mode.
(config)#	Currently, the device is in Global Configuration mode.
Syntax	Brief Description
[]	Reference parameter.
[-s size] [-r repeat] [-t timeout]	These three parameters are used in ping command and are optional, which means that you can ignore these three parameters if they are unnecessary when executing ping command.
[A.B.C.D]	Brackets represent that this is a required field. Enter an IP address or gateway address.
[255.X.X.X]	Brackets represent that this is a required field. Enter the subnet mask.
[port]	Enter one port number. See Section 2.6.34 for detailed explanations.
[port_list]	Enter a range of port numbers or several discontinuous port numbers. See Section 2.6.34 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

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

2.3.4 Login Username & Password

Default Login

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

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

Privileged Mode Password

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

Forgot Your Login Username & Password

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

2.4 User Mode

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

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

2.4.1 Ping Command

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

2.4.2 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
```

2.5 Privileged Mode

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

Command	Description
copy-cfg	Restore or backup configuration file via FTP or TFTP server.
disable	Exit Privileged mode and return to User Mode.
exit	Exit Privileged mode and return to User Mode.
firmware	Allow users to update firmware via FTP or TFTP.
help	Display a list of available commands in Privileged mode.
history	Show commands that have been used.
ip	Set up the DHCP recycle.
logout	Logout from the Managed Switch.
ping	Test whether a specified network device or host is reachable or not.
reload	Restart the Managed Switch.
traceroute	Trace the route to HOST.
write	Save your configurations to Flash.
configure	Enter Global Configuration mode.
show	Show a list of commands or show the current setting of each listed command.

2.5.1 Copy-cfg Command

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

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

Command	Parameter	Description
Switch# copy-cfg from ftp [A.B.C.D A:B:C:D:E:F:G:H] [file name] [user_name] [password]	[A.B.C.D A:B:C:D:E:F:G:H]	Enter the IPv4/IPv6 address of your FTP server.
	[file name]	Enter the configuration file name that you would like to restore.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
Switch# copy-cfg from tftp [A.B.C.D A:B:C:D:E:F:G:H] [file_name]	[A.B.C.D A:B:C:D:E:F:G:H]	Enter the IPv4/IPv6 address of your TFTP server.
	[file name]	Enter the configuration file name that you would like to restore.
Example		
Switch# copy-cfg from ftp 192.168.1.198 HS_0600_file.conf misadmin1 abcxyz		
Switch# copy-cfg from tftp 192.168.1.198 HS_0600_file.conf		

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

Command	Parameter	Description
Switch# copy-cfg to ftp [A.B.C.D A:B:C:D:E:F:G:H]	[A.B.C.D A:B:C:D:E:F:G:H]	Enter the IPv4/IPv6 address of your FTP server.
	[file name]	Enter the configuration file name that you want to

[file_name] [running default startup] [user_name] [password]		backup.
	[running default startup]	Specify backup config to be running, default or startup
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
Switch# copy-cfg to tftp [A.B.C.D A:B:C:D:E:F:G:H] [file_name] [running default startup]	[A.B.C.D A:B:C:D:E:F:G:H]	Enter the IPv4/IPv6 address of your TFTP server.
	[file_name]	Enter the configuration file name that you want to backup.
	[running default startup]	Specify backup config to be running, default or startup
Example		
Switch# copy-cfg to ftp 192.168.1.198 HS_0600_file.conf running misadmin1 abcxyz Switch# copy-cfg to tftp 192.168.1.198 HS_0600_file.conf startup		

3. Restore the Managed Switch back to default settings.

Command	Description
Switch# copy-cfg from default	Enter the IPv4/IPv6 address of your FTP server.
Switch# copy-cfg from default keep event	Restore the Managed Switch back to default settings but keep the entire data of event log.
Switch# copy-cfg from default keep event ip	Restore the Managed Switch back to default settings but keep both of the IP configurations and the entire data of event log.
Switch# copy-cfg from default keep ip	Restore the Managed Switch back to default settings but keep IP configurations.
Switch# copy-cfg from default keep ip event	Restore the Managed Switch back to default settings but keep both of the IP configurations and the entire data of event log.

2.5.2 Firmware Command

To upgrade firmware via TFTP or FTP server.

Command	Parameter	Description
Switch# firmware upgrade ftp [A.B.C.D A:B:C:D:E:F:G:H] [file_name][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 edgswitch10 abcxyz		
Switch# firmware upgrade tftp 192.168.1.198 HS_0600_file.bin alternate-image		

2.5.3 IP Command

Command	Parameter	Description
Switch# ip address dhcp recycle		DHCP Release packets and Discover packets will be sent to DHCP server in a manual way. And it will ask for IP address from DHCP server again. Note 1: Need to enable DHCP mode under the IP global configuration mode before issuing this command. See Section 2.6.9 “IP Command” for more details. Note 2: The command is just one-time command, and the setting will not be saved into the configuration file.

2.5.4 Ping Command

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

	[-c 1-99]	Enter the counts of PING packets that would be transmitted. The allowable value is from 1 to 99. (optional)
Example		
Switch# ping 8.8.8.8		
Switch# ping 8.8.8.8 -s 128 -c 10		
Switch# ping 2001:4860:4860::8888		
Switch# ping 2001:4860:4860::8888 -s 128 -c 10		

2.5.5 Reload Command

1. To restart the Managed Switch.

Command / Example
Switch# reload

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

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

2.5.6 Traceroute Command

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

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

2.5.7 Write Command

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

Command / Example
Switch# write Save Config Succeeded!

2.5.8 Configure Command

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

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

2.5.9 Show Command

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

1. Display system information

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

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

System Object ID: Display the predefined System OID.

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

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

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

DHCPv4/DHCPv6 Vendor ID: Display the Vendor Class Identifier used for DHCP/DHCPv6 relay agent function. Use “switch-info dhcp-vendor-id [dhcp_vendor_id]” command to edit this field.

Model Name: Display the product’s model name.

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

Current Boot Image: The image that is currently using.

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

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

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

M/B Version: Display the main board version.

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

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

Up Time: Display the up time since last restarting.

Local Time: Display the local time of the system.

Power: Display the installation status, the type, and the state of the power source.

CPU Temperature: Display the current CPU temperature of this device.

2. Display or verify currently-configured settings

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

3. Display interface information or statistics

Refer to “Show interface statistics command” and “Show sfp command” sections.

4. Show default, running and startup configurations

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

5. Show CPU & Memory Statistics

Show CPU utilization and memory usage rate. Refer to “Switch-info command” section.

6. Show Event Log

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

2.6 Configuration Mode

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

Command	Description
archive	Manage archive configuration files.
channel-group	Configure static link aggregation groups.
digital	Global Digital Input/Output configuration commands.
event-record	Configure the Event Record function.
exit	Exit the global configuration mode.
fast-redundancy	Set up the Fast Redundancy function.
help	Display a list of available commands in the global configuration mode.
history	Show commands that have been used.
ip	Set up the IPv4 address and enable DHCP mode & IGMP snooping.
ipv6	To enable ipv6 function and set up IP address.
lldp	LLDP global configuration mode.
loop-detection	Configure loop-detection to prevent loop between switch ports by locking them.
mac	Set up MAC learning function of each port.
management	Set up console/telnet/web/SSH access control and timeout value, RADIUS/TACACS+, and authentication method management.
mirror	Set up target port for mirroring.
ntp	Set up required configurations for Network Time Protocol.
poe	Set up Power over Ethernet and the related alarm configuration.
qos	Set up the priority of packets within the Managed Switch.
security	Configure broadcast, unknown multicast, unknown unicast storm control settings.
sfp	Configure SFP monitored items’ parameters and view the current value of each item.
snmp-server	Create a new SNMP community and trap destination and specify the trap types.
spanning-tree	Set up RSTP status of each port and aggregated ports.
switch	Set up acceptable frame size and address learning, etc.
switch-info	Edit the system information.
syslog	Set up required configurations for Syslog server.
terminal	Set up Terminal functions.
time-range	Time Range management.
user	Create a new user account.
vlan	Set up VLAN mode and VLAN configuration.
no	Disable a command or reset it back to its default setting.
interface	Select a single interface or a range of interfaces.
show	Show a list of commands or show the current setting of each listed command.

2.6.1 Entering Interface Numbers

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

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

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

2.6.2 No Command

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

2.6.3 Show Command

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

1. Display system information

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

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

System Object ID: Display the predefined System OID.

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

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

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

DHCPv4/DHCPv6 Vendor ID: Display the Vendor Class Identifier used for DHCP/DHCPv6 relay agent function. Use “switch-info dhcp-vendor-id [dhcp_vendor_id]” command to edit this field.

Model Name: Display the product’s model name.

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

Current Boot Image: The image that is currently using.

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

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

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

M/B Version: Display the main board version.

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

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

Up Time: Display the up time since last restarting.

Power: Display the installation status, the type, and the state of the power source.

CPU Temperature: Display the current CPU temperature of this device.

2. Display or verify currently-configured settings

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

3. Display interface information or statistics

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

4. Show default, running and startup configurations

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

5. Show CPU & Memory Statistics

Show CPU utilization and memory usage rate. Refer to "Switch-info command" section.

6. Show Event Log

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

2.6.4 Archive Command

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

2.6.5 Channel-group Command

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

Channel-group Command	Parameter	Description
Switch(config)# channel-group trunking [group_name]	[group_name]	Specify a name for this link aggregation group. Up to 15 alphanumeric characters can be accepted.
Switch(config)# channel-group trunking [group_name] rename [new_group_name]	[group_name] [new_group_name]	Specify a new name for this link aggregation group. Up to 15 alphanumeric characters can be accepted.
Switch(config)# interface [port_list] Switch(config-if-PORT-PORT)# channel-group trunking [group_name]	[port_list] [group_name]	Use “interface” command to configure a group of ports’ link aggregation link membership. Assign the selected ports to the specified link aggregation group.
Switch(config)# channel-group distribution-rule destination-ip		Load-balancing depending on destination IP address.
Switch(config)# channel-group distribution-rule destination-mac		Load-balancing depending on destination MAC address.
Switch(config)# channel-group distribution-rule source-ip		Load-balancing depending on source IP address.
Switch(config)# channel-group distribution-rule source-mac		Load-balancing depending on source MAC address.
No command		
Switch(config)# no channel-group trunking [group_name]	[group_name]	Delete a link aggregation group.
Switch(config)# interface [port_list] Switch(config-if-PORT-PORT)# no channel-group trunking	[port_list]	Remove the selected ports from a link aggregation group.
Switch(config)# no channel-group distribution-rule destination-ip		Disable load-balancing based on destination IP address.
Switch(config)# no channel-group type destination-mac		Disable load-balancing based on destination MAC address.
Switch(config)# no channel-group distribution-rule source-ip		Disable load-balancing based on source IP address.
Switch(config)# no channel-group type source-mac		Disable load-balancing based on source MAC address.
Show command		
Switch(config)# show channel-group trunking		Show link aggregation settings and distribution rule information.
Switch(config)# show channel-group trunking [trunk_name]	[trunk_name]	Show a specific link aggregation group’s settings including aggregated port numbers and distribution rule information.

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

	Command	Purpose
STEP1	configure Example: Switch# config Switch(config)#	Enter the global configuration mode.
STEP2 <i>(Optional)</i>	channel-group distribution-rule source-ip Example: Switch(config)# channel-group distribution-rule source-ip OK !	Enable Source IP Address in Distribution Rule.
STEP3 <i>(Optional)</i>	channel-group distribution-rule destination-ip Example: Switch(config)# channel-group distribution-rule destination-ip OK !	Enable Destination IP Address in Distribution Rule.
STEP4 <i>(Optional)</i>	channel-group distribution-rule source-mac Example: Switch(config)# channel-group distribution-rule source-mac OK !	Enable Source Mac Address in Distribution Rule.
STEP5 <i>(Optional)</i>	channel-group distribution-rule destination-mac Example: Switch(config)# channel-group distribution-rule destination-mac OK !	Enable Destination Mac Address in Distribution Rule.
STEP6	channel-group trunking <i>group_name</i> Example: Switch(config)# channel-group trunking CTSGROUP OK !	In this example, it configures the name of the Trunking Group as "CTSGROUP".
STEP7	interface <i>port_list</i> Example: Switch(config)# interface 1,3 Switch(config-if-1,3)#	Speciy the interface that you would like to set to Trunking Group.
STEP8	channel-group trunking <i>group_name</i> Example: Switch(config-if-1,3)# channel-group trunking CTSGROUP OK !	In this example, it configures Port 1 and Port 3 as the link membership of "CTSGROUP"Trunking Group
STEP9	exit Example: Switch(config-if-1,3)# exit Switch(config)#	Return to the global configuration mode.

STEP10	exit Example: Switch(config)# exit Switch#	Return to the Privileged mode.
STEP11	write Example: Switch# write Save Config Succeeded! OK !	Save the running configuration into the startup configuration.

2.6.6 Digital Input Command

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

2.6.7 Digital Output Command

Digital Input Command	Parameter	Description
Switch(config)# digital output [1]	[1]	Specify the digital output number.
Switch(config-output-1)# normal [open close]	[open close]	Specify the normal digital output type between open and close status for the digital Output 1.
Switch(config-output-1)# event digital-input [1]	[1]	Enable the alarm of the specified digital input number for the Digital Output 1.
Switch(config-output-1)# event port [port_list]	[port_list]	Enable the port alarm of the specified port(s) for the Digital Output 1.
Switch(config-output-1)# event power [a b]	[a b]	Enable the power alarm of the specified power source for the Digital Output 1.
Switch(config-output-1)# trigger		Enable the digital output trigger event function for the Digital Output 1.
No command		
Switch(config-output-1)# no normal		Reset the normal digital output type back to the default. (Open)

Switch(config-output-1)# no event digital-input [1]	[1]	Disable the alarm of the specified digital input number for the Digital Output 1
Switch(config-output-1)# no event port [port_list]	[port_list]	Disable the port alarm of the specified port(s) for the Digital Output 1.
Switch(config-output-1)# no event power [a b]	[a b]	Disable the power alarm of the specified power source for the Digital Output 1.
Switch(config-output-1)# no trigger		Disable the digital output trigger event function for the Digital Output 1.
Show command		Description
Switch# show digital output		Display the current digital output information.
Switch# show digital output status		Display the digital output status.
Switch(config)# show digital output		Display the current digital output information.
Switch(config)# show digital output status		Display the digital output status.
Switch(config-output-1)# show		Display the current normal and event trigger status as well as Event Configuration of the specified Digital Output.

2.6.8 Event Record

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# show event-record		Show the Event Record function configuration.
Switch(config)# show event-record		Show the Event Record function configuration.

2.6.9 Fast Redundancy Command

Besides RSTP and Ring Detection, the employment of CTS's proprietary fast redundancy on your network will help protect mission-critical links against failures, avoid the occurrence of network loops, and keep network downtime to a minimum to assure the reliability of the network. With these network redundancy, it allows the user to set up redundant loops in a network to provide a backup data transmission route in the event of the disconnection or damage of the cables. By means of this important feature in the network recovery applications, you can be totally free from any loss resulting from the time spent in locating the cable that fails to connect.

CTS's fast redundancy provides **Fast Ring v2** and **Chain** two redundancy protocols, which allows you to configure 2 rings, 2 chains, or 1 ring & 1 chain at most for a switch.

Please note that all switches on the same ring or chain must be the ones with the same brand and configured using the same redundancy protocol when configuring a redundant ring or chain. You are not allowed to use switches with different brands or mix the Ring Detection, Fast Ring v2 and Chain protocols within the same ring or chain.

In the following table, it lists the difference among forementioned redundancy protocols for your evaluation when employing network redundancy on your network.

	Ring Detection	Fast Ring v2	Chain	RSTP
Topology	Ring	Ring	Ring	Ring
Recovery Time	<30 ms	<50 ms	<div><1 second (for copper ports)</div> <div><50 ms (for fiber ports)</div>	Up to 5 seconds

Fast Redundancy Command	Parameter	Description
Switch(config)# fast-redundancy id [group_id]	[1-2]	Create a fast redundancy group and assign it to an id number.
Switch(config-fr-ID)# description [description]	[description]	Enter a brief description for the specified fast redundancy group. Up to 35 alphanumeric characters can be accepted.
Switch(config-fr-ID)# enable		Enable the specified group of fast redundancy. Note: The port setting must be done beforehand to successfully enable the fast redundancy group.
Switch(config-fr-ID)# protocol chain		Apply the Chain protocol on the specified group of fast redundancy.
Switch(config-fr-ID-chain)# chain-port1 interface [port_number] role [head member tail] chain-port2	[port_number]	Specify a single port to serve as the 1 st interface of the Chain protocol. Note:

[disable]		Each port can only be assigned to one single interface in the entire configuration of the fast redundancy.
	[head member tail]	Assign a role to the 1 st interface of the Chain protocol.
	[disable]	Disable the 2 nd interface of the Chain protocol. Only when the role of the 1 st interface of the Chain protocol is specified as either head or tail can the 2 nd interface be disabled.
Switch(config-fr-ID-chain)# chain-port1 interface [port_number] role [head member tail] chain-port2 interface [port_number] role [member]	[port_number]	Specify a single port to serve as the 2 nd interface of the Chain protocol. Note: Each port can only be assigned to one single interface in the entire configuration of the fast redundancy.
	[head member tail]	Assign a role to the 2 nd interface of the Chain protocol.
	[port_number]	Specify a single port to serve as the 2 nd interface of the Chain protocol. Note: Each port can only be assigned to one single interface in the entire configuration of the fast redundancy.
	[member]	Assign a role to the 2 nd interface of the Chain protocol. Only member is allowed.
Switch(config-fr-ID)# protocol [fast-ringv2] role [master slave]	[fast-ringv2]	Apply the Fast Ring v2 protocol on the specified group of fast redundancy.
	[master slave]	Specify the role of the Managed Switch.
Switch(config-fr-ID-ringv2- ROLE)# ring-port1 interface [port_number] ring-port2 interface [port_number]	[port_number]	Specify a single port to serve as the 1 st interface of the Fast Ring v2 protocol. Note: Each port can only be assigned to one single interface in the entire configuration of the fast redundancy.
	[port_number]	Specify a single port to serve as the 2 nd interface of the Fast Ring v2 protocol. Note: Each port can only be assigned to one single interface in the

		entire configuration of the fast redundancy.
No Command		
Switch(config)# no fast-redundancy id [group_id]	[1-2]	Remove the specified fast redundancy group.
Switch(config-fr-ID)# no description		Remove the configured description for the specified fast redundancy group.
Switch(config-fr-ID)# no enable		Disable the specified group of fast redundancy.
Show Command		
Switch(config)# show fast-redundancy all		Show the current configuration, the topology change status, and the statistics of the entire fast redundancy function.
Switch(config)# show fast-redundancy id [group_id]	[1-2]	Show the current configuration of the specified fast redundancy group and the topology change status.
Switch(config)# show fast-redundancy id [group_id] statistics	[1-2]	Show the current configuration and the statistics of the specified fast redundancy group.
Switch(config)# show fast-redundancy id [group_id] statistics clear	[1-2]	Clear the statistics of the specified fast redundancy group.
Switch(config)# show fast-redundancy topology		Show the fast redundancy topology change status.
Switch(config)# show fast-redundancy topology clear		Clear the record of the fast redundancy topology change status.
Examples of Fast Redundancy Command		
Switch(config)# fast-redundancy id 1		Create a fast redundancy group and specify its ID to 1.
Switch(config-fr-1)# description 18F_office		Add a brief description "18F_office" to the fast redundancy group.
Switch(config-fr-1)# protocol chain		Apply the Chain protocol on the fast redundancy group.
Switch(config-fr-1-chain)# chain-port1 interface 6 role head chain-port2 disable		Specify the 6 th port of the Managed Switch as the 1 st interface and disable the 2 nd interface of the chain protocol. And assign the 1 st interface as the role of head.
Switch(config-fr-1-chain)# chain-port1 interface 4 role head chain-port2 interface 5 role member		Specify the 4 th port of the Managed Switch as the 1 st interface and the 5 th port as the 2 nd interface of the chain protocol, and assign the 1 st interface as head, and the 2 nd interface as member.
Switch(config-fr-1)# protocol fast-ringv2 role master		Apply the Fast Ring v2 protocol on the fast redundancy group, and specify the role of the Managed Switch as master.
Switch(config-fr-1-ringv2-master)# ring-port1 interface 2 ring-port2 interface 3		Specify the 2 nd port as the 1 st interface of the Fast Ring v2

	protocol, and the 3 rd port as the 2 nd interface.
Switch(config-fr-1)# enable	Enable the fast redundancy group.

2.6.10 IP Command

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

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

2. Enable IPv4 DHCP Auto Recycle function.

IP Auto Recycle Command	Parameter	Description
Switch(config)# ip address dhcp auto-recycle		Enable IPv4 DHCP Auto Recycle function globally. NOTE: Please configure IPv4 DHCP Auto Recycle function via interface command first.
No command		
Switch(config)# no ip address dhcp auto-recycle		Disable IPv4 DHCP Auto Recycle function globally.

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

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

4. Enable DHCPv4/DHCPv6 relay function.

DHCP Snooping Command	Parameter	Description
Switch(config)# ip dhcp snooping		Enable DHCPv4/DHCPv6 snooping function.
No command		
Switch(config)# no ip dhcp snooping		Disable DHCPv4/DHCPv6 snooping function.
Show command		
Switch(config)# show ip dhcp snooping		Show DHCPv4/DHCPv6 snooping configuration.

5. Use “Interface” command to configure a group of ports’ DHCP Snooping settings.

DHCP Snooping & Interface Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# ip dhcp snooping server-trust		Enable the selected interfaces as DHCPv4/DHCPv6 server trust ports.
No command		
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# no ip dhcp snooping server-trust		Reset the selected interfaces back to non-DHCPv4/DHCPv6 server trust ports.

6. Enable or disable IGMP/MLD snooping globally.

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

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

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

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

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

IGMP/MLD Snooping Command	Parameter	Description
Switch(config)# ip igmp snooping		Enable IGMP/MLD snooping. When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic. This is for IGMPv1, v2 and MLDv1 only.
Switch(config)# ip igmp snooping version-3		Enable IGMPv3/MLDv2 snooping. When enabled, the Managed Switch will monitor network traffic and determine which hosts to receive multicast traffic. This is for IGMPv3 and MLDv2 only.
Switch(config)# ip igmp snooping immediate-leave		Enable immediate leave function.
Switch(config)# ip igmp snooping stream-life-time		Enable IGMP/MLD snooping stream life time function. The multicast packet stream will be stopped once reaching the end of its specified lifespan. Note: The length of stream life time is determined by the total amount of the specified <u>query-interval</u> and <u>max-response-time</u> (125 and 10 seconds in default, respectively).
Switch(config)# ip igmp snooping max-response-time [1-	[1-255] (Unit:1/10secs)	Specify the IGMP/MLD querier maximum response time. This determines the

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

7. Use “Interface” command to configure a group of ports’ IGMP/MLD snooping settings.

IGMP/MLD Snooping & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# ip igmp snooping mcast-router		Specify the selected port(s) as the multicast router port.

No command		
Switch(config-if-PORT-PORT)# no ip igmp snooping mcast-router		Remove the selected port(s) from the multicast router port list.
Examples of IP IGMP Snooping & Interface		
Switch(config)# interface 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 igmp snooping mcast-router		Configure Port 1~3 as the multicast router port.
Switch(config-if-1-3)# no ip igmp snooping mcast-router		Remove Port 1~3 from the multicast router port list.

8. Set Up IP Source Binding Function.

IP Source Binding Command	Parameter	Description
Switch(config)# ip source		Globally enable IPv4/IPv6 address security binding.
Switch(config)# ip source binding [1-5]	[1-5]	Enable IPv4/IPv6 address security binding for the specified number.
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.
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.

2.6.11 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 IPv6 global address and prefix-length of the Managed Switch.
[A:B:C:D:E:F:G:H/10~128] [A:B:C:D:E:F:G:H]	[A:B:C:D:E:F:G:H]	Specify IPv6 default gateway IP address of the Managed Switch.
Switch(config)# ipv6 address link-local	[A:B:C:D:E:F:G:H/10~128]	Specify IPv6 link-local address and prefix-length of the Managed Switch.
[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 address processing.
Show command		
Switch# show ipv6 address		Display IPv6 configuraiton and the current IPv6 status of the Managed Switch.
Switch(config)# show ipv6 address		Display IPv6 configuraiton and the current IPv6 status of the Managed Switch.
Examples of IPv6 command		
Switch(config)# ipv6 address autoconfig		Enable IPv6 autoconfiguration.
Switch(config)# ipv6 address dhcp auto		Enable DHCPv6 auto mode.

2.6.12 LLDP Command

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

LLDP Command	Parameter	Description
Switch(config)# lldp		Enable LLDP function globally.
Switch(config)# lldp hold-time [1-3600]	[1-3600]	Specify the amount of time in seconds. A receiving device will keep the information sent by your device for a period of time you specify here before discarding it. The allowable hold-time value is between 1 and 3600 seconds.
Switch(config)# lldp interval [1-180]	[1-180]	Specify the time interval for updated LLDP packets to be sent. The allowable interval value is between 1 and 180 seconds.
Switch(config)# lldp packets [1-16]	[1-16]	Specify the amount of packets that are sent in each discovery. The allowable packet value is between 1 and 16 packets.
Switch(config)# lldp tlv-select capability		Enable Capability attribute to be sent.
Switch(config)# lldp tlv-select management-address		Enable Management Address attribute to be sent.
Switch(config)# lldp tlv-select port-description		Enable Port Description attribute to be sent.
Switch(config)# lldp tlv-select system-description		Enable System Description attribute to be sent.
Switch(config)# lldp tlv-select system-name		Enable System Name attribute to be sent.
No command		
Switch(config)# no lldp		Disable LLDP function.
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	
Switch(config)# lldp hold-time 60	Set the hold-time value to 60 seconds.
Switch(config)# lldp interval 10	Set the updated LLDP packets to be sent in very 10 seconds.
Switch(config)# lldp packets 2	Set the number of packets to be sent in each discovery to 2.
Switch(config)# lldp tlv-select capability	Enable Capability attribute to be sent.
Switch(config)# lldp tlv-select management-address	Enable Management Address attribute to be sent.
Switch(config)# lldp tlv-select port-description	Enable Port Description attribute to be sent.
Switch(config)# lldp tlv-select system-description	Enable System Description to be sent.
Switch(config)# lldp tlv-select system-name	Enable System Name to be sent.

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

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

2.6.13 Loop Detection Command

In a real network, it is possible for people to misconnect network cables, leading to a loop condition. In the worst-case scenario, this can cause the network to become non-operational. This section provides guidance on configuring the system's Loop Detection function to prevent such loops.

When the Loop Detection function is properly configured, the system detects loop conditions by checking the VLAN and MAC addresses of received packets and comparing them against the MAC address table. Once a loop condition is detected on specific port(s), the system takes the following actions:

1. **Block the affected port(s):** The system stops forwarding all traffic through the looped port(s).
2. **Send an SNMP trap:** This notification informs the network administrator of the detected loop condition.

After the system blocks relevant port, there are two ways to unlock it:

1. **Automatic Unlock:** The system will automatically unlock the blocked port after the configured Unlock Interval (in minutes) has elapsed. The default interval is 1440 minutes.
2. **Manual Unlock:** The network administrator can manually unlock the blocked port.

NOTE: Loop Detection, Fast redundancy and RSTP (Rapid Spanning Tree Protocol) is not allowed to be enabled on the same port at the same time.

Loop Detection Command	Parameter	Description
Switch(config)# loop-detection		Enable Loop Detection function.
Switch(config)# loop-detection unlock-interval [1-1440]	[1-1440]	Set the unlock time interval for ports that have been blocked by the loop detection function. After the specified unlock interval has elapsed, the system will automatically unlock the blocked port. The unlock interval can be set to any value between 1 and 1440 minutes, with a default value of 1440 minutes. NOTE: <i>Users can also manually unlock a port that has been blocked by the loop detection function</i>
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# show loop-detection		Show Loop Detection configuration.
Switch# show loop-detection status		Show Loop Detection status of all ports.
Switch# show loop-detection	[port_list]	Show Loop Detection status of the

status [port_list]		specified port(s).
Switch(config)# show loop-detection		Show Loop Detection configuration.
Switch(config)# show loop-detection status		Show Loop Detection status of all ports.
Switch(config)# show loop-detection status [port_list]	[port_list]	Show Loop Detection status of the specified port(s).
Examples of Loop Detection command		
Switch(config)# loop-detection unlock-interval 120		Set the Loop Detection unlock time interval to 120 minutes.

Use the “Interface” command to manually unlock the blocked port(s).

Loop Detection & Interface Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# loop-detection unlock		Unlock the selected port(s) that are locked.

2.6.14 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 [7-600000]	[7-600000]	Specify MAC address table aging time between 7 and 600000 seconds. "0" means that MAC addresses will never age out.
No command		
Switch(config)# no mac address-table aging-time		Reset MAC address table aging time back to the default. (300 seconds).
Show command		
Switch(config)# show mac address-table all		Show all of MAC table information.
Switch(config)# show mac address-table all [mac vid port]	[mac vid port]	Show all learned MAC addresses sorted by specific option.
Switch(config)# show mac address-table clear		Clear MAC address table.
Switch(config)# show mac address-table clear [port_list]	[port_list]	Clear MAC addresses learned by the specified port.
Switch(config)# show mac address-table count		Show the statistics of MAC address table.
Switch(config)# show mac address-table interface [port_list] [mac vid port]	[port_list]	Show the MAC addresses learned by the specified port.
	[mac vid port]	Show the learned MAC addresses sorted by specific option.
Switch(config)# show mac address-table mac [xx:xx:xx xx:xx:xx:xx:xx:xx] [mac vid port]	[xx:xx:xx]	Show the MAC address that its first 3 bytes starting with the specified MAC.
	[xx:xx:xx:xx:xx:xx]	Show the MAC address that its 6 bytes totally meet the specified MAC.
	[mac vid port]	Show the matched MAC addresses sorted by specific option.
Switch(config)# show mac address-table vlan [vlan_id] [mac vid port]	[vlan_id]	Show the MAC addresses that belongs to the specified VLAN ID.
	[mac vid port]	Show the specified VLAN's MAC addresses sorted by specific option.
Switch(config)# show mac 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] [mac port vlan sort-by]	[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 sort-by]	(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.

2.6.15 Management Command

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

Management Command	Parameter	Description
Switch(config)# management cli timeout [1-1440]	[1-1440]	To disconnect the Managed Switch when cli management is inactive for a certain period of time. The allowable value is from 1 to 1440 (seconds).
Switch(config)# management cli timeout [1-1440] min	[1-1440]	To disconnect the Managed Switch when cli management is inactive for a certain period of time. The allowable value is from 1 to 1440 (minutes).
Switch(config)# management console		Enable Console management. To manage the Managed Switch via Console.
Switch(config)# management console fail-retry [1-10]	[1-10]	Configure the retry times if the console login fails. The allowable value is 1~10 (times).
Switch(config)# management console block-time [1-120]	[1-120]	Configure the console block time of the Managed Switch if the console login retry times are more than the console fail-retry value you set up. The allowable value 1-120 (minutes).
Switch(config)# management ssh		Enable SSH management. To manage the Managed Switch via SSH.
Switch(config)# management telnet		Enable Telnet Management. To manage the Managed Switch via Telnet.
Switch(config)# management telnet port [1-65535]	[1-65535]	When telnet is enabled, you can set up the port number that allows telnet access. The default port number is set to 23. However, you can also identify a port number between 1 and 65535.
Switch(config)# management web		Enable Web management by the http method.
Switch(config)# management web [http https disable]	[http https disable]	Enable or disable Web Management. You can enable this management and manage the Managed Switch via the specified web management method between http and https.
Switch(config)# management web timeout [1-1440]	[1-1440]	To disconnect the Managed Switch when web management is inactive for a certain period of time. The allowable value is from 1 to 1440 (minutes).
No command		
Switch(config)# no management cli timeout		Reset cli timeout value back to the default (300 seconds).
Switch(config)# no management console		Disable Console management.
Switch(config)# no management console fail-retry		Reset console fail-retry times back to the default (3 times).

Switch(config)# no management console block-time		Reset console block-time back to the default (5 minutes).
Switch(config)# no management ssh		Disable SSH management.
Switch(config)# no management telnet		Disable Telnet management.
Switch(config)# no management telnet port		Reset Telnet port back to the default. The default port number is 23.
Switch(config)# no management web		Disable Web management.
Switch(config)# no management web timeout		Reset web timeout value back to the default (20 minutes).
Show command		
Switch(config)# show management		Show the current management configuration of the Managed Switch.
Examples of Management command		
Switch(config)# management cli timeout 300		The cli management will timeout (logout automatically) when it is inactive for 300 seconds.
Switch(config)# management telnet		Enable Telnet management.
Switch(config)# management telnet port 23		Set Telnet port to port 23.
Switch(config)# management web https		Enable Web Management and manage the Managed Switch via "https" web management method.

Configure RADIUS server authentication method.

Management Radius Command	Parameter	Description
Switch(config)# management radius secret-key-encryption [aes-128]	[aes-128]	Specify AES-128 as the encryption method to secure the secret key against potential malicious attacks. aes-128 (advanced encryption method): An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data.
Switch(config)# management radius retry-time [0-3]	[0-3]	Specify the retry time value. This is the number of times that the Managed Switch will try to reauthenticate if the RADIUS server is not reachable.
Switch(config)# management radius timeout [1-3]	[1-3]	Specify the timeout value (second). This is the amount of time that the Managed Switch will wait if the RADIUS server is not responding.
Switch(config)# management radius [1-2]	[1-2]	Specify a RADIUS server number to configure.
Switch(config-radius-NUMBER)# enable		Enable the RADIUS server.
Switch(config-radius-NUMBER)# port [1025-65535]	[1025-65535]	Specify the RADIUS server's port number.

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

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

Configure TACACS+ server authentication method.

Management Tacacs Command	Parameter	Description
Switch(config)# management tacacs secret-key-encryption [aes-128]	[aes-128]	Specify AES-128 as the encryption method to secure the secret key against potential malicious attacks. aes-128 (advanced encryption method): An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data.
Switch(config)# management tacacs retry-time [0-3]	[0-3]	Specify the retry time value. This is the number of times that the Managed Switch will try to reauthenticate if the TACACS+ server is not reachable.
Switch(config)# management tacacs timeout [1-3]	[1-3]	Specify the timeout value (second). This is the amount of time that the Managed Switch will wait if the TACACS+ server is not responding.
Switch(config)# management tacacs [1-2]	[1-2]	Specify a TACACS+ server number to configure.
Switch(config-tacacs-NUMBER)# enable		Enable the TACACS+ server.
Switch(config-tacacs-NUMBER)# port [49, 1025-65535]	[49, 1025-65535]	Specify the TACACS+ server's port number.
Switch(config-tacacs-NUMBER)# secret [secret]	[secret]	Specify a secret, up to 32 alphanumeric characters, for the TACACS+ server. This secret key is used to validate communications with the TACACS+ server.
Switch(config-tacacs-NUMBER)# secret aes-128 [base64]	[base64]	Specify the secret encrypted by aes-128. aes-128 (advanced encryption method): An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data.
Switch(config-tacacs-NUMBER)# server-ip [A.B.C.D A:B:C:D:E:F:G:H]	[A.B.C.D A:B:C:D:E:F:G:H]	Specify the TACACS+ server's IPv4/IPv6 address.

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

Configure authentication method management.

Management Command	Parameter	Description
--------------------	-----------	-------------

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

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

2.6.16 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 sets of port mirroring can be set up.
Switch (config-mirror-index)# enable		Enable the specified port mirroring. NOTE: This command works only when its mirroring-related settings are completed.
Switch(config-mirror-index)# destination [port_number]	[port_number]	Specify the preferred destination port 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-1)# destination 4		The selected source ports' data will mirror to Port 4 in the port mirroring of Index No. 1.
Switch(config-mirror-1)# source 1-3 direction tx		Port 1 to 3's transmitting packets will mirror to the destination port in the port mirroring of Index No. 1.

2.6.17 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.

2.6.18 PoE Command

PoE (Power over Ethernet) is the technology that a data-carrying RJ-45 cable can play a role in power supplier. Typically, a PoE switch is deployed at the center of the network for power transmission and supplies electricity to PDs (powered devices) up to 100 meters away through TP ports. PDs can be installed wherever there is a RJ-45 cable rather than AC power source. The user need not be present at powered devices location, which greatly reduces truck rolls. The Managed PoE Switch even supports time-based PoE, defining the time interval when powered devices are desired to be automatically powered on a daily or weekly basis, for budget-conscious users to be more efficient power management.

NOTE: The PoE command is available only on PoE switch models. This command will not be shown or executable on non-PoE devices.

1. Set up PoE power budget, PoE alarm and PoE sequence.

Command	Parameter	Description
Switch(config)# poe		Enable the function of Power over Ethernet globally.
Switch(config)# poe alarm-threshold [1-99]	[1-99]	Set up the power usage alarm threshold in percentage.
Switch(config)# poe sequence		Enabled the PoE Power on Sequence function.
Switch (config)# poe sequence interval [3-30]	[3-30]	Configure the PoE power on sequence interval time (secs).
Switch (config)# poe sequence option [port priority]	[port priority]	Configure the PoE power on sequence by port number or by PoE priority. Port: Each PoE ports is power on in sequence according to port number. Priority: Each PoE ports is power on in sequence according to assigned port priority.
Switch (config)# poe total-budget [0-300]	[0-300]	Configure the total PoE budget for the system, with a valid range from 0 to 300 watts.
No command		
Switch(config)# no poe		Disable the function of Power over Ethernet globally.
Switch(config)# no poe alarm-threshold		Reset the alarm percentage threshold of power usage back to the default. (95%).
Switch (config)# no poe sequence		Disable the PoE Power on Sequence function.
Switch (config)# no poe sequence interval		Reset the power on sequence interval to default value of 3 seconds.
Switch (config)# no poe sequence option		Reset the PoE power on sequence option to default, which is to power on in sequence according to port number.
Switch (config)# no poe total-budget		Reset the total PoE budget for the system, the default value is 300 watts.
Show command		

Switch# show poe		Show the total PoE power budget in watts for the system and the current PoE system configuration.
Switch# show poe status		Show the current total PoE budget, total PoE power consumption and PoE status of all PoE ports.
Switch# show poe status interface		Show the current total PoE budget, total PoE power consumption and PoE status of all PoE ports.
Switch# show poe status interface [port_list]	[port_list]	Show the current total PoE budget and total PoE power consumption, and PoE status on selected port(s).
Switch# show poe interface		Show the current PoE configuration of all PoE ports.
Switch# show poe interface [port_list]	[port_list]	Show the current PoE configuration of specific port(s).
Switch# show poe interface detailed		Show PoE interface detailed configuration and status on all PoE ports.
Switch# show poe interface detailed [port_list]	[port_list]	Show PoE interface detailed configuration and status on specific PoE port(s).
Switch# show poe interface schedule		Show the current PoE Schedule configuration and schedule status of all PoE ports.
Switch# show poe interface schedule [port_list]	[port_list]	Show the current PoE Schedule configuration and schedule status of specific port(s).

2. Use “interface” command to configure PoE parameters per TP port for PDs.

Interface Command	Parameter	Description
Switch (config)# interface [port_list]	[port_list]	Select specific port(s) to make further configuration.
Switch(config-if-PORT-PORT)# poe budget [10-900]	[10-900]	Configure maximum PoE budget in unit of 1/10 watt. Note: This configuration only takes effect when PoE inline mode is in the fix and force mode.
Switch(config-if-PORT-PORT)# poe inline [auto-af/at auto-bt fix force]	[auto-af/at auto-bt fix force]	Configure specify port's inline mode, default PoE inline mode is auto-bt mode. auto-af/at: Specified PoE port(s) offers PoE power with PoE class level in 802.3af/at mode. auto-bt: Specified PoE port(s) offers PoE power with PoE class level in 802.3af/at/bt mode. fix: Specified PoE port(s) offers PoE power by user's definition according to 802.3af/at/bt mode.

		force: 1) Specified PoE port(s) offers PoE power according to user definition. 2) Specified PoE port(s) provide non-standard PoE output no matter what device is attached.
Switch(config-if-POR-T-POR-T)# poe pdname [device_name]	[device_name]	Name the powered device that is connected to the selected port(s). Maximum 32 alphanumeric characters.
Switch(config-if-POR-T-POR-T)# poe priority [critical high low]	[critical high low]	Configure PoE output priority when total power consumption is over total power budget. low: It indicates the port(s) with this priority will be the first port(s) to get power cut off. high: It indicates the port(s) with this priority will terminate the power supply after all ports assigned with the “Low” priority get power cut off. critical: It indicates the port(s) with this priority will be the last port(s) to get power cut off. NOTE: Power will be cut off upon the order of port number (Port4→Port3→Port2→Port1) if ports are assigned with the same priority. For example, in case Port2 and Port4 are both the low-priority ports, power supplied by Port4 will be cut off earlier than Port2.
Switch(config-if-POR-T-POR-T)# poe re-enabled		Shut down the PoE output on selected port(s), it will restart after the re-enabled interval. The re-enabled interval is defined by “poe re-enabled interval.”
Switch(config-if-POR-T-POR-T)# poe re-enabled interval [5-60]	[5-60]	Configure PoE output restarting interval, in seconds.
Switch (config-if-POR-T-POR-T)# poe state [disable enable schedule]	[disable enable schedule]	Configure the PoE status of specific port(s). disable: Disable PoE output for specified port(s). enable: Enable PoE output for specified port(s). schedule: Enable or disable PoE output for specified port according to scheduling rule.

Switch(config-if-POR-PORT)# poe schedule [poe-on poe-off]	[poe-on poe-off]	<p>Configure how the port should react to the schedule setting.</p> <p>poe-on: PoE port is delivering PoE power during specified time range.</p> <p>poe-off: PoE port is cutting off PoE power during specified time range.</p> <p>Note: Need to configure the PoE State to “Schedule” to enable this function. Also need to set up PoE Schedule Time-range to complete the schedule setup.</p>
Switch(config-if-POR-PORT)# poe schedule time-range [time_range_name]	[time_range_name]	<p>Specified the pre-defined “Time Range Name” for selected PoE port to follow the scheduling rule. Max. 32 characters.</p> <p>Note: To set up time range rule, please refer to Section 2.6.31 Time-range Command.</p>
No command		
Switch(config-if-POR-PORT)# no poe budget		<p>Reset PoE budget back to the default of 900 in unit of 1/10 watt.</p> <p>Note: This configuration only takes effect when PoE budget mode is in the fixed or force mode.</p>
Switch (config-if-POR-PORT)# no poe inline		Reset the PoE inline mode to auto-bt mode to selected port(s).
Switch(config-if-POR-PORT)# no poe pdname		Remove the powered device name from the selected port(s).
Switch(config-if-POR-PORT)# no poe priority		Reset the power management priority back to the default, which is low priority.
Switch(config-if-POR-PORT)# no poe re-enable interval		Reset re-enabled PoE interval time to 10 seconds.
Switch(config-if-POR-PORT)# no poe state		Reset the PoE state in default parameter, which is enable.
Switch(config-if-POR-PORT)# no poe schedule		Disable PoE schedule function in sepcify PoE port.
Switch(config-if-POR-PORT)# no poe schedule time-range		Delete PoE schedule time range in specify PoE port.

2.6.19 QoS Command

1. Set up QoS

QoS Command	Parameter	Description
Switch(config)# qos [802.1p dscp]	[802.1p dscp]	Specify QoS mode.
Switch(config)# qos dscp-map [0-63] [0-3]	[0-63]	Specify a DSCP bit value.
	[0-3]	Specify a queue value.
Switch(config)# qos management-priority [0-7]	[0-7]	Specify management default 802.1p bit.
Switch(config)# qos queuing-mode [weight strict]	[weight strict]	Specify QoS Queue mode between weight and strict mode.
Switch(config)# qos queue-weighted [1:2:4:8]	[1:2:4:8]	Specify the queue weighted.
Switch(config)# qos remarking dscp		Globally enable DSCP remarking.
Switch(config)# qos remarking dscp-map [1-8]	[1-8]	Specify the DSCP and priority mapping ID.
Switch (config-dscp-map-ID)# active		Enable the mapping entry.
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)# active		Enable the mapping entry.
Switch (config-802.1p-map-ID)# priority [0-7]	[0-7]	Specify the new 802.1p bit value for the selected priority mapping ID.
Switch(config)# qos 802.1p-map [0-7] [0-3]	[0-7]	Specify an 802.1p bit value.
	[0-3]	Specify a queue value.
No command		
Switch(config)# no qos		Disable QoS function.
Switch(config)# no qos dscp-map [0-63]	[0-63]	Reset the specified DSCP bit value back to the default queue value (Q(0)).
Switch(config)# no qos management-priority		Reset management 802.1p bit back to the default (0).
Switch(config)# no qos queuing-mode		Specify QoS queuing mode as strict mode.
Switch(config)# no qos queue-weighted		Reset the queue weighted value back to the default.
Switch(config)# no qos remarking dscp		Globally disable DSCP remarking.
Switch(config)# no qos remarking dscp-map [1-8]	[1-8]	Reset the DSCP remarking for the specified priority mapping ID

		back to the default.
Switch (config-dscp-map-ID)# no active		Disable the mapping entry.
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 active		Disable the mapping entry.
Switch (config-802.1p-map-ID)# no priority		Reset the new 802.1p bit value for the selected priority mapping ID back to the default.
Switch(config)# no qos 802.1p-map [0-7]	[0-7]	Reset the specified 802.1p bit value back to the default queue value (Q(0)).
Show command		
Switch(config)# show qos		Show QoS and user priority configuration.
Switch(config)# show qos interface		Show QoS interface overall information.
Switch(config)# show qos interface [port-list]	[port-list]	Show the specific QoS interface information.
Switch(config)# show qos remarking		Show QoS remarking-mapping information.
Switch (config-dscp-map-ID)# show		Show the DSCP mapping configuration for the selected priority mapping ID.
Switch (config-802.1p-map-ID)# show		Show the 802.1p mapping configuration for the selected priority mapping ID.

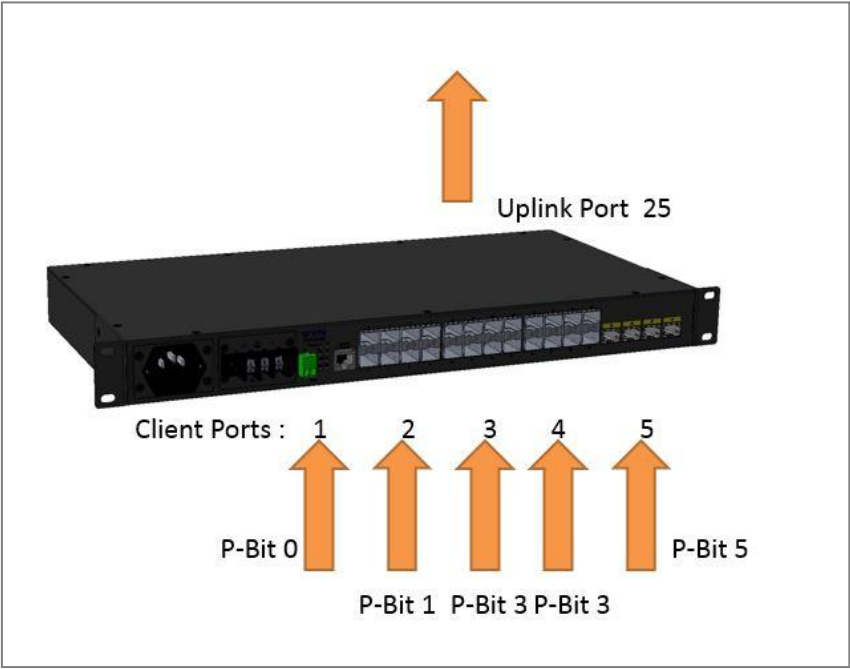
2. Use “interface” command to configure a group of ports’ QoS settings.

QoS & Interface Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# qos rate-limit ingress		Enable QoS ingress rate limit settings.
Switch(config-if-PORT-PORT)# qos rate-limit ingress rate [32-1000000 1-1000] Kbps/Mbps	[32-1000000 1-1000] Kbps/Mbps	Specify the ingress rate limit value. (Valid range is from 32-1000000 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 [32-1000000 1-1000] Kbps/Mbps	[32-1000000 1-1000] Kbps/Mbps	Specify the egress rate limit value. (Valid range is from 32-1000000 in unit of Kbps or 1-1000 in unit of Mbps).
Switch(config-if-PORT-PORT)# qos rate-limit egress unit [Kbps Mbps]	[Kbps Mbps]	Specify the unit of the egress rate limit between Kbps and Mbps.
Switch(config-if-PORT-PORT)# qos user-priority [0-7]	[0-7]	Specify the default priority bit (P-bit) to the selected interfaces.
No command		
Switch(config-if-PORT-PORT)# no qos rate-limit ingress		Disable QoS ingress rate limit settings.
Switch(config-if-PORT-PORT)# no qos rate-limit ingress rate		Reset the ingress rate limit value back to the default.
Switch(config-if-PORT-PORT)# no qos rate-limit ingress unit		Reset the unit of the ingress rate limit back to the default (Kbps).
Switch(config-if-PORT-PORT)# no qos rate-limit egress		Disable QoS egress rate limit settings.
Switch(config-if-PORT-PORT)# no qos rate-limit egress rate		Reset the egress rate limit value back to the default.
Switch(config-if-PORT-PORT)# no qos rate-limit egress unit		Reset the unit of the egress rate limit back to the default (Kbps).
Switch(config-if-PORT-PORT)# no qos user-priority		Reset the user priority value setting back to the default.(0)

For QoS configuration via CLI, we take a 28-port Managed Switch for example to let the users have a clear understanding of these QoS commands.

Under this network environment, the Managed Switch will be configured as Table 2-1. Port 1-5 are client ports and Port 25 is the uplink port of the device. Client ports will receive the data traffic with different VLAN P-bit value. Port 3, Port 4 and Port 5 are also limited to specified bandwidth in the different rate limit in ingress and egress.



QoS Mode: 802.1p; Queue Mode: Weight; Port 25: Uplink Port. Queue-Weighted: 1(Q0):2(Q1):3(Q2):4(Q3):5(Q4):6(Q5):7(Q6):8(Q7)					
802.1p Priority Map	P-Bit	Queue Mapping	Ingress Rate	Egress Rate	Remark
Port 1	0	Q0	Default	Default	The rest of P-Bits are default value.
Port 2	1	Q1	Default	Default	
Port 3	3	Q2	10000	10000	
Port 4	3	Q2	10000	10000	
Port 5	5	Q3	1G	1G	

Table 2-1

Below is the complete CLI commands applied to the Managed Switch.

Command		Purpose
STEP1	configure Example: Switch# config Switch(config)#	Enter the global configuration mode.

STEP2	qos 802.1p Example: Switch(config)# qos 802.1p OK !	In this example, it configures the QoS Mode to 802.1p.
STEP3	qos queuing-mode weight Example: Switch(config)# qos queuing-mode weight OK !	In this example, it configures Queue Mode as "Weight".
STEP4	qos queue-weighted <i>weighted</i> Example: Switch(config)# qos queue-weighted 1:2:3:4:5:6:7:8 OK !	In this example, it configures the Queue Weighted to : 1(Q0):2(Q1):3(Q2):4(Q3): 5(Q4):6(Q5):7(Q6):8(Q7).
STEP5	qos 802.1p-map <i>802.1p_list queue_value</i> Example: Switch(config)# qos 802.1p-map 0 0 Switch(config)# qos 802.1p-map 1 1 Switch(config)# qos 802.1p-map 3 2 Switch(config)# qos 802.1p-map 5 3	In this example, it configures the P-Bit 0 with Queue Mapping to Q0, the P-Bits 1 with Queue Mapping to Q1, the P-Bits 3 with Queue Mapping to Q2, and the P-Bit 5 with Queue Mapping to Q3.
STEP6	interface <i>port_list</i> Example: Switch(config)# interface 1 Switch(config-if-1)#	Specify the Port 1 that you would like to configure P-Bit.
STEP7	qos user-priority <i>P-Bit</i> Example: Switch(config-if-1)# qos user-priority 0	In this example, it configures P-Bit value as 0 for Port 1.
STEP8	exit Example: Switch(config-if-1)# exit Switch(config)#	Return to the global configuration mode.
STEP9	interface <i>port_list</i> Example: Switch(config)# interface 2 Switch(config-if-2)#	Specify the Port 2 that you would like to configure P-Bit.
STEP10	qos user-priority <i>P-Bit</i> Example: Switch(config-if-2)# qos user-priority 1	In this example, it configures P-Bit value as 1 for Port 2.
STEP11	exit Example: Switch(config-if-2)# exit Switch(config)#	Return to the global configuration mode.

STEP12	interface <i>port_list</i> Example: Switch(config)# interface 3, 4 Switch(config-if-3,4)#	Specify the Port 3 and Port 4 that you would like to configure QoS Rate limit.
STEP13	qos rate-limit ingress unit <i>kbps/Mbps</i> Example: Switch(config-if-3,4)# qos rate-limit ingress unit Mbps OK !	In this example, it configures the unit of the ingress rate limit as" Mbps" for Port 3 and Port 4.
STEP14	qos rate-limit ingress rate <i>limit_rate(kbps/Mbps)</i> Example: Switch(config-if-3,4)# qos rate-limit ingress rate 10 OK !	In this example, it configures Port 3 and Port 4 with 10M Ingress Rate.
STEP15	qos rate-limit egress unit <i>kbps/Mbps</i> Example: Switch(config-if-3,4)# qos rate-limit egress unit Mbps OK !	In this example, it configures the unit of the egress rate limit as" Mbps" for Port 3 and Port 4.
STEP16	qos rate-limit egress rate <i>limit_rate(kbps/Mbps)</i> Example: Switch(config-if-3,4)# qos rate-limit egress rate 10 OK !	In this example, it configures Port 3 and Port 4 with 10M Egress Rate.
STEP17	qos user-priority <i>P-Bit</i> Example: Switch(config-if-3,4)# qos user-priority 3	In this example, it configures P-Bit value as 3 for Port 3 and Port 4.
STEP18	exit Example: Switch(config-if-3,4)# exit Switch(config)#	Return to the global configuration mode.
STEP19	interface <i>port_list</i> Example: Switch(config)# interface 5 Switch(config-if-5)#	Specify the Port 5 that you would like to configure QoS Rate limit.
STEP20	qos rate-limit ingress unit <i>kbps/Mbps</i> Example: Switch(config-if-5)# qos rate-limit ingress unit Kbps OK !	In this example, it configures the unit of the ingress rate limit as" Kbps" for Port 5
STEP21	qos rate-limit ingress rate <i>limit_rate(kbps/Mbps)</i> Example: Switch(config-if-5)# qos rate-limit ingress rate 1000000 OK !	In this example, it configures Port 5 with 1G Ingress Rate.

STEP22	qos rate-limit egress unit <i>kbps/Mbps</i> Example: Switch(config-if-5)# qos rate-limit egress unit Kbps OK !	In this example, it configures the unit of the egress rate limit as " Kbps" for Port 5
STEP23	qos rate-limit egress rate <i>limit_rate(kbps/Mbps)</i> Example: Switch(config-if-5)# qos rate-limit egress rate 1000000 OK !	In this example, it configures Port 5 with 1G Egress Rate.
STEP24	qos user-priority <i>P-Bit</i> Example: Switch(config-if-5)# qos user-priority 5	In this example, it configures P-Bit value as 5 for Port 5.
STEP25	exit Example: Switch(config-if-5)# exit Switch(config)#	Return to the global configuration mode.
STEP26	exit Example: Switch(config)# exit Switch#	Return to the Privileged mode.
STEP27	write Example: Switch# write Save Config Succeeded!	Save the running configuration into the startup configuration.

After completing the QoS settings for the Managed Switch, you can issue the commands listed below for checking your configuration

Example 1,

Switch(config)# show qos

```
=====
QoS Information
=====
```

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

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

```
Priority  Queue
-----
```

```
0   Q0
1   Q1
2   Q0
3   Q2
4   Q0
5   Q3
6   Q0
7   Q0
```

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

```
DSCP  Queue  DSCP  Queue  DSCP  Queue  DSCP  Queue
-----
```

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

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

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

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

Port	Priority
-----	-----

1	0
2	1
3	3
4	3
5	5
6	0
7	0
8	0
9	0
10	0

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

11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0

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

21	0
22	0
23	0
24	0
25	0
26	0
27	0
28	0
CPU	0

Switch(config)#

Example 2,

Switch(config)# show qos interface

=====

QoS port Information :

=====

Ingress Rate				Egress Rate		
Port	State	Rate	Unit	State	Rate	Unit
1	disable	500	Kbps	disable	500	Kbps
2	disable	500	Kbps	disable	500	Kbps
3	disable	10	Mbps	disable	10	Mbps
4	disable	10	Mbps	disable	10	Mbps
5	disable	1000000	Kbps	disable	1000000	Kbps
6	disable	500	Kbps	disable	500	Kbps
7	disable	500	Kbps	disable	500	Kbps
8	disable	500	Kbps	disable	500	Kbps

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

9	disable	500	Kbps	disable	500	Kbps
10	disable	500	Kbps	disable	500	Kbps
11	disable	500	Kbps	disable	500	Kbps
12	disable	500	Kbps	disable	500	Kbps
13	disable	500	Kbps	disable	500	Kbps
14	disable	500	Kbps	disable	500	Kbps
15	disable	500	Kbps	disable	500	Kbps
16	disable	500	Kbps	disable	500	Kbps

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

17	disable	500	Kbps	disable	500	Kbps
18	disable	500	Kbps	disable	500	Kbps
19	disable	500	Kbps	disable	500	Kbps
20	disable	500	Kbps	disable	500	Kbps
21	disable	500	Kbps	disable	500	Kbps
22	disable	500	Kbps	disable	500	Kbps
23	disable	500	Kbps	disable	500	Kbps
24	disable	500	Kbps	disable	500	Kbps

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

25	disable	500	Kbps	disable	500	Kbps
26	disable	500	Kbps	disable	500	Kbps
27	disable	500	Kbps	disable	500	Kbps
28	disable	500	Kbps	disable	500	Kbps

Switch(config)#

2.6.20 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 port basis so as to protect network from broadcast storms. Any broadcast packets exceeding the specified value will then be dropped.

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

1. Enable or disable storm control and port isolation.

Security Command	Parameter	Description
Switch(config)# security port-isolation		Globally enable the port isolation function. If port isolation is set to enabled, the ports cannot communicate with each other. Note 1: If the port isolation function is enabled, the Port-based VLAN will be invalid automatically. Note 2: "Port Isolation" function is not "Private VLAN" function.
Switch(config)# security storm-protection		Globally enable the storm control function.
Switch(config)# security storm-protection rates [32-1000000]	[32-1000000]	Specify the Storm rate for storm protection.
No command		
Switch(config)# no security port-isolation		Globally disable port isolation function.
Switch(config)# no security storm-protection		Globally disable the storm control function.
Switch(config)# no security storm-protection rates		Reset the storm rate for storm protection back to the default value of 256 Kbps.
Show command		
Switch(config)# show security port-isolation		Show the current port isolation configuration.
Switch(config)# show security storm-protection		Show the current storm control global configuration.

2. Use "Interface" command to configure port isolation uplink port.

Security & Interface Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For

		example:1,3 or 2-4
Switch(config-if-POR- PORT)# security port-isolation up-link-port		Configure the selected port(s) as uplinks that are allowed to communicate with other ports.
No command		
Switch(config-if-POR- PORT)# no security port- isolation up-link-port		Disable the specified port(s) as non-up- link-port.

2.6.21 Sfp Command

SFP Threshold Configuration function not only displays all SFP ports' current temperature, voltage, current, TX power and RX power information but is capable of detecting whether these SFP ports are at normal status or not.

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

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

SFP Threshold command	Parameter	Description
Switch(config)# sfp threshold		Globally enable the alarm notification of temperature/voltage/current/TX power/RX power for SFP ports of the Managed Swtich.
Switch(config)# sfp threshold notification continuous-alarm		Enable the continuous alarm message sending function for SFP ports' temperature/voltage/current/TX power/RX power.
Switch(config)# sfp threshold notification continuous-alarm interval [60-86400]	[60-86400]	<p>Specify the continuous alarm interval for SFP ports' temperature/voltage/current/TX power/RX power alarm message in seconds.</p> <p>Note:</p> <p>1. For this to work, the continuous alarm meassage sending function has to be enabled.</p> <p>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.</p>
Switch(config)# sfp threshold notification interval [120-86400]	[120-86400]	Specify the time interval of sending SFP ports' temperature/voltage/current/TX power/RX power alarm message in seconds.
No command		
Switch(config)# no sfp threshold		Globally disable the alarm notification of temperature/voltage/current/TX power/RX power for SFP ports of the Managed

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

		parameter.
Switch(config)# show sfp threshold voltage		Show SFP threshold configuration, all SFP ports' current voltage and their threshold information of this parameter.
Switch(config)# show sfp threshold voltage [port_list]	[port_list]	Show SFP threshold configuration, the specific SFP ports' current voltage and their threshold information of this parameter.
Example of SFP Threshold		
Switch(config)# sfp threshold notification interval 300		Configure the time interval of sending SFP ports' temperature/voltage/current/TX power/RX power alarm message as 300 seconds. If their SFP threshold is enabled, the alarm message will be sent in 300 seconds when temperature/voltage/TX power/RX power is higher or lower than the threshold.
Switch(config)# sfp threshold notification continuous-alarm interval 60		<p>Configure the continuous alarm interval for SFP ports' temperature/voltage/current/TX power/RX power alarm message as 60 seconds.</p> <p>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.</p> <p>Please be noted that the function of continuous alarm and SFP threshold must be enabled beforehand for this to work properly.</p>
Switch(config)# show sfp threshold 5-6		Display SFP Port 5~Port 6's current temperature/voltage/current/TX power/RX power and their threshold information of these parameters.

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

SFP Threshold & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# sfp threshold detect		Enable auto detect alarm and warning threshold for the selected port(s). Default value is enabled.
Switch(config-if-PORT-PORT)# sfp threshold current [high low]	[high low]	Enable high/low current threshold for the selected port(s).

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

Switch(config-if-POR-PORT)# sfp 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-POR-PORT)# sfp 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-POR-PORT)# sfp threshold voltage [high low]	[high low]	Enable high/low voltage threshold for the selected port(s).
Switch(config-if-POR-PORT)# sfp 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-POR-PORT)# sfp 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-POR-PORT)# no sfp threshold detect		Disable auto detect alarm and warning threshold for the selected port(s).
Switch(config-if-POR-PORT)# no sfp threshold current [high low]	[high low]	Disable high/low current threshold for the selected port(s).
Switch(config-if-POR-PORT)# no sfp threshold current [high low] value	[high low]	Reset the high/low alarm and warning current threshold values to default.
Switch(config-if-POR-PORT)# no sfp 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-POR-PORT)# no sfp threshold rx-power [high low]	[high low]	Disable high/low RX power threshold for the selected port(s).
Switch(config-if-POR-PORT)# no sfp threshold rx-power [high low] value	[high low]	Reset the high/low alarm and warning RX power threshold values to default.
Switch(config-if-POR-	[high low]	Respectively reset the high/low alarm or

PORT)# no sfp threshold rx-power [high low] value [alarm warning]	[alarm warning]	warning RX power threshold value to default.
Switch(config-if-PORT-PORT)# no sfp threshold temperature [high low]	[high low]	Disable high/low temperature threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no sfp threshold temperature [high low] value	[high low]	Reset the high/low alarm and warning temperature threshold values to default.
Switch(config-if-PORT-PORT)# no sfp threshold temperature [high low] value [alarm warning]	[high low]	Respectively reset the high/low alarm or warning temperature threshold value to default.
	[alarm warning]	
Switch(config-if-PORT-PORT)# no sfp threshold tx-power [high low]	[high low]	Disable high/low TX power threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no sfp threshold tx-power [high low] value	[high low]	Reset the high/low alarm and warning TX power threshold values to default.
Switch(config-if-PORT-PORT)# no sfp threshold tx-power [high low] value [alarm warning]	[high low]	Respectively reset the high/low alarm or warning TX power threshold value to default.
	[alarm warning]	
Switch(config-if-PORT-PORT)# no sfp threshold voltage [high low]	[high low]	Disable high/low voltage threshold for the selected port(s).
Switch(config-if-PORT-PORT)# no sfp threshold voltage [high low] value	[high low]	Reset the high/low alarm and warning voltage threshold values to default.
Switch(config-if-PORT-PORT)# no sfp threshold voltage [high low] value [alarm warning]	[high low]	Respectively reset the high/low alarm or warning voltage threshold value to default.
	[alarm warning]	
Example of SFP Threshold & Interface		
Switch(config-if-1-10)# sfp threshold temperature high		Enable high temperature threshold for Ports 1-10.
Switch(config-if-1-10)# sfp threshold temperature high value 800		Configure both high alarm and warning temperature thresholds as 80 degrees Celsius for Ports 1-10.
Switch(config-if-1-10)# sfp threshold temperature low value warning -100		Configure low warning temperature threshold as -10 degrees Celsius for Ports 1-10.

2.6.22 SNMP-Server Command

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

Snmp-server Command	Parameter	Description
Switch(config)# snmp-server		Enable SNMP Management. To manage the Managed Switch via SNMP.
Switch(config)# snmp-server community [community]	[community]	Create/modify a SNMP community name. Up to 20 alphanumeric characters can be accepted.
Switch(config-community-NAME)# active		Enable the specified SNMP community account.
Switch(config-community-NAME)# description [description]	[description]	Enter the description for the specified SNMP community. Up to 35 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. Disable SNMP Management.
Switch(config)# no snmp-server community [community]	[community]	Delete the specified community.
Switch(config-community-NAME)# no active		Disable the specified SNMP community account.
Switch(config-community-NAME)# no description		Remove the description of SNMP community.
Switch(config-community-NAME)# no level		Reset the access privilege level back to the default. (Read Only)
Show command		
Switch(config)# show snmp-server		Show SNMP server configuration.
Switch(config)# show snmp-server community		Show SNMP server community configuration.
Switch(config)# show snmp-server community [community]		Show the specified SNMP server community's configuration.
Switch(config-community-NAME)# show		Show the selected community's settings.

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

2. Set up a SNMP trap destination.

Trap-destination Command	Parameter	Description
Switch(config)# snmp-server trap-destination [1-3]	[1-3]	Specify the index of SNMP trap destination you would like to modify. Up to 3 sets of SNMP trap destination can be set up.
Switch(config-trap-ID)# active		Enable the specified SNMP trap destination. Up to 20 alphanumeric characters can be accepted.
Switch(config-trap-ID)# community [community]	[community]	Enter the description for the specified SNMP trap destination.
Switch(config-trap-ID)# destination [A.B.C.D A:B:C:D:E:F :G:H]	[A.B.C.D A:B:C:D:E:F :G:H]	Specify SNMP server's IPv4/IPv6 address for the specified SNMP trap destination.
No command		
Switch(config)# no snmp-server trap-destination [1-3]	[1-3]	Reset the specified SNMP trap destination configuration back to the default.
Switch(config-trap-ID)# no active		Disable the specified SNMP trap destination.
Switch(config-trap-ID)# no community		Delete the description for the specified SNMP trap destination.
Switch(config-trap-ID)# no destination		Delete SNMP server's IPv4/IPv6 address for the specified SNMP trap destination.
Show command		
Switch(config)# show snmp-server trap-destination		Show all of SNMP trap destination configurations.
Switch(config)# show snmp-server trap-destination [1-3]	[1-3]	Show the specified SNMP trap destination configuration.
Switch(config-trap-ID)# show		Show the configuration of the selected SNMP trap destination.
Exit command		
Switch(config-trap-ID)# exit		Return to the global configuration mode.
Examples of Trap-destination		
Switch(config)# snmp-server trap-destination 1		Specify the trap destination 1 to configure.
Switch(config-trap-1)# active		Activate the trap destination ID 1.

Switch(config-trap-1)# community mycomm	Add the description "mycomm" to this trap destination.
Switch(config-trap-1)# destination 192.168.1.254	Set SNMP server's IP address as "192.168.1.254" for this trap destination.

3. Set up SNMP trap types that will be sent

Trap-type Command	Parameter	Description
Switch(config)# snmp-server trap-type [all auth-fail auto-backup cold-start console-port-link cpu-load cpu-temperature digital fast-redundancy poe port-link power-down sfp-threshold warm-start]	[all auth-fail auto-backup cold-start console-port-link cpu-load cpu-temperature digital fast-redundancy poe port-link power-down sfp-threshold warm-start]	<p>Specify a trap type that will be sent when a certain situation occurs.</p> <p>all: A trap will be sent when authentication fails, auto-backup succeeds or fails, the cold/warm starts of the Managed Switch, port link is up or down, cpu is overloaded, power failure occurs, console port link is up or down, and so on.</p> <p>auth-fail: A trap will be sent when any unauthorized user attempts to login.</p> <p>auto-backup: A trap will be sent when the auto backup succeeds or fails.</p> <p>cold-start: A trap will be sent when the Managed Switch boots up.</p> <p>console-port-link: A trap will be sent when console port link up/link down occurs.</p> <p>cpu-load: A trap will be sent when the CPU is overloaded.</p> <p>cpu-temperature: A trap will be sent when CPU temperature is over High Temperature Threshold value, CPU temperature returns to the normal status (at or under High Temperature Threshold value), CPU temperature exceeds the range of threshold (0~95 degrees centigrade), or the temperature sensor fails to detect CPU temperature.</p> <p>digital: A trap will be sent when the alarm occurs.</p> <p>fast-redundancy: A trap will be sent when any specified redundancy port in fast redundancy is link up/link down.</p> <p>poe: A trap will be sent when specified PoE events occur, such as system power</p>

		<p>exceeding the threshold or port power exceeding the budget.</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>sfp-threshold: A trap will be sent when Temperature/Voltage/Current/TX Power/RX Power of any SFP ports 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 auto-backup cold-start console-port-link cpu-load cpu-temperature digital fast-redundancy poe port-link power-down sfp-threshold warm-start]	[all auth-fail auto-backup cold-start console-port-link cpu-load cpu-temperature digital fast-redundancy poe port-link power-down sfp-threshold warm-start]	Specify a trap type that will not be sent when a certain situation occurs.
Show command		
Switch(config)# show snmp-server trap-type		Show the current enable/disable status of each type of trap.
Examples of Trap-type		
Switch(config)# snmp-server trap-type all		All types of SNMP traps will be sent.

4. Set up detailed configurations for SNMPv3 USM User

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

Note: The SNMPv3 community user account is generated from "User Command". (See [Section 2.6.27.](#))

Snmp-server Command	Parameter	Description
---------------------	-----------	-------------

Switch(config)# snmp-server password-encryption [aes-128]	[aes-128]	<p>Enable encryption method AES-128 on the SNMPv3 user password.</p> <p>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.</p>
Switch(config)# snmp-server user [user_name]	[user_name]	<p>Modify an existing username generated in CLI of “User Command” for a SNMPv3 user.</p>
Switch (config-v3-user-user_name)# authentication [md5 sha]	[md5 sha]	<p>Specify the authentication method for the specified SNMPv3 user.</p> <p>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.</p> <p>sha(Secure Hash Algorithm): A 160-bit hash function which resembles the said MD5 algorithm.</p>
Switch (config-v3-user-user_name)# authentication password [password]	[password]	<p>Specify the authentication password for the specified SNMPv3 user. The password length must be between 8 and 32 characters, and special characters like ‘ “ % \ are acceptable.</p>
Switch (config-v3-user-user_name)# authentication password aes-128 [base64]	[base64]	<p>Specify the password encrypted by aes-128.</p> <p>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.</p>
Switch (config-v3-user-user_name)# private [des aes128]	[des aes128]	<p>Specify the method to ensure confidentiality of data.</p> <p>des (data encryption standard): An algorithm to encrypt critical information such as message text message signatures...etc.</p> <p>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.</p>
Switch (config-v3-user-user_name)# private password [password]	[password]	<p>Specify the private password for the specified SNMPv3 user. The password length must be between 8 and 32 characters, and special characters like ‘ “ % \ are acceptable.</p>

Switch (config-v3-user-user_name)# private password aes-128 [base64]	[base64]	Specify the password encrypted by aes-128.
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.

2.6.23 Spanning-tree Command

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

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

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

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

Spanning-tree Command	Parameter	Description
Switch(config)# spanning-tree		Globally enable spanning tree protocol function.
Switch(config)# spanning-tree aggregated-port		Enable Spanning Tree Protocol function on aggregated ports.
Switch(config)# spanning-tree aggregated-port cost [0-2000000000]	[0-2000000000]	Specify aggregated ports' path cost.
Switch(config)# spanning-tree aggregated-port priority [0-15]	[0-15]	Specify aggregated ports' priority. 0=0, 1=16, 2=32, 3=48, 4=64, 5=80 6=96, 7=112, 8=128, 9=144, 10=160 11=176, 12=192, 13=208, 14=224, 15=240
Switch(config)# spanning-tree aggregated-port edge		Enable aggregated ports to shift to forwarding state when the link is up. If you know a port is directly connected to an end device (that doesn't support RSTP) then set it as an edge port to ensure maximum performance. This will tell the switch to immediately start forwarding traffic on the port and not bother trying to establish a RSTP connection. Otherwise, turn it off.
Switch(config)# spanning-tree aggregated-port p2p [forced_true forced_false auto]	[forced_true forced_false auto]	Set the aggregated ports to point to point ports (forced_true), non-point to point ports (forced_false) or allow the Managed Switch to detect point to point status automatically (auto). By default, aggregated ports are set to non-point to point ports (forced_false).

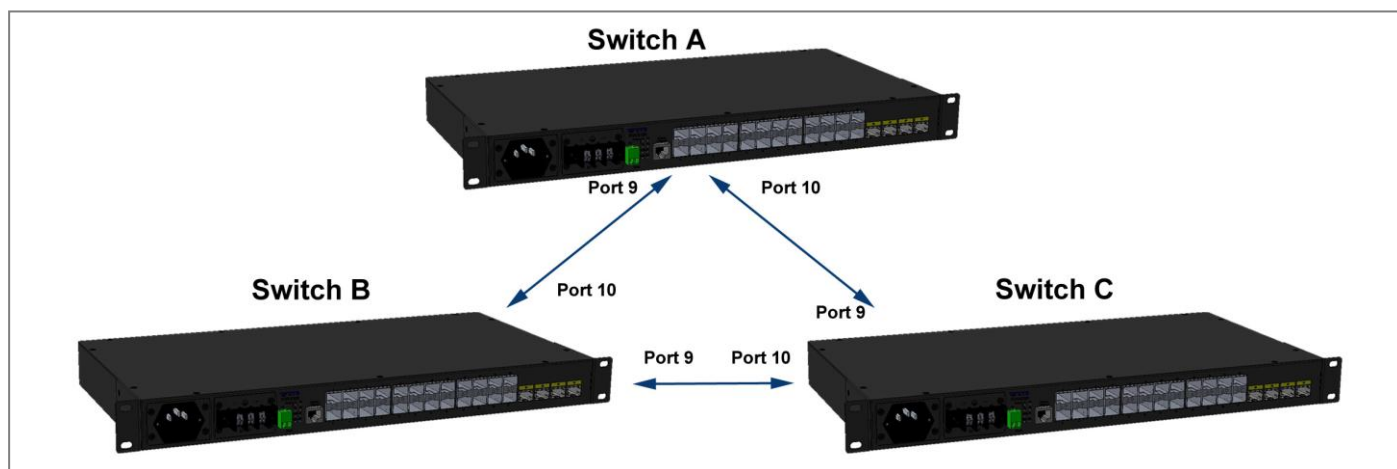
Switch(config)# spanning-tree delay-time [4-30]	[4-30]	Specify the forward delay time value in seconds. The allowable value is between 4 and 30 seconds.
Switch(config)# spanning-tree hello-time [1-10]	[1-10]	Specify the hello interval value in seconds. The allowable value is between 1 and 10 seconds.
Switch(config)# spanning-tree max-age [6-40]	[6-40]	Specify the maximum age time value in seconds. The allowable value is between 6 and 40 seconds.
Switch(config)# spanning-tree priority [0-15]	[0-15]	Specify a priority value on a per switch basis. The allowable value is between 0 and 15. 0=0, 1=4096, 2=8192, 3=12288, 4=16384, 5=20480, 6=24576, 7=28672, 8=32768, 9=36864, 10=40960, 11=45056, 12=49152, 13=53248, 14=57344, 15=61440
Switch(config)# spanning-tree version [compatible normal]	[compatible normal]	Set up RSTP version. “ compatible ” means that the Managed Switch is compatible with STP. “ normal ” means that the Managed Switch uses RSTP.
No command		
Switch(config)# no spanning-tree		Globally disable spanning tree protocol function.
Switch(config)# no spanning-tree aggregated-port		Disable STP on aggregated ports.
Switch(config)# no spanning-tree aggregated-port cost		Reset aggregated ports' cost back to the default.
Switch(config)# no spanning-tree aggregated-port priority		Reset aggregated ports' priority back to the default.
Switch(config)# no spanning-tree aggregated-port edge		Disable aggregated ports' edge ports status.
Switch(config)# no spanning-tree aggregated-port p2p		Reset aggregated ports back to non-point to point ports (forced_ false).
Switch(config)# no spanning-tree delay-time		Reset the Forward Delay time back to the default.
Switch(config)# no spanning-tree hello-time		Reset the Hello Time back to the default.
Switch(config)# no spanning-tree max-age		Reset the Maximum Age back to the default.
Switch(config)# no spanning-tree priority		Reset the priority value on a per switch basis back to the default.
Switch(config)# no spanning-tree version		Reset the RSTP version back to the default.
Show command		
Switch(config)# show spanning-tree		Show RSTP settings on the per switch basis.
Switch(config)# show spanning-tree aggregated-port		Show RSTP settings on aggregated ports.

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

Use “Interface” command to configure a group of ports’ Spanning Tree settings.

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

For RSTP configuration via CLI, we take the following ring network topology composed of 3 sets of 28-port Managed Switches, including Switch A, Switch B and Switch C for example to let the users have a clear understanding of these RSTP commands. Under this network environment, Switch A, Switch B and Switch C will be configured as Table 2-2, and the “Root Switch” will automatically be determined by this network.



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

Table 2-2

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

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

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

After completing the RSTP Switch settings for your Managed Switches, you can issue the commands listed below for checking your configuration

Example 1,

Switch(config)# show spanning-tree

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

Switch(config)#
```

Example 2,

Switch(config)# show spanning-tree aggregated-port

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

Switch(config)#
```

Example 3,

Switch(config)# show spanning-tree interface

=====

RSTP Port Information

=====

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

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

9	enable	0	0	disable	forced-true
10	enable	0	0	disable	forced-true
11	disable	0	128	disable	forced-true
12	disable	0	128	disable	forced-true

: :

: :

: :

27	disable	0	128	disable	forced-true
28	disable	0	128	disable	forced-true

Switch(config)#

Example 4,

Switch(config)# show spanning-tree overview

=====

RSTP overview

=====

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

Switch(config)#

Example 5,

Switch(config)# show spanning-tree status

RSTP Port Status

```
Port          :1
Path Cost     :0
Edge Cost     :no
P2P Cost      :yes
Protocol      :RSTP
Role          :Non-STP
Port State    :Non-STP
```

Packet Statistics

```
RSTP Received      :0
RSTP Transmitted   :0
STP Received       :0
STP Transmitted    :0
TCN Received       :0
TCN Transmitted    :0
Illegal Received   :0
Unknown Received   :0
```

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

: :

: :

: :

```
Port          : 9
Path Cost     : 2000000
Edge Cost     : no
P2P Cost      : yes
Protocol      : RSTP
Role          : Disable
Port State    : Disable
```

Packet Statistics

```
RSTP Received      : 0
RSTP Transmitted   : 0
STP Received       : 0
STP Transmitted    : 0
TCN Received       : 0
TCN Transmitted    : 0
Illegal Received   : 0
Unknown Received   : 0
```

Switch(config)#

Port : 10
Path Cost : 2000000
Edge Cost : no
P2P Cost : yes
Protocol : RSTP
Role : Disable
Port State : Disable

Packet Statistics

RSTP Received :0
RSTP Transmitted :0
STP Received :0
STP Transmitted :0
TCN Received :0
TCN Transmitted :0
Illegal Received :0
Unknown Received :0

: :
: :
: :

Port : lag8
Path Cost : 0
Edge Cost : no
P2P Cost : no
Protocol : RSTP
Role : Non-STP
Port State : Non-STP

Packet Statistics

RSTP Received : 0
RSTP Transmitted : 0
STP Received : 0
STP Transmitted : 0
TCN Received : 0
TCN Transmitted : 0
Illegal Received : 0
Unknown Received : 0

Switch(config)#

2.6.24 Switch Command

Switch Command	Parameter	Description
Switch(config)# switch mtu [1518-9228]	[1518-9228]	Specify the maximum frame size in bytes. The allowable MTU value is between 1518 and 9228 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.
Switch(config)# switch mtu 9000		Set the maximum transmission unit to 9000 bytes.

2.6.25 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 notification		Enable the CPU loading notification.
Switch(config)# switch-info cpu-loading notification threshold [1-99]	[1-99]	Specify CPU loading threshold in percentage for notification.
Switch(config)# switch-info cpu-loading notification restore [1-99]	[1-99]	Specify CPU loading restore threshold in percentage for notification, the value should be lower than the CPU loading threshold.
Switch(config)# switch-info cpu-loading notification observation interval [5-86400]	[5-86400]	Specify a value for Threshold and Restore Observation Interval time in seconds.
Switch(config)# switch-info cpu-temperature notification continuous-alarm		Enable the continuous alarm message sending function for CPU temperature of the system.
Switch(config)# switch-info cpu-temperature notification threshold [0-95]	[0-95]	Specify a value as CPU temperature threshold (Valid Range: 0~95 degrees centigrade).
Switch(config)# switch-info cpu-temperature notification interval [120-86400]	[120-86400]	Specify the time interval of sending cpu-temperature alarm message in seconds.
Switch(config)# switch-info dhcp-vendor-id [dhcp_vendor_id]	[dhcp_vendor_id]	Enter the user-defined DHCP vendor ID, and up to 55 alphanumeric characters can be accepted. Please make sure you have an exact DHCP Vendor ID with the value specified in "vendor-classes" in your dhcpd.conf file. For detailed information, see Appendix B .
Switch(config)# switch-info host-name [host_name]	[host_name]	Enter a new hostname, up to 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 notification		Disable the CPU loading notification.
Switch(config)# no switch-info cpu-loading notification threshold		Reset CPU loading threshold back to the default (95 percentage)
Switch(config)# no switch-info cpu-loading notification restore		Reset CPU loading restore threshold back to the default (80 percentage)
Switch(config)# no switch-info cpu-loading notification observation-interval		Reset the Observation interval back to the default. (60 seconds)
Switch(config)# no switch-info cpu-temperature notification continuous-alarm		Disable the continuous alarm message sending function for CPU temperature of the system.
Switch(config)# no switch-info cpu-temperature notification threshold		Reset CPU temperature threshold back to the default. (80 degrees centigrade)
Switch(config)# no switch-info cpu-temperature notification interval		Reset the time interval of sending cpu-temperature alarm message back to the default. (600 seconds)
Switch(config)# no switch-info dhcp-vendor-id		Reset the entered DHCP vendor ID information back to the default.
Switch(config)# no switch-info host-name		Reset the hostname back to the default.
Switch(config)# no switch-info system-contact		Reset the entered system contact information back to the default.
Switch(config)# no switch-info system-location		Reset the entered system location information back to the default.
Switch(config)# no switch-info system-name		Reset the entered system name information back to the default.
Show command		
Switch(config)# show switch-info		Show the switch-related information including company name, system contact, system location, system name, model name, firmware version and so on.
Switch(config)# show switch-info cpu-loading		Show the current configuration of CPU loading.
Switch(config)# show switch-info cpu-loading statistics		Show the current CPU loading statistics.
Switch(config)# show switch-info cpu-loading statistics average clear		Clear the CPU loading average records.

Switch(config)# show switch-info memory statistics	Show the current memory usage rate of the switch.
Switch(config)# show switch-info cpu-temperature	Show the current cpu-temperature alarm notification configuration and CPU temperature status.
Examples of Switch-info	
Switch(config)# switch-info company-name telecomxyz	Set the company name to “telecomxyz”.
Switch(config)# switch-info system-contact info@company.com	Set the system contact field to “info@compnay.com”.
Switch(config)# switch-info system-location 13thfloor	Set the system location field to “13thfloor”.
Switch(config)# switch-info system-name backbone1	Set the system name field to “backbone1”.
Switch(config)# switch-info host-name edgswitch10	Change the Managed Switch’s hostname into “edgswitch10”.

2.6.26 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.

2.6.27 Terminal Length Command

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

2.6.28 Time-range Command

This command defines a time interval to be activated on a daily or weekly basis. This is convenient to assign when a function should be automatically taken effect. Before using the function, make sure that gateway NTP time server is configured in **Time Server Configuration** (See [Section 2.6.16](#)). The PoE functions scheduled by Time Range will be executed when the system time of the Switch is synchronized with NTP time server.

Command	Parameter	Description
Switch(config)# time-range [time_range_name]	[time_range_name]	<p>Create a new time-range name of the time interval, or enter its Edit mode to modify the settings. Up to 32 alphanumeric characters can be accepted. 10 time-ranges can be set up at most.</p> <p>Time intervals can be classified into three types: Absolute, Periodic and Periodic List.</p> <p>Absolute: An absolute interval to enable a function.</p> <p>Periodic: An interval to enable a function on a weekly basis. The periodic interval only takes effect within the specified absolute interval.</p> <p>Periodic List: An interval to enable a function on a daily basis. The periodic list interval only takes effect within the specified absolute interval.</p> <p>NOTE: Under a time range name, user may add one absolute start time and one absolute end time at most. Users may also add two optional time ranges at most using Periodic and Periodic List time range.</p> <p>For example, users may set:</p> <ol style="list-style-type: none">1. Two Periodics in time range, or2. One Periodic and one Periodic List in time range, or3. Two Periodic Lists in time range.
Switch(config-timerange-name)# absolute start [hh:mm dd MMM yyyy]	[hh:mm dd MMM yyyy]	<p>Specify an absolute start time to a time-range, using the following format:</p> <p>hh:mm dd MMM yyyy</p> <p>hh: 0-23; mm: 0-59; dd: 1-31; yyyy: 2000-2097;</p> <p>MMM: jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec</p>

		Example: 8:00 10 jan 2015
Switch(config-timerange-name)# absolute end [hh:mm dd MMM yyyy]	[hh:mm dd MMM yyyy]	Specify an absolute end time to a time- range, using the following format: hh:mm dd MMM yyyy hh: 0-23; mm: 0-59; dd: 1-31; yyyy: 2000-2097; MMM: jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec Example: 8:00 10 jan 2015
Switch(config-timerange-name)# periodic [hh:mm day] to [hh:mm day]	[hh:mm day] to [hh:mm day]	Set up a periodic time range, using the following format: hh:mm day to hh:mm day hh: 0-23, mm:0-59 day: sun, mon, tue, wed, thu, fri, sat Example: 10:00 mon to 20:00 wed NOTE: Maximum 2 periodic time range rules can be assigned per time-range-name.
Switch (config-timerange- NAME)# periodic list [hh:mm] to [hh:mm day]	[hh:mm to hh:mm day]	Set up a periodic time range to repeat on several days per week, using the following format: [hh:mm to hh:mm day] hh: 0-23, mm: 0-59 day: sun, mon, tue, wed, thu, fri, sat ex.20:00 to 4:00 sun tue sat NOTE: Maximum 2 periodic list time range rules can be assigned per time-range-name.
No Command		
Switch(config)# no time-range [time_range_name]	[time_range_n ame]	Remove a specified time-range name.
Switch (config-timerange- NAME)# no absolute start [hh:mm dd MMM yyyy]	[hh:mm dd MMM yyyy]	Remove the absolute start time configuration from the specified time- range name.
Switch (config-timerange- NAME)# no absolute end [hh:mm dd MMM yyyy]	[hh:mm dd MMM yyyy]	Remove the absolute end time configuration from the specified time- range name.
Switch (config-timerange- NAME)# no periodic [hh:mm day to hh:mm day]	[hh:mm day to hh:mm day]	Delete the periodic rules that is setup in the selected time range name.
Switch (config-timerange- NAME)# no periodic list [hh:mm	[hh:mm to hh:mm day]	Delete the periodic list rules that is setup in the selected time range name.

to hh:mm day]		
Show Command		
Switch# show time-range	Display the time-range configuration.	
Switch# show time-range [time-range-name]	Display the specified time-range configuration.	
Switch(config)# show time-range	Display the time-range configuration.	
Switch(config)# show time-range [time-range-name]	Display the specified time-range configuration.	
Switch (config-timerange-name)# show	Display the configuration of the current time range entry.	
Examples of Time-range command		
Switch(config)# time-range name	Create a new time-range "name".	
Switch(config-timerange-name)# absolute start 8:00 10 jan 2015	Set effective time range start from 8:00, January 10th, 2015.	
Switch(config-timerange-name)# absolute end 18:00 10 dec 2015	Set an effective time range that stops at 18:00, December 10th, 2015.	
Switch(config-timerange-name)# periodic 10:00 mon to 20:00 wed	Set an effective time range that start from 10:00, Monday to 20:00 Wednesday.	
Switch(config-timerange-name)# no periodic 10:00 mon to 20:00 wed	Delete the periodic rule.	
Switch(config-timerange-name)# periodic list 09:00 to 18:00 mon tue wed thu fri	Set an effective time range that start from 09:00 to 18:00 every weekday.	
Switch(config-timerange-name)# no periodic list 09:00 to 18:00 mon tue wed thu fri	Delete the periodic list rule.	
Switch(config-timerange-name)# periodic list 20:00 to 04:00 tue wed thu fri sat	Set an effective time range that start from 20:00, Tuesday to 04:00 Saturday.	
Switch(config-timerange-name)# no periodic list 20:00 to 04:00 tue wed thu fri sat	Delete the periodic list rule.	
Switch(config-timerange-name)# periodic list 08:00 to 10:00 wed thu	Set an effective time range that start from 08:00 to 10:00 every Wednesday and Thursday.	
Switch (config-timerange-name)# show	Display the configuration of the current time range entry.	

2.6.29 User Command

Create a new login account.

User command	Parameter	Description
Switch(config)# user name [user_name]	[user_name]	Enter the new account's username. The authorized user login name is up to 32 alphanumeric characters. Only 10 login accounts can be registered in this device.
Switch(config)# user password-encryption aes-128		Select AES-128 (Advanced Encryption Standard) as the password encryption method. NOTE: 1. The acquired password from backup config file is not applicable for user login on CLI/Web interface. 2. We strongly recommend not to alter off-line Auth Method setting in backup configure file. 3. If Auth-Method is enabled and do firmware downgrade, users must reset default config.
Switch(config-user-USERNAME)# active		Activate this user account.
Switch(config-user-USERNAME)# description [description]	[description]	Enter the brief description for this user account, up to 35 alphanumeric characters are acceptable.
Switch(config-user-USERNAME)# level [admin rw ro]	[admin rw ro]	Specify user account level. By default, when you create a community, the access privilege for this account is set to "read only". Admin: Full access right, including maintaining user account, system information, loading factory settings, etc. rw: Read & Write access privilege. Partial access right, unable to modify system information, user account, load factory settings and upgrade firmware. Ro: Read Only access privilege.
Switch(config-user-USERNAME)# password [password]	[password]	Enter the password for this user account up to 32 alphanumeric characters.
Switch (config-user-USERNAME)# password aes-128 [base64]	[base64]	Specify the password encrypted by aes-128.
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".

2.6.30 VLAN Command

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

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

2.6.30.1 Port-Based VLAN

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

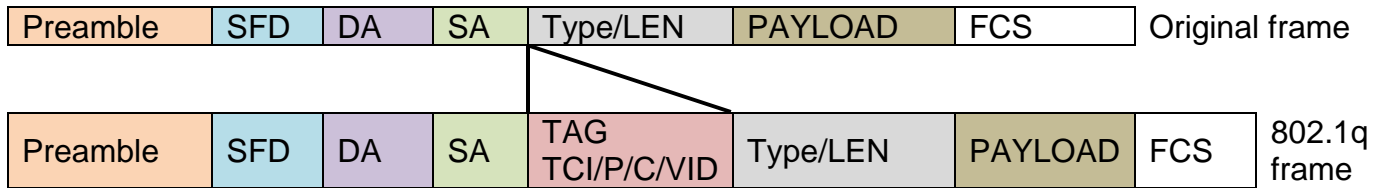
Since source addresses of the packets are listed in MAC address table of specific VLAN (except broadcast/multicast packets), in every VLAN the traffic between two ports will be two-way without restrictions.

2.6.30.2 802.1Q 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 :

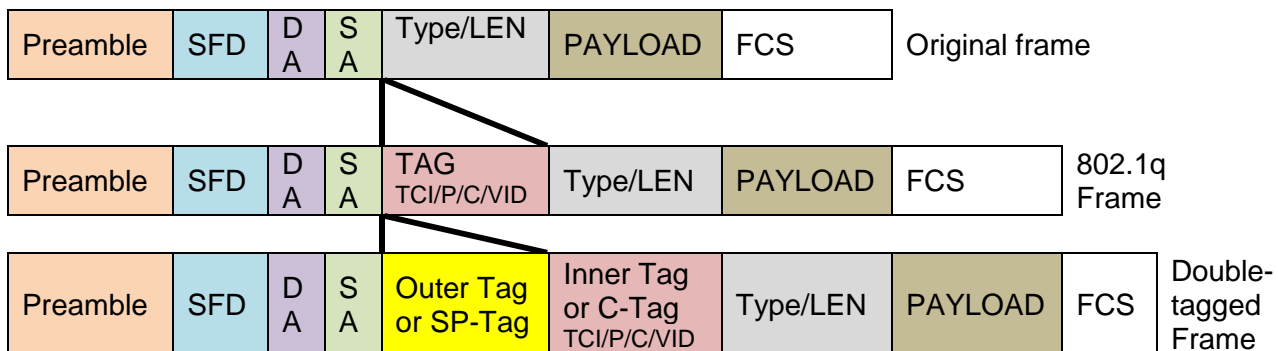
A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.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

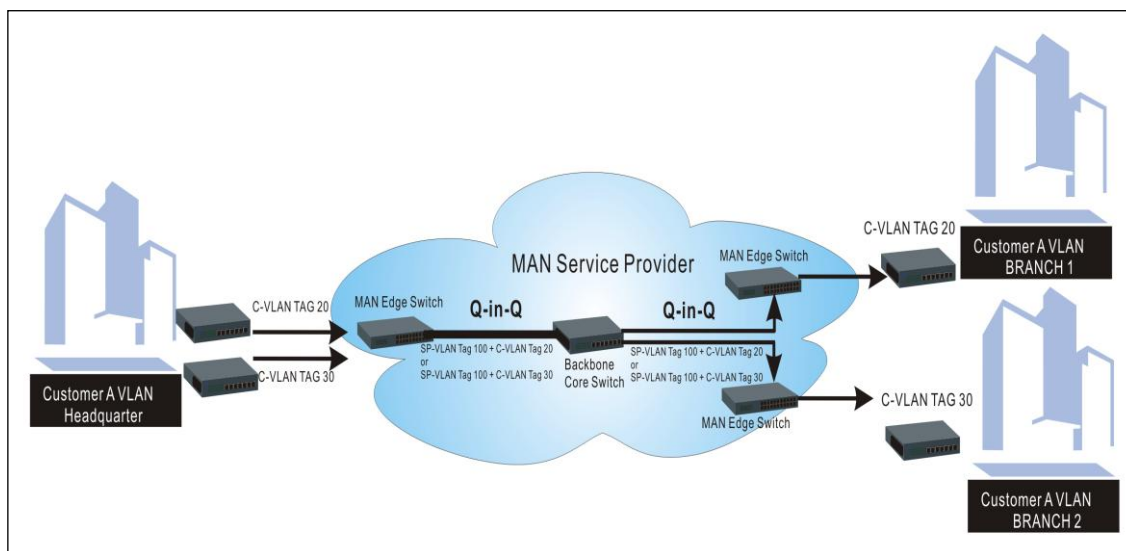
2.6.30.3 Introduction to Q-in-Q (ISP Mode)

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]	[name]	Specify a name for the created VLAN ID, maximum 15 characters.
Switch(config)# vlan port-based [name] rename [new_name]	[new_name]	Specify a new name for the created VLAN ID, maximum 15 characters.
Switch(config)# vlan 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 management-stag-vid [1-4094]	[1-4094]	Specify the service tag VID. Valid values are 1 through 4094.
Switch(config)# vlan isp-mode stag-ethertype [0xWXYZ]	[0xWXYZ]	Specify the service tag's ethertype. (Range: 0000~FFFF)
No command		
Switch(config)# no vlan dot1q-vlan		Disable 802.1q VLAN mode globally.
Switch(config)# no vlan dot1q-vlan [1-4094]	[1-4094]	Remove the specific VLAN ID from the IEEE 802.1q Tag VLAN table.
Switch(config)# no vlan port-based		Disable port based VLAN mode globally.
Switch(config)# no vlan port-based [name]	[name]	Delete the specified port based VLAN by its name.
Switch(config)# no vlan port-based [name] include-cpu	[name]	Exclude CPU from the specified any existing port based VLAN.
Switch(config)# no vlan isp-mode		Disable ISP mode (IEEE 802.1Q double tagging VLAN) globally.
Switch(config)# no vlan isp-mode management-stag-vid		Reset the service tag VID back to the default.
Switch(config)# no vlan isp-mode stag-ethertype		Reset the service tag's ethertype to the default.
Show command		
Switch(config)# show vlan		Show VLAN table.
Switch(config)# show vlan interface		Show all ports' VLAN assignment and VLAN mode.
Switch(config)# show vlan interface [port_list]	[port_list]	Show the selected ports' VLAN assignment and VLAN mode.
Switch(config)# show vlan port-based		Show port-based VLAN table.
Switch(config)# show vlan isp-mode		Show ISP mode (IEEE 802.1Q double tagging VLAN) configuration.
Example of VLAN dot1q & interface		
Switch(config)# vlan dot1q-vlan 100		Create a new VLAN 100.
Switch(config)# vlan port-based MKT_Office		Create a port-based VLAN "MKT_Office".
Switch(config)# vlan management-vlan 1 management-port 1-3 mode access		Set VLAN 1 to management VLAN (untagged) and Port 1~3 as management ports.

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

VLAN & Interface command

Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if-PORT-PORT)# vlan dot1q-vlan pvid [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode access		Set the selected ports to the access mode (untagged).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk		Set the selected ports to the trunk mode (tagged).
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk native		Enable native VLAN for untagged traffic on the selected ports. (Tagged and untagged) Note: When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.
Switch(config-if-PORT-PORT)# vlan isp-mode isp-port		Specify the selected ports to be the ISP ports (IEEE 802.1Q double tagging port).
Switch(config-if-PORT-PORT)# vlan isp-mode stag-vid [1-4094]	[1-4094]	Specify the stag vid for selected 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).
Switch(config-if-PORT-PORT)# no vlan isp-mode stag-vid		Reset the service tag VID for selected port back to default.
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

2. 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.

3. 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.

2.6.31 Interface Command

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

1. Entering interface numbers.

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

Note: You need to enter interface numbers first before issuing below 2-13 commands.

2. Enable port auto-negotiation.

Command	Parameter	Description
Switch(config-if-PORTR-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-PORTR-PORT)# no auto-negotiation		Reset auto-negotiation setting back to the default. (Manual)

3. Set up port description.

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

4. Set up port duplex mode.

Command	Parameter	Description
Switch(config-if-PORTR-PORT)# duplex [full half]	[full half]	Configure the port duplex as full or half . Note1: Copper 1000M and fiber ports cannot be configured as half duplex.
No command		
Switch(config-if-PORTR-PORT)# no duplex		Reset the port duplex to default value. Note1: Copper 1000M and fiber ports cannot be configured as half duplex.

5. Enable flow control operation.

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

6. Shutdown interface.

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

7. Set up port speed.

Command	Parameter	Description
Switch(config-if-PORTR-PORT)# speed [1000 100 10]	[1000 100 10]	Configure the port speed. Note 1: Speed can only be configured when auto-negotiation is disabled. Note 2: The specified speed can only be configured when it's supported on the selected interface.
No command		
Switch(config-if-PORTR-PORT)# no speed		Reset the port speed setting back to the default.

2.6.32 Show interface status Command

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

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

2.6.33 Show interface statistics Command

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

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

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

2.6.34 Show sfp Command

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

Show command	Parameters	Description
Switch(config)# show sfp information		Show the speed, distance, vendor name, vendor PN and vendor SN of SFP.
Switch(config)# show sfp state		Show the temperature, voltage, TX Bias, TX port and RX power of SFP.
Switch(config)# show sfp threshold		Show SFP threshold configuration, all SFP ports' current temperature/voltage/current(mA) /TX power/RX power and their threshold information of these parameters.
Switch(config)# show sfp threshold [port_list]	[port_list]	Show SFP threshold configuration, the specific SFP ports' current temperature/voltage/current(mA)/TX power/RX power and their threshold information of these parameters.
Switch(config)# show sfp threshold current		Show SFP threshold configuration, all SFP ports' current(mA) and their threshold information of this parameter.
Switch(config)# show sfp threshold current [port_list]	[port_list]	Show SFP threshold configuration, the specific SFP ports' current(mA) and their threshold information of this parameter.
Switch(config)# show sfp threshold rx-power		Show SFP threshold configuration, all SFP ports' current RX power and their threshold information of this parameter.
Switch(config)# show sfp threshold rx-power [port_list]	[port_list]	Show SFP threshold configuration, the specific SFP ports' current RX power and their threshold information of this parameter.
Switch(config)# show sfp threshold temperature		Show SFP threshold configuration, all SFP ports' current temperature and their threshold information of this parameter.
Switch(config)# show sfp threshold temperature [port_list]	[port_list]	Show SFP threshold configuration, the specific SFP ports' current temperature and their threshold information of this parameter.
Switch(config)# show sfp threshold tx-power		Show SFP threshold configuration, all SFP ports' current TX power and their threshold information of this parameter.
Switch(config)# show sfp threshold tx-power [port_list]	[port_list]	Show SFP threshold configuration, the specific SFP ports' current TX power and their threshold information of this parameter.
Switch(config)# show sfp threshold voltage		Show SFP threshold configuration, all SFP ports' current voltage and their threshold information of this parameter.
Switch(config)# show sfp threshold voltage [port_list]	[port_list]	Show SFP threshold configuration, the specific SFP ports' current voltage and their threshold information of this parameter.

2.6.35 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 Managed 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 Managed Switch for the specific port(s).
Switch(config)# show running-config interface [port_list] include [string]		Specify the keyword to search for the matched information from the running configuration of the specific port(s).
Switch(config)# show start-up-config		Show the difference between the startup configuration and the default configuration.
Switch(config)# show start-up-config include [string]	[string]	Specify the keyword to search for the matched information from the difference between the startup configuration and the default configuration.
Switch(config)# show start-up-config full		Display the system configuration stored in Flash.
Switch(config)# show start-up-config full include [string]	[string]	Specify the keyword to search for the matched information from the full startup configuration.
Switch(config)# show default-config		Display the system factory default configuration.
Switch(config)# show default-config include [string]	[string]	Specify the keyword to search for the matched information from the system factory default configuration.

2.6.36 Show log Command

Show Log Command	Parameters	Description
Switch(config)# show log		Display the entire event log currently stored in the Managed Switch, by each time showing 10 events from the newest to the oldest.
Switch(config)# show log clear		Remove the entire event log currently stored in the Managed Switch.
Switch#(config) show log index [ID range]	[1-500]	Display a certain part of the event log from a specified index to another according to the specified ID range, by each time showing 10 events from the newest to the oldest. ID range: Enter a range of event indexes with a hyphen. For example: 2-4 or 4-500
Switch#(config) show log terminal-length [1-500]	[1-500]	Display the entire event log, by each time showing a specified number of events from the newest to the oldest.
Switch#(config) show log reverse		Display the entire event log, by each time showing 10 events from the oldest to the newest.
Switch#(config) show log log-item [exclude include] [item_list]	[exclude include]	Display events by filtering out or encompassing events of the specified category.
	[1-53]	Specify the event category from the item list for log filtering. item_list: Enter several discontinuous numbers separated by commas or a range of items with a hyphen. For example: 1,3 or 2-4 Note: Use quick key: a “space” followed by “?” to view the comprehensive item list.
Switch#(config) show log log-item [exclude include] [item_list] time-range [exclude include] [ntp-time] start [hh:mm dd MMM yyyy] end [hh:mm dd MMM yyyy]	[exclude include]	Display events by filtering out or encompassing events of the specified category.
	[1-53]	Specify the event category from the item list for log filtering.
	[exclude include]	Display events that occurred (didn't occur) during a specified NTP time period.
	[ntp-time]	Filter the events according to NTP time.
	[hh:mm dd MMM yyyy]	Specify the starting point of an NTP time period. hh: 0-23

		mm: 0-59 dd: 1-31 MMM: jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec yyyy: 2021-2037
	[hh:mm dd MMM yyyy]	Specify the ending point of an NTP time period. hh: 0-23 mm: 0-59 dd: 1-31 MMM: jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec yyyy: 2021-2037
Switch#(config) show log log-item [exclude include] [item_list] time-range [exclude include] [up-time] start [hh:mm dddd] end [hh:mm dddd]	[exclude include]	Display events by filtering out or encompassing events of the specified category.
	[1-53]	Specify the event category from the item list for log filtering.
	[exclude include]	Display events that occurred (didn't occur) during a specified uptime period.
	[up-time]	Filter the events according to the Managed Switch's uptime.
	[hh:mm dddd]	Specify the starting point of a Managed Switch's uptime period. hh: 0-23 mm: 0-59 dddd: 0-9999
	[hh:mm dddd]	Specify the ending point of a Managed Switch's uptime period. hh: 0-23 mm: 0-59 dddd: 0-9999

3. SNMP NETWORK MANAGEMENT

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

SNMP consists of the following key components.

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

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

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

SNMP Manager/NMS executes applications that monitor and control managed devices. NMS provide the bulk of the processing and memory resources required for the complete network management. SNMP Manager is often composed by desktop computer/work station and software program such like HP OpenView.

Totally 4 types of operations are used between SNMP Agent & Manager to change the MIB information. These 4 operations all use the UDP/IP protocol to exchange packets.

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

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

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

Trap: Trap is used by the managed device to report asynchronously a specified event to the SNMP Manager. When certain types of events occur, a managed device will send a trap to alert the SNMP Manager.

The system built-in management module also supports SNMP management. Users must install the MIB file before using the SNMP based network management system. The MIB file is on a disc or diskette that accompanies the system. The file name extension is .mib, which SNMP based compiler can read.

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

4. WEB MANAGEMENT

You can manage the Managed Switch via a web browser. However, you must first assign a unique IP address to the Managed Switch before doing so. Through the connection of any SFP ports using the fiber cable or any TP ports using a RJ-45 cable, you will be allowed to have an access of the Managed Switch and set up the IP address for the first time. (Note: The Managed Switch can be reached with the default IP address of “**192.168.0.1**”. You can change the IP address of the switch to the desired one later in its **Network Management** menu.)

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







After you login successfully, the screen with the Main Menu will show up. The functions of Main Menu in the Web Management are similar to those described at the Console Management.

On the top side, it shows the front panel of Managed Switch. On this front panel image, the corresponding link-up ports will be displayed in green color; as to the link-down ports, they will be dark. Red color will be displayed on the corresponding ports while these ports' port state is disabled.

Additionally, there are clicking functions on this front panel image. When clicking on any port of this panel image, you will directly jump to the **Port Setup &Status** webpage.

In this **Port Setup &Status** webpage, it shows the basic information and configuration of each port. For more details about this, please refer to [Section 4.2.1 “Port Setup & Status”](#).

Besides the Main Menu, a general overview of the Managed Switch's all functions will also be displayed when clicking on the  **Content** icon among the quick buttons located on the top-right corner of each webpage. You can also reach each functions from the listed hyperlink.

As for other quick buttons, the  **Save** icon is provided for the user to save any new settings permanently into Flash, the  **Reboot** icon is used to restart the switch, and the  **Logout** icon is used to log out the management interface.

In the Main Menu, there are 15 main functions in the SRS-3106-4BT (PoE Switch), and 14 in the SRS-3106 (Switch).

System Setup	▼
Port Management	▼
Link Aggregation	▼
VLAN Setup	▼
Rapid Spanning Tree	▼
Fast Redundancy	▼
MAC Address Management	▼
QoS Setup	▼
Multicast	▼
Security Setup	▼
LLDP	▼
Power over Ethernet	▼
Maintenance	▼
Management	▼
Logout	

- **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.
- **Link Aggregation:** Configure static port trunking and distribution rules, including MAC and IP address-based options.

- **VLAN Setup:** Set up VLAN mode as well as VLAN configuration, and view the IEEE802.1q VLAN Table of the Managed Switch.
- **Rapid Spanning Tree:** Set up RSTP switch settings, aggregated port settings, physical port settings, etc. And view RSTP VLAN Bridge, port status, and statistics.
- **Fast Redundancy:** Set up CTS's fast redundancy functionality, including two redundancy protocols Fast Ring v2 and Chain.
- **MAC Address Management:** Set up MAC address, enable or disable MAC security, etc.
- **QoS Setup:** Set up the priority queuing, remarking, rate limit, and so on.
- **Multicast:** Configure IGMP/MLD Snooping, static multicast, and view the IGMP/MLD status and Groups table.
- **Security Setup:** Set up DHCP Snooping, 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.
- **Power over Ethernet:** Configure PoE settings and view PoE status. **(Available on SRS-3106-4BT)**
- **Maintenance:** View the operation status and event logs of the system, ping, etc.
- **Management:** Enable or disable the specified network services, view the RS-232 serial port setting, user account management, do the firmware upgrade, load the factory default settings, etc..
- **Logout:** Log out the management interface.

4.1 System Setup

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

System Setup » Switch Information

Company Name	The Company				
System Object ID	.1.3.6.1.4.1.9304.100.31069				
System Contact	contact@company.com				
System Name	Managed 6 Ports 1000M Switch				
System Location					
DHCPv4/DHCPv6 Vendor ID	Switch				
Model Name	Switch				
Host Name	Switch				
Current Boot Image	Image-1				
Configured Boot Image	Image-1				
Image-1 Version	0.99.08				
Image-2 Version	0.99.07				
M/B Version	A02				
Serial Number	ABBCDDEF7766888	Date Code	20250325		
Up Time	0 day 01:05:35	Local Time	Not Available		
CPU Temperature	35.0 °C	View Details			
PowerA	Installed	Type	DC	State	Active
PowerB	N/A	Type	N/A	State	N/A

[Ok](#) [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.
6. **Time Range:** Set up the time interval of PSE's power supply over Ethernet to PDs (powered devices).

4.1.1 Switch Information

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

Company Name	<input type="text" value="The Company"/>				
System Object ID	<input type="text" value=".1.3.6.1.4.1.9304.100.31069"/>				
System Contact	<input type="text" value="contact@company.com"/>				
System Name	<input type="text" value="Managed 6 Ports 1000M Switch"/>				
System Location	<input type="text"/>				
DHCPv4/DHCPv6 Vendor ID	<input type="text" value="Switch"/>				
Model Name	<input type="text" value="Switch"/>				
Host Name	<input type="text" value="Switch"/>				
Current Boot Image	Image-1				
Configured Boot Image	Image-1				
Image-1 Version	0.99.08				
Image-2 Version	0.99.07				
M/B Version	A02				
Serial Number	ABBCDDEF7766888	Date Code	20250325		
Up Time	0 day 01:05:35	Local Time	Not Available		
CPU Temperature	35.0 °C	<button>View Details</button>			
PowerA	Installed	Type	DC	State	Active
PowerB	N/A	Type	N/A	State	N/A
<div><button>Ok</button><button>Reset</button></div>					

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

System Object ID: Display the predefined System OID.

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

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

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

DHCPv4/DHCPv6 Vendor ID: Vendor Class Identifier that is used for DHCP/DHCPv6 relay agent function. Enter the user-defined DHCP vendor ID, and up to 55 alphanumeric characters can be accepted. Please make sure you have an exact DHCP Vendor ID with the value specified in “vendor-classes” in your dhcpd.conf file. For detailed information, see [Appendix B](#).

Model Name: Display the product’s model name.

Host Name: Enter the product’s host name.

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

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

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

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

M/B Version: Display the main board version.

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

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

Up Time: Display the up time since last restarting.

Local Time: Display the local time of the system.

CPU Temperature: Display the current CPU temperature of this device. In case CPU temperature is shown in red color, it stands that CPU temperature currently detected is higher than the **High Temperature Threshold** value you configure. For more details on this or do the further alarm notification settings for CPU temperature of the system, click **View Details** to directly jump to the **CPU Temperature Status** webpage under **Maintenance** folder from the **Main Menu**.

PowerA: Display the information about PowerA, including type and state.

PowerB: Display the information about PowerB, including type and state.

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 a web interface for 'System Setup' with a sub-menu 'IP Setup'. The page title is 'IPv4'. At the top right, there are buttons for 'Content', 'Save', 'Reboot', and 'Logout'. The main configuration area includes:

- Enable IPv4:** A dropdown menu set to 'Enabled'.
- MAC Address:** A read-only field showing '00:06:19:00:00:00'.
- Configuration Type:** A dropdown menu set to 'Manual'.
- IPv4 Address:** A text input field containing '192.168.0.6'.
- Subnet Mask:** A text input field containing '255.255.255.0'.
- Gateway:** A text input field containing '0.0.0.0'.
- DHCP Recycle:** A blue button labeled 'Recycle'.
- DHCP Auto Recycle:** A dropdown menu set to 'Enabled'.
- DHCP Auto Recycle Port:** A checkbox labeled 'Select All'.

At the bottom, there is a row of six checkboxes, each with a checkmark and a number from 1 to 6.

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.

NOTE: Need to choose “DHCP” as the Configuration Type before running the follow-up functions.

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

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

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

Just click on the checkbox of the corresponding port number to select the port(s) as IPv4 DHCP auto recycle port. Besides, you can choose all ports at a time by clicking on the checkbox in front of **Select All** as well.

IPv6

Enable IPv6

Disabled ▾

Auto-configuration

Enabled ▾

Current State

IPv6 Link-local Address/Prefix Length

fe80::206:19ff:fe00:0/64

::/0

IPv6 Global Address/Prefix Length

::/64

IPv6 Gateway

::

DHCPv6

Enable force mode ▾

Rapid Commit

☒

DHCPv6 Unique Identifier (DUID)

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.

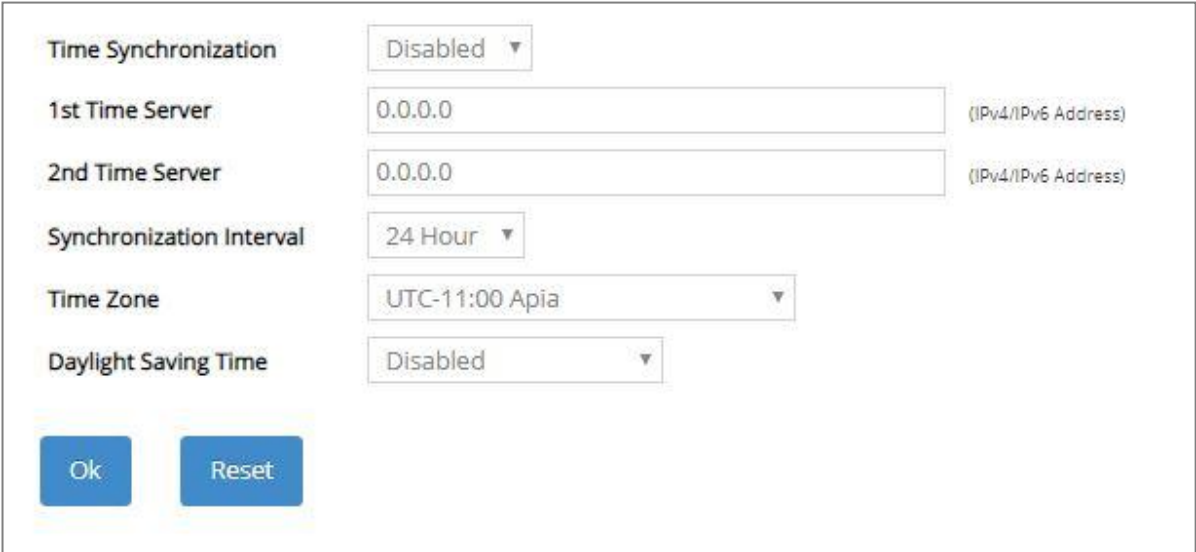
State: Disable or enable the assigned IP address to reach the management.

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.



The screenshot shows a configuration window for Time Server Setup. It includes the following fields and controls:

- Time Synchronization:** A dropdown menu set to "Disabled".
- 1st Time Server:** A text input field containing "0.0.0.0" with a placeholder "(IPv4/IPv6 Address)".
- 2nd Time Server:** A text input field containing "0.0.0.0" with a placeholder "(IPv4/IPv6 Address)".
- Synchronization Interval:** A dropdown menu set to "24 Hour".
- Time Zone:** A dropdown menu set to "UTC-11:00 Apia".
- Daylight Saving Time:** A dropdown menu set to "Disabled".
- Buttons:** "Ok" and "Reset" buttons at the bottom left.

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 'Syslog Configuration' window. It is titled 'Log Server' and 'Logging Type'. The 'Log Server' section includes a dropdown for 'Log Server' (set to 'Disabled'), a text field for 'SNTP Status' (set to 'Disabled'), a dropdown for 'Facility' (set to 'Local 0'), and three text fields for '1st Log Server', '2nd Log Server', and '3rd Log Server', all set to '0.0.0.0'. The 'Logging Type' section includes a dropdown for 'Terminal History' (set to 'Disabled'). At the bottom are 'Ok' and 'Reset' buttons.

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

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

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

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

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

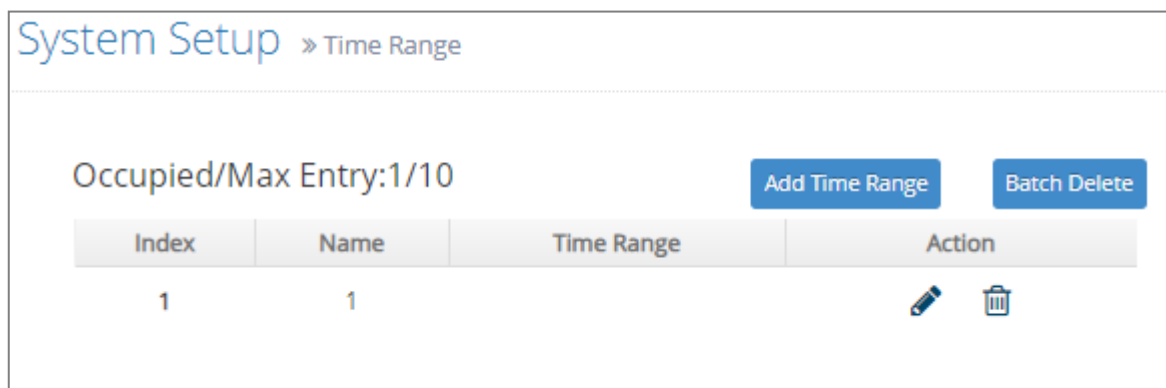
2nd Log Server: Specify the secondary log server's IPv4/IPv6 address. When the first log server is down, the Managed Switch will automatically contact the second or third Log server.

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

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

4.1.6 Time Range



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



System Setup » Time Range

Occupied/Max Entry: 1/10

Add Time Range Batch Delete

Index	Name	Time Range	Action
1	1		 

This table displays the overview of each configured time range. Up to 10 entries can be set up.

Occupied/Max Entry: View-only field.


Occupied: This shows the amount of total Time Ranges that have already been created.


Max: This shows the maximum number of Time Ranges that can be created. The maximum number is 10.

Index: The identification number for each Time Range entry.

Name: Display the name of the specific Time Range.

Time Range: Display the time intervals you set up for the specific Time Range.

Click the  icon to edit and then the following screen page appears for the further time interval settings.

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

Click **Add Time Range** to add a new time range entry and then the following screen page appears for the further Time Range settings.

System Setup » Time Range

Occupied/Max Entry:0/10 Add Time Range Batch Delete

Index	Name	Time Range	Action
-------	------	------------	--------

Add Time Range Entry

Name

Absolute Start ☐ 00 : 00 Day 1 Month JAN Year 2000

Absolute End ☐ 00 : 00 Day 1 Month JAN Year 2000

Periodic - 1 ☐ 00 : 00 Day Sun to 00 : 00 Day Sun

Periodic - 2 ☐ 00 : 00 Day Sun to 00 : 00 Day Sun

Periodic List - 1 ☐ 00 : 00 to 00 : 00 ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Periodic List - 2 ☐ 00 : 00 to 00 : 00 ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Ok Cancel

Name: Specify a name for the Time Range Entry. Up to 32 alphanumeric characters can be accepted.

Absolute Start: Specify an absolute start time for a time interval for a PoE function.

Absolute End: Specify an absolute end time for a time interval for a PoE function.

Periodic: Specify a time interval for a PoE function on a weekly basis.

Periodic List: Specify a time interval for a PoE function on a daily basis.

NOTE:

1. Click the checkbox first to enable the dropdown menu on its right side, so that you can configure it.
 2. Users are only allowed to choose up to two options from Periodic-1, Periodic-2, Periodic List-1 and Periodic List-2 simultaneously under a time range entry.
-

Click **OK**, the new settings will be taken effect immediately. This entry will be listed on the Time Range table.

Click **Cancel** to cancel the settings.

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' interface, specifically the 'Port Setup & Status' section. The left sidebar shows a navigation menu with 'Port Management' selected, and 'Port Setup & Status' highlighted. The main content area includes a 'Maximum Frame Size' input field set to 9472 Bytes, a 'Quick Select' dropdown set to 1,2,3-6, and a table of port configurations. The table has columns for Select, Port, Port State (Enable, State, Reason), Description, Preferred Media Type, Port Type, Speed (State, Speed, Duplex), Flow Control, and MAC Address. Ports 1 through 6 are listed, with Port 3 being 'Up' and the others 'Down Link Down'. 'Ok' and 'Reset' buttons are at the bottom.

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"/>	Down	Link Down		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:00:00:01
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Down	Link Down		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:00:00:02
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Up	--		Copper	Auto-Negotiation	1000 Mbps / Full	1000Mbps	Full	<input type="checkbox"/>	00:06:19:00:00:03
<input type="checkbox"/>	4	<input checked="" type="checkbox"/>	Down	Link Down		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:00:00:04
<input type="checkbox"/>	5	<input checked="" type="checkbox"/>	Down	Link Down		Fiber	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:00:00:05
<input type="checkbox"/>	6	<input checked="" type="checkbox"/>	Down	Link Down		Fiber	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:00:00:06

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 (1518-9228)

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"/>	00:06:19:00:31:07
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Down	LKD		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:00:31:08
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Down	LKD		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:00:31:09
<input type="checkbox"/>	4	<input checked="" type="checkbox"/>	Down	LKD		Copper	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:00:31:0A
<input type="checkbox"/>	5	<input checked="" type="checkbox"/>	Down	LKD		Fiber	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:00:31:0B
<input type="checkbox"/>	6	<input checked="" type="checkbox"/>	Down	LKD		Fiber	Auto-Negotiation	--	1000Mbps	Full	<input type="checkbox"/>	00:06:19:00:31:0C

Maximum Frame Size: Specify the maximum frame size between 1518 and 9228 bytes. The default maximum frame size is 9228 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, 3-6) 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 operating speed of ports, which can be 10M/100M/1000M on 1-4 copper port(s) and 100M/1000M on 5-6 SFP port(s), with the current operation duplex mode of the port, either Full or Half.

Speed of Port in Speed field: When you select "**Manual**" as the port type, you can specify the transmission speed **10M/100M/1000M** for copper ports 1-4 and **100M/1000M** for SFP ports 5-6.

When you select “**Auto-Negotiation**” as the port type for ports 1-4 or 5-6, the transmission speed is **1000M**.

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: Each port’s unique factory-assigned MAC address.

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.

Monitor	Rate									Refresh
Port	Rate Event	Bytes Received	Frames Received	Received Utilization	Bytes Sent	Frames Sent	Sent Utilization	Total Bytes	Total Utilization	
1		0	0	0.00%	0	0	0.00%	0	0.00%	
2		0	0	0.00%	0	0	0.00%	0	0.00%	
3		0	0	0.00%	0	0	0.00%	0	0.00%	
4		0	0	0.00%	0	0	0.00%	0	0.00%	
5		0	0	0.00%	0	0	0.00%	0	0.00%	
6		0	0	0.00%	0	0	0.00%	0	0.00%	

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	Rx CRC Error	Rx Align Error	Rx Undersize	Rx Fragments	Rx Oversize Frames (9228 Bytes)	Tx Collisions	Total Errors
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
6	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 Error: CRC Error frames received.

Rx Align Error: Align Error frames received.

Rx Undersize: Undersize frames received.

Rx Fragments: Fragments frames received.

Rx Oversize Frames (9228 Bytes): Oversize frames received.

Tx Collisions: Each port’s Collision frames.

Total Errors: Total error frames received.

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

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

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

4.2.4 Port Packet Analysis Statistics

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

													Clear All	Refresh
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		
Rx Frames 64 Bytes	8	910	0	0	0	0	0	0	0	0	0	0	0	0
Rx Frames 65-127 Bytes	0	209	0	0	0	0	0	0	0	0	0	0	0	0
Rx Frames 128-255 Bytes	0	13	0	0	0	0	0	0	0	0	0	0	0	0
Rx Frames 256-511 Bytes	0	17	0	0	0	0	0	0	0	0	0	0	0	0
Rx Frames 512-1023 Bytes	0	24	0	0	0	0	0	0	0	0	0	0	0	0
Rx Frames 1024-1518 Bytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Frames 1519-Max(9228) Bytes	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Unicast Frames	8	863	0	0	0	0	0	0	0	0	0	0	0	0
Tx Unicast Frames	0	1378	0	0	0	0	0	0	0	0	0	0	0	0
Rx Multicast Frames	0	218	0	0	0	0	0	0	0	0	0	0	0	0
Tx Multicast Frames	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Broadcast Frames	0	92	0	0	0	0	0	0	0	0	0	0	0	0
Tx Broadcast Frames	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rate Units = pps														
Max = Maximum Frame Size (default is 9228)														

Frames 64 Bytes: 64 bytes frames received.

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

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

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

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

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

Frames 1519-Max(9228) Bytes: Over 1519 bytes frames received.

Rx Unicast Frames: Good unicast frames received.

Tx Unicast Frames: Good unicast frames sent.

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.

Port Management » Port Mirroring

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

Disabled ▾

Ok

Occupied/Max Entry: 0/1

Add Port Mirror

Batch Delete

Index	Enabled	Source Port		Destination Port	Action
		Tx	Rx		

This table will display the overview of each configured port mirroring. Up to 1 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

Add Port Mirror

Batch Delete

Index	Enabled	Source Port		Destination Port	Action
		Tx	Rx		
1	Disabled ▾			Port 1 ▾	✓ ✕



150

Enabled: Enable or disable the specific port mirroring.


TX Source Port: Input the port number (e.g.1, 2, 3-6) 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, 3-6) to specify the receiving packets of preferred source port(s) for mirroring. Please note that the port selected as the destination port cannot be the source port.

Destination Port: Choose from port 1 to port 6 from the pull-down menu to designate the destination port. Please note that if there is more than one index, the destination ports for port mirroring cannot be the same across indexes.

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 Link Aggregation

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

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

This Managed switch supports 1 link aggregation modes: static **Port Trunk** using the IEEE 802.3ad standard. These allow several devices to communicate simultaneously at their full single-port speed while not allowing any one single device to occupy all available backbone capacities.

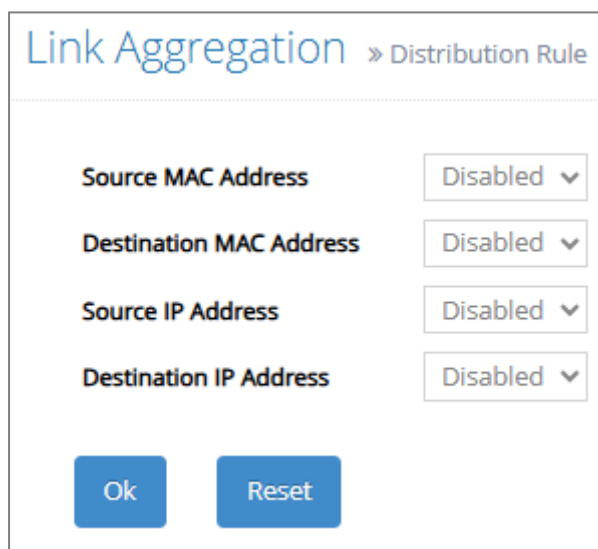
Click the folder **Link Aggregation** from the **Main Menu** and then 2 options within this folder will be displayed as follows.

The screenshot shows a network management interface. On the left is a sidebar menu with the following items: 'Welcome: admin', 'System Setup', 'Port Management', 'Link Aggregation' (highlighted in blue), 'Distribution Rule' (indented under Link Aggregation), 'Static Port Trunking' (indented under Link Aggregation), 'VLAN Setup', 'Rapid Spanning Tree', and 'Fast Redundancy'. The main content area is titled 'Link Aggregation » Distribution Rule'. It contains four configuration fields, each with a 'Disabled' dropdown menu: 'Source MAC Address', 'Destination MAC Address', 'Source IP Address', and 'Destination IP Address'. At the bottom of the main area are two blue buttons: 'Ok' and 'Reset'.

1. **Distribution Rule:** Configure the distribution rule of Port Trunking group(s).
2. **Static Port Trunking:** Create, edit or delete port trunking group(s).

4.3.1 Distribution Rule

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



The screenshot shows a web interface for configuring the 'Distribution Rule' under 'Link Aggregation'. The title bar reads 'Link Aggregation » Distribution Rule'. Below the title, there are four configuration items, each with a label and a dropdown menu:

- Source MAC Address: Disabled ▼
- Destination MAC Address: Disabled ▼
- Source IP Address: Disabled ▼
- Destination IP Address: Disabled ▼

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

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

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

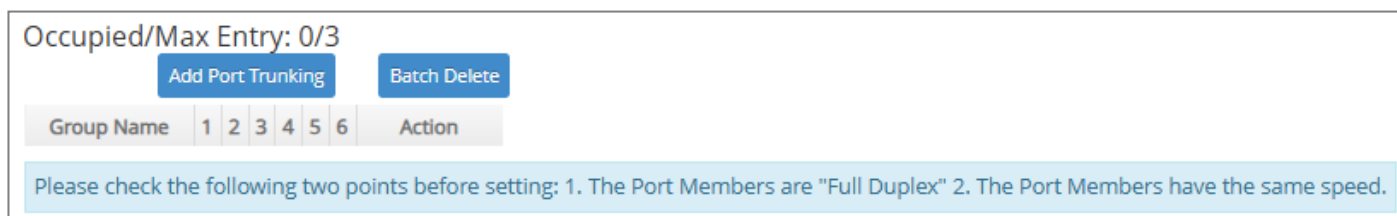
Destination MAC Address: Enable or disable packets according to Destination MAC address.

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

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

4.3.2 Static Port Trunking

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



The screenshot shows a web interface for 'Static Port Trunking'. At the top left, it says 'Occupied/Max Entry: 0/3'. Below this, there are two blue buttons: 'Add Port Trunking' and 'Batch Delete'. Below the buttons is a table with the following structure:

Group Name	1	2	3	4	5	6	Action
Please check the following two points before setting: 1. The Port Members are "Full Duplex" 2. The Port Members have the same speed.							

The Managed Switch allows users to create 3 trunking groups. Each group consists of 2 to 4 links (ports).

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total registered trunking groups.



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

Click **Add Port Trunking** to create a new trunking group and then the following screen page appears for the further port trunking settings.


Group Name: Specify the trunking group name. Up to 15 alphanumeric characters can be accepted.

Port Members: Click on the checkbox of the corresponding port number to select ports that belong to the specified trunking group. Please keep the rules below in mind when assigning ports to a trunking group.

- Must have 2 to 4 ports in each trunking group.
- Each port can only be grouped in one group.

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

Click the  icon to modify the settings of a registered trunking group.

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

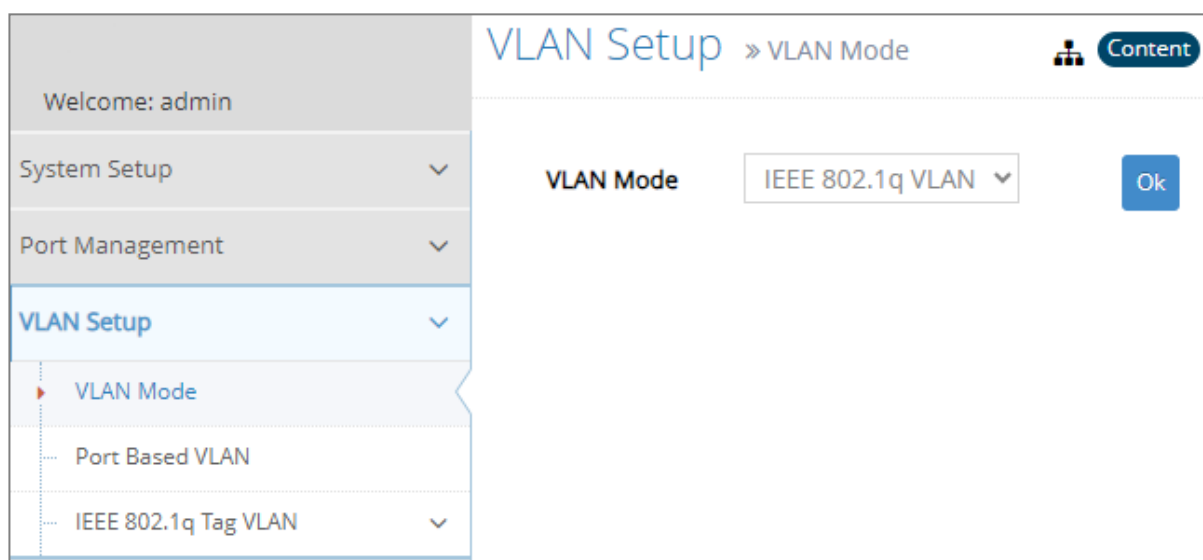
NOTE: All trunking ports in the group must be members of the same VLAN, and their Spanning Tree Protocol (STP) status and QoS default priority configurations must be identical. Port locking, port mirroring and 802.1X cannot be enabled on the trunking group. Furthermore, the LACP aggregated links must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

4.4 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.

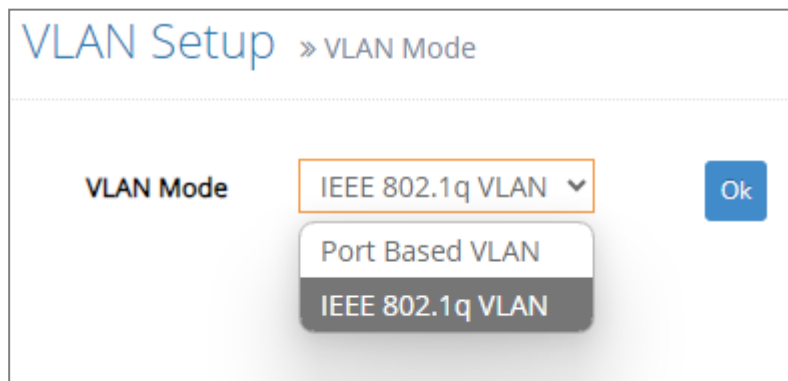
Click **VLAN Setup** folder from the **Main Menu** and then three options within this folder will be displayed.



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 VLAN:** Configure Trunk VLAN Setup, VLAN interface, and view the VLAN Table.

4.4.1 VLAN Mode

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



VLAN Setup » VLAN Mode

VLAN Mode IEEE 802.1q VLAN ▼ Ok

Port Based VLAN

IEEE 802.1q VLAN

VLAN Mode: Specify **Port Based VLAN** or **IEEE 802.1q VLAN** from the drop-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.

4.4.2 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.

Occupied/Max Entry: 1/6

Add Port Based VLAN


Batch Delete


Name	1	2	3	4	5	6	CPU	Action
Default_VLAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	 

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

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: 1/6

Add Port Based VLAN

Batch Delete

Name	1	2	3	4	5	6	CPU	Action
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Default_VLAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	 

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



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.

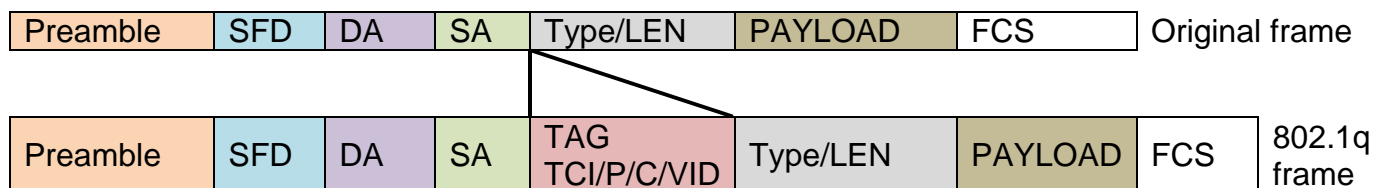
Click  when the settings are completed, this new Port-Based VLAN will be listed on the Port-Based VLAN table, or click  to cancel the settings.

4.4.3 IEEE 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

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

Welcome: admin
System Setup
Port Management
VLAN Setup
VLAN Mode
Port Based VLAN
IEEE 802.1q Tag VLAN
Trunk VLAN Setup
VLAN Interface
VLAN Table
Fast Redundancy
MAC Address Management
QoS Setup
Multicast
Security Setup
LLDP
Power over Ethernet
Maintenance

VLAN Setup » IEEE 802.1q Tag VLAN > VLAN Interface

CPU VLAN ID: 1 (1-4094)
ISP Mode: Disabled
CPU Stag VID: 1 (1-4094)
CPU Stag Priority: 0 (0-7)
Stag EtherType: 0x 9100 (0000-FFFF)

Note: (CPU) Stag Priority uses the same value as User Priority configured in QoS Setup -> Qos Priority page.

Select	Port	Mode	PVID	Trunk-VLAN	Stag VID	Stag Priority	ISP Port
<input type="checkbox"/>	All						<input type="checkbox"/>
<input type="checkbox"/>	1	ACCESS	1	1	1	0	<input type="checkbox"/>
<input type="checkbox"/>	2	ACCESS	1	1	1	0	<input type="checkbox"/>
<input type="checkbox"/>	3	ACCESS	1	1	1	0	<input type="checkbox"/>
<input type="checkbox"/>	4	ACCESS	1	1	1	0	<input type="checkbox"/>
<input type="checkbox"/>	5	ACCESS	1	1	1	0	<input type="checkbox"/>
<input type="checkbox"/>	6	ACCESS	1	1	1	0	<input type="checkbox"/>

Ok
Reset

- Trunk VLAN Setup:** To create, modify or remove IEEE 802.1q Tag VLAN settings.
- VLAN Interface:** To set up VLAN mode, create 802.1q VLAN on the selected port(s), and set up CPU VLAN ID.
- VLAN Table:** View the IEEE 802.1q VLAN table of the Managed Switch.

4.4.3.1 Trunk VLAN Setup

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

VLAN Setup » IEEE 802.1q Tag VLAN > Trunk VLAN Setup

Content Save Reboot Logout

Occupied/Max Entry: 6/128

Add Trunk VLAN Batch Delete

VLAN Name	VID	1	2	3	4	5	6	CPU	Action
Default_VLAN	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
VLAN1000	1000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
VLAN2000	2000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
VLAN3000	3000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
VLAN4000	4000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
VLAN4094	4094	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

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

Click **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: 6/128

Add Trunk VLAN Batch Delete

VLAN Name	VID	1	2	3	4	5	6	CPU	Action
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Default_VLAN	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
VLAN1000	1000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
VLAN2000	2000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
VLAN3000	3000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
VLAN4000	4000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
VLAN4094	4094	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

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

Occupied/Max Entry: View-only field.



Occupied: This shows the amount of total 802.1q VLANs that have already been created.

Max: This shows the maximum number of 802.1q VLANs that can be created. The maximum number is 128.

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

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

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

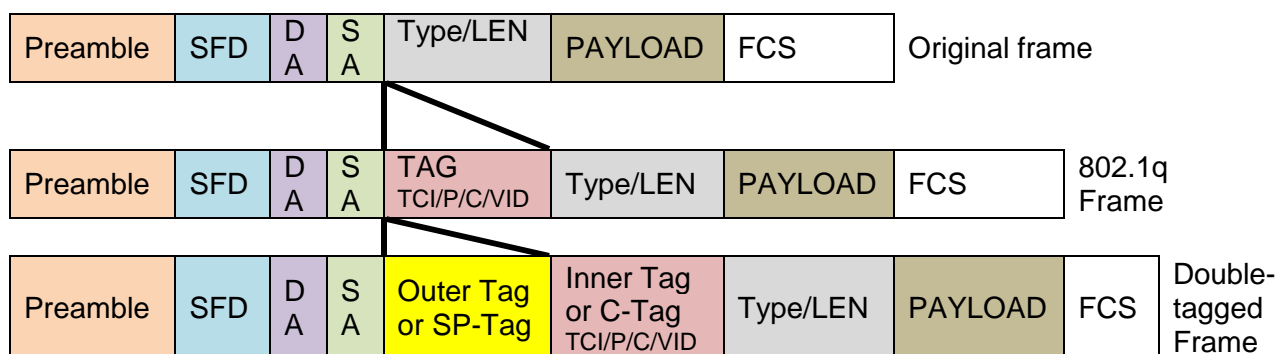
Click  when the settings are completed, this new 802.1q VLAN will be listed on the IEEE 802.1q Tag VLAN Setup table, or click  to cancel the settings.

4.4.3.2 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.

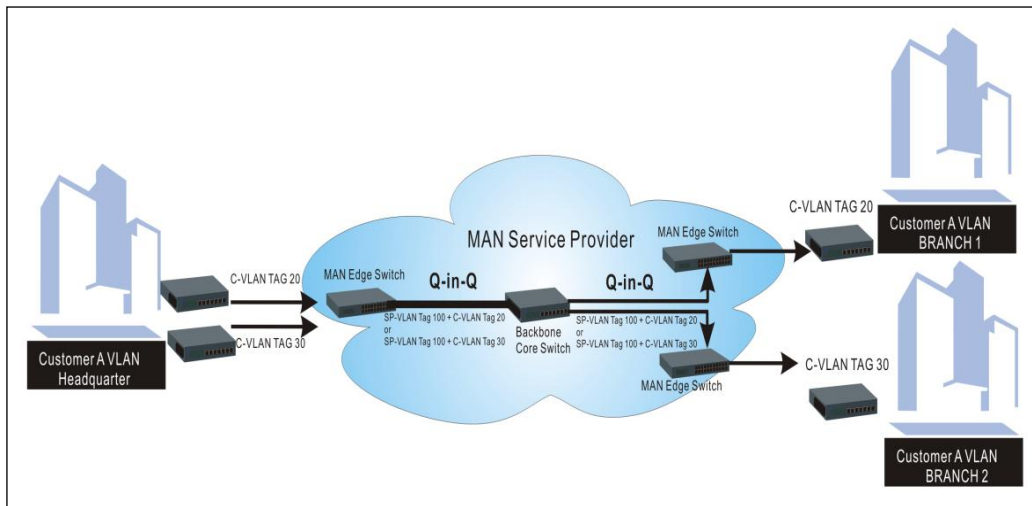
Introduction to Q-in-Q (ISP Mode)

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

CPU Stag VID (1-4094)

CPU Stag Priority (0-7)

Stag EtherType 0x (0000-FFFF)

Note: (CPU) Stag Priority uses the same value as User Priority configured in QoS Setup -> Qos Priority page.

Select	Port	Mode	PVID	Trunk-VLAN	Stag VID	Stag Priority	ISP Port
<input type="checkbox"/>	All	<input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<input type="checkbox"/>	1	ACCESS <input type="button" value="v"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="checkbox"/>
<input type="checkbox"/>	2	ACCESS <input type="button" value="v"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	ACCESS <input type="button" value="v"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	ACCESS <input type="button" value="v"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	ACCESS <input type="button" value="v"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	ACCESS <input type="button" value="v"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="checkbox"/>

CPU VLAN ID: Specify an existing VLAN ID. (Valid range: 1-4094)

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

CPU Stag VID: Specify a service tag VID for the CPU. (Valid range: 1-4094)

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

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

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 VLAN Interface 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.

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

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

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

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

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.

Stag VID: Specify the service tag VID. (Valid range: 1-4094)

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

4.4.3.3 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
VLAN1000	1000	-	-	-	-	-	-	-
VLAN2000	2000	-	-	-	-	-	-	-
VLAN3000	3000	-	-	-	-	-	-	-
VLAN4000	4000	-	-	-	-	-	-	-
VLAN4094	4094	-	-	-	-	-	-	-

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

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

4.5 Rapid Spanning Tree

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

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

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

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

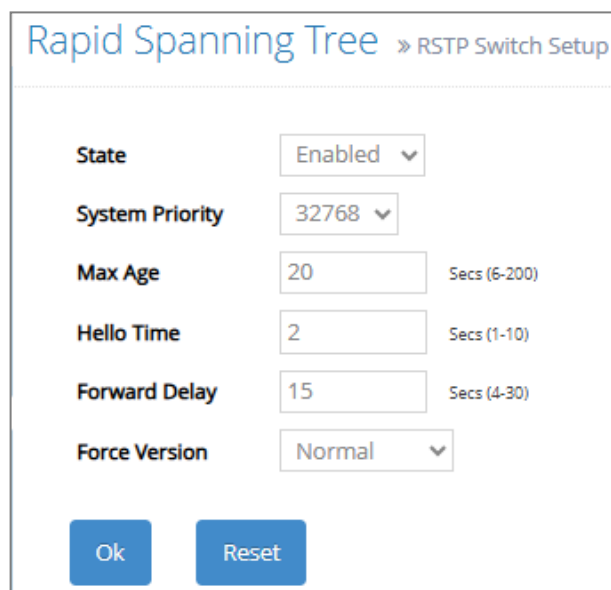
Click the folder **Rapid Spanning Tree** from the **Main Menu** and then 3 options within this folder will be displayed as follows.

The screenshot shows a web interface for configuring Rapid Spanning Tree (RSTP). On the left is a sidebar menu with the following items: 'Welcome: admin', 'System Setup', 'Port Management', 'Link Aggregation', 'VLAN Setup', 'Rapid Spanning Tree' (highlighted), 'RSTP Switch Setup' (sub-item under RSTP), 'RSTP Port Setup', 'RSTP Status', and 'Fast Redundancy'. The main content area is titled 'Rapid Spanning Tree » RSTP Switch Setup'. It contains several configuration fields: 'State' (dropdown menu set to 'Enabled'), 'System Priority' (dropdown menu set to '32768'), 'Max Age' (text input '20' with a range 'Secs (6-200)' to its right), 'Hello Time' (text input '2' with a range 'Secs (1-10)' to its right), 'Forward Delay' (text input '15' with a range 'Secs (4-30)' to its right), and 'Force Version' (dropdown menu set to 'Normal'). At the bottom of the configuration area are two buttons: 'Ok' and 'Reset'.

1. **RSTP Switch Setup:** Set up the system priority, max age, hello time, forward delay time and force version.
2. **RSTP Port Setup:** Set up the RSTP state, path cost, priority, edge status, and point to point setting of each physical port.
3. **RSTP Status:** View RSTP VLAN Bridge, RSTP port status, and RSTP statistics.

4.5.1 RSTP Switch Setup

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



State	Enabled	
System Priority	32768	
Max Age	20	Secs (6-200)
Hello Time	2	Secs (1-10)
Forward Delay	15	Secs (4-30)
Force Version	Normal	

Ok Reset

State: Enable or disable Rapid Spanning Tree function globally.

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

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

Max Age: If another switch in the spanning tree does not send out a hello packet for a long period of time, it is assumed to be disconnected. The default Max. Age is 20 seconds.

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

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

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

4.5.2 RSTP Port Setup

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

Select	Port	State	Port Path Cost (0-200000000)	Port Priority	Port Edge	Port Point to Point
<input type="checkbox"/>	All	<input type="text" value="Disabled"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="checkbox"/>	<input type="text" value="Forced True"/>
<input type="checkbox"/>	1	<input type="text" value="Disabled"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="checkbox"/>	<input type="text" value="Forced True"/>
<input type="checkbox"/>	2	<input type="text" value="Disabled"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="checkbox"/>	<input type="text" value="Forced True"/>
<input type="checkbox"/>	3	<input type="text" value="Disabled"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="checkbox"/>	<input type="text" value="Forced True"/>
<input type="checkbox"/>	4	<input type="text" value="Disabled"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="checkbox"/>	<input type="text" value="Forced True"/>
<input type="checkbox"/>	5	<input type="text" value="Disabled"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="checkbox"/>	<input type="text" value="Forced True"/>
<input type="checkbox"/>	6	<input type="text" value="Disabled"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="checkbox"/>	<input type="text" value="Forced True"/>
<input type="checkbox"/>	Aggregated	<input type="text" value="Disabled"/>	<input type="text" value="1"/>	<input type="text" value="16"/>	<input type="checkbox"/>	<input type="text" value="Forced False"/>

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 RSTP Port Setup 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.

State: Pull down the menu of the corresponding port number to enable or disable RSTP for each port. Default is disable.

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

Port Priority: From the pull-down menu of the corresponding port number, you can choose Port Priority value between 0 and 240 for each port. The default value is “128”.

Port Edge: Click on the checkbox of the corresponding port number to enable or disable Port Edge for each port. Default is disable.

Port Point to Point: Pull down the menu of the corresponding port number to set up the Point to Point setting of each port. The default setting is “Forced True”.

4.5.3 RSTP Status

RSTP Status allows users to view a list of RSTP brief information such as Bridge ID, topology status and Root ID, a list of all RSTP ports' information, and the real-time RSTP statistics of the Managed Switch. Please select the option **RSTP Status** from the **Rapid Spanning Tree** menu and then the following screen page appears.

Refresh

Bridge ID		Max Age	Hello Time	Fwd Delay	Topology	Root ID		Root Port						
32769:00-06-19-00-31-06		20	2	15	Steady	32769:00-06-19-00-31-06		0						
Port	Path Cost	Edge Port	P2P Port	Protocol	Role	Port State	RSTP		STP		TCN		Illegal Received	Unknown Received
							Tx	Rx	Tx	Rx	Tx	Rx		
1	0	no	yes	RSTP	Non-STP	Non-STP	0	0	0	0	0	0	0	0
2	0	no	yes	RSTP	Non-STP	Non-STP	0	0	0	0	0	0	0	0
3	0	no	yes	RSTP	Non-STP	Non-STP	0	0	0	0	0	0	0	0
4	0	no	yes	RSTP	Non-STP	Non-STP	0	0	0	0	0	0	0	0
5	0	no	yes	RSTP	Non-STP	Non-STP	0	0	0	0	0	0	0	0
6	0	no	yes	RSTP	Non-STP	Non-STP	0	0	0	0	0	0	0	0
LLAG1	0	no	no	RSTP	Non-STP	Non-STP	0	0	0	0	0	0	0	0
LLAG2	0	no	no	RSTP	Non-STP	Non-STP	0	0	0	0	0	0	0	0
LLAG3	0	no	no	RSTP	Non-STP	Non-STP	0	0	0	0	0	0	0	0

Refresh: Click **Refresh** to update the latest RSTP status.

Bridge ID: Display RSTP Bridge ID of the Managed Switch

Max Age: Display Max Age setting of the Managed Switch.

Hello Time: Display Hello Time setting of the Managed Switch.

Fwd Delay: Display Forward Delay Time setting of the Managed Switch.

Topology: Display Managed Switch's state of the topology.

Root ID: Display the Root ID of the Managed Switch.

Root port: Display the Root Port Number of the Managed Switch.

Port: The number of the port.

Path Cost: The Path Cost of each port.

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

P2P Port: "Yes" is displayed if the port link is connected to another STP device.

Protocol: Display RSTP or STP.

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

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

RSTP Tx: The total transmitted RSTP packets from each port.

RSTP Rx: The total received RSTP packets from each port.

STP Tx: The total transmitted STP packets from each port.

STP Rx: The total received STP packets from each port.

TCN Tx: The total transmitted TCN (Topology Change Notification) packets from each port.

TCN Rx: The total received TCN (Topology Change Notification) packets from each port.

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

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

4.6 Fast Redundancy

Besides RSTP and Ring Detection as we previously mentioned, the employment of CTS's proprietary fast redundancy on your network will help protect mission-critical links against failures, avoid the occurrence of network loops, and keep network downtime to a minimum to assure the reliability of the network. With these network redundancy, it allows the user to set up redundant loops in a network to provide a backup data transmission route in the event of the disconnection or damage of the cables. By means of this important feature in the network recovery applications, you can be totally free from any loss resulting from the time spent in locating the cable that fails to connect.

CTS's fast redundancy provides **Fast Ring v2** and **Chain** two redundancy protocols, which allows you to configure 2 rings, 2 chains, or 1 ring & 1 chain at most for a switch.

Please note that all switches on the same ring or chain must be the ones with the same brand and configured using the same redundancy protocol when configuring a redundant ring or chain. You are not allowed to use switches with different brands or mix the Ring Detection, Fast Ring v2 and Chain protocols within the same ring or chain.

In the following table, it lists the difference among forementioned redundancy protocols for your evaluation when employing network redundancy on your network.

	Ring Detection	Fast Ring v2	Chain	RSTP
Topology	Ring	Ring	Ring	Ring
Recovery Time	<30 ms	<50 ms	<div><1 second (for copper ports)</div> <div><50 ms (for fiber ports)</div>	Up to 5 seconds

Click the folder **Fast Redundancy** from the **Main Menu** and then 2 options within this folder will be displayed as follows.

- 1. Fast Redundancy Setup:** Configure Fast Ring v2 or Chain protocol to achieve network redundancy and maximum availability.
- 2. Fast Redundancy Status:** Investigate a comprehensive table displaying the up-to-date Fast Redundancy status for the monitoring and analysis of your configured network redundancy.

4.6.1 Fast Redundancy Setup

To configure the Fast Ring v2 or Chain fast redundancy, click the option **Fast Redundancy Setup** from the **Fast Redundancy** menu and then the following screen page appears.

Click **Add Fast Redundancy Entry** to add a new fast redundancy. Up to 2 sets of fast redundancy can be created.

Occupied/Max Entry: 0/2

Add Fast Redundancy Entry

Batch Delete

Entry	Group ID	Enable	Description	Protocol	Role	1st Redundancy Port		2nd Redundancy Port		Action
						Port	Role	Port	Role	

4.6.1.1 Fast Ring v2 Protocol

Fast Ring v2 protocol, the newer version of our Ring Detection, is to optimize communication redundancy and achieve a fast recovery time (<50 ms) on the network for up to 200 switches. Like Ring Detection, Fast Ring v2 protocol manually specifies one switch as the master of the network to identify which segment in the redundant ring acts as the backup path, and then automatically block packets from traveling through any of the network's redundant loops.

In the event that one branch of the ring disconnects from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can rebuild the communication with the rest of the network.

In the following subsection, we will explain how the backup path is selected for rings configured by Fast Ring v2 redundancy protocol.

Occupied/Max Entry: 0/2

Add Fast Redundancy EntryBatch Delete

Entry	Group ID	Enable	Description	Protocol	Role	1st Redundancy Port		2nd Redundancy Port		Action
						Port	Role	Port	Role	

Add New Fast Redundancy

Group ID

1

Enable

Enabled

Description

Protocol

Fast Ring V2

Role

Slave

1st Redundancy Port

Disable

2nd Redundancy Port

Disable

Ok

Cancel

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total fast redundancy that have already been created.

Max: This shows the maximum number available for fast redundancy. The maximum number is 2.

Group ID: The group ID of the fast redundancy. Up to 2 group IDs can be supported.

Enable: Enable or disable the ring you configure.

Description: The description of the group.

Protocol: Include “Fast Ring v2” and “Chain” two redundancy protocols. To configure a Fast Ring v2 ring redundancy, pull down the menu of **Protocol** and choose **Fast Ring v2** as the protocol for the fast redundancy you configure.

Role: Pull down the menu of **Role** to assign the role of the Managed Switch as either Slave or Master when Fast Ring v2 protocol is chosen.

Master: A role possesses the ability of blocking or forwarding packets. Please note that the blocked segment is the segment that connects to the 2nd redundancy port on the master.


Slave: A role possesses the ability of forwarding packets only.

1st Redundancy Port: Specify which port of the Managed Switch to be acted as the first redundant port. Default value is **Disable**.

2nd Redundancy Port: Specify which port of the Managed Switch to be acted as the secondary redundant port. Default value is **Disable**.

Click **OK**, the new settings will be taken effect immediately. This entry will be listed on the fast redundancy table.

Click the  icon to modify the settings of a specified fast redundancy.

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

4.6.1.1.1 Configure a Ring Example using the Fast Ring v2 Protocol

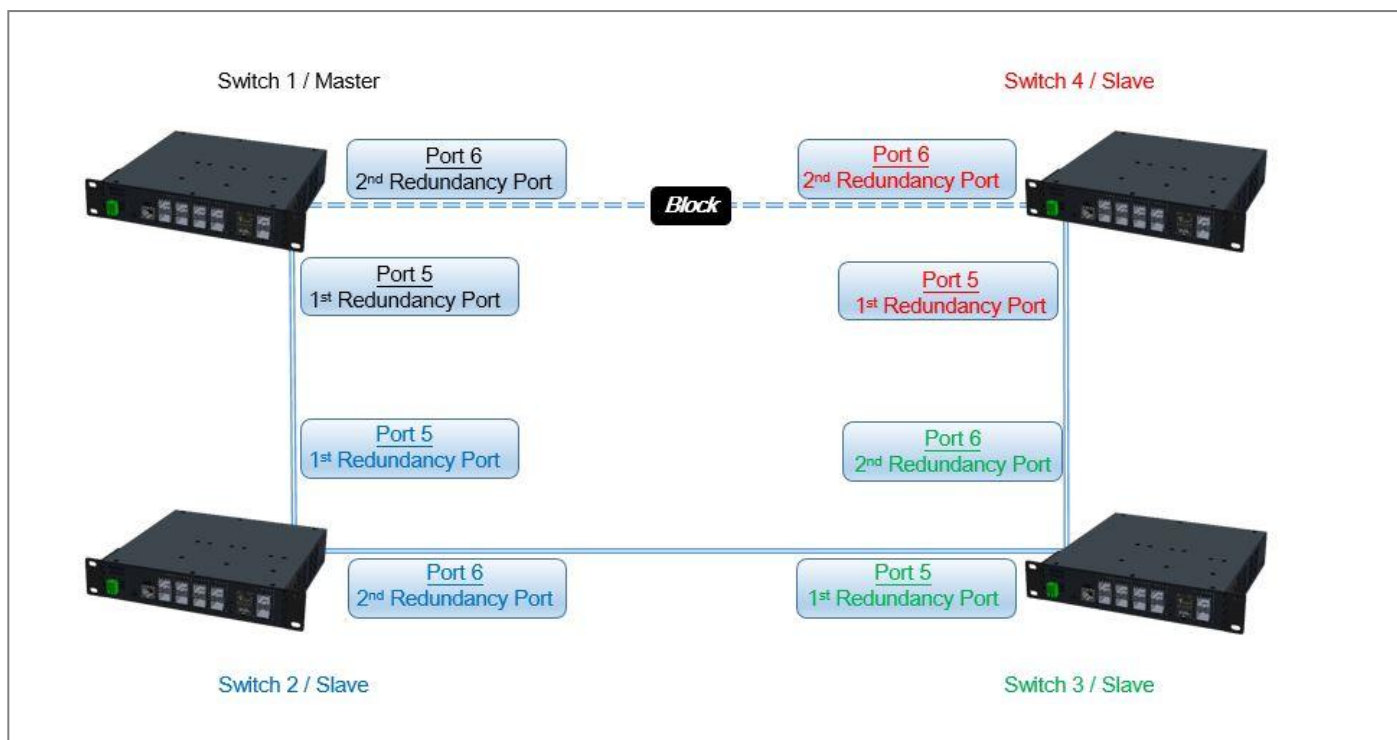


Fig. 4-1 Fast Ring v2 Example Diagram

The above topology often occurs using the Fast Ring v2 protocol and is configured as the following table.

Switch ID	Role	Redundancy Port	Physical Port
Switch 1	Master	1 st Redundancy Port	Port 5
		2 nd Redundancy Port	Port 6
Switch 2	Slave	1 st Redundancy Port	Port 5
		2 nd Redundancy Port	Port 6
Switch 3	Slave	1 st Redundancy Port	Port 5
		2 nd Redundancy Port	Port 6
Switch 4	Slave	1 st Redundancy Port	Port 5
		2 nd Redundancy Port	Port 6

Table 4-1 Fast Ring v2 Configuration

The scenario is described as below:

1. Disable DHCP client and set proper static IP address for Switch 1, 2, 3 & 4. In this example, Switch 1 is 192.168.0.101/24; Switch 2 is 192.168.0.102/24; Switch 3 is 192.168.0.103/24 and Switch 4 is 192.168.0.104/24.
2. On Switch 1~4, disable spanning tree protocol to avoid conflict with Fast Ring v2.

Just follow the procedures listed below for step-by-step instructions to configure a ring as Fig. 4-1 using the Fast Ring v2 protocol.

Step 1: Set up the Fast Ring v2 configuration on Switch 1.

1-1. Connect a computer to Switch 1 directly; do not connect to Port 5 & 6.

1-2. Login into the Switch 1 and go to **Fast Redundancy Setup** from the **Fast Redundancy** menu for the Fast Ring v2 configuration. Click the **Add Fast Redundancy Entry** button to create a Fast Ring v2.

Fast Redundancy » Fast Redundancy Setup


Occupied/Max Entry: 0/2

Add Fast Redundancy Entry

Batch Delete

Entry	Group ID	Enable	Description	Protocol	Role	1st Redundancy Port		2nd Redundancy Port		Action
						Port	Role	Port	Role	

1-3. Please refer to each column parameter below, set “Group ID” = 1, “Enable” = Enabled, “Protocol” = Fast Ring v2, “Role” = Master, “1st Redundancy Port” = Port 5 & “2nd redundancy Port” = Port 6, click **OK** when completing the Fast Ring v2 configuration for Switch 1.

 Add New Fast Redundancy

Group ID

1

Enable

Enabled

Description

Protocol

Fast Ring V2

Role

Slave

1st Redundancy Port

Port 5

2nd Redundancy Port

Port 6

Ok


Cancel

Step 2: Set up the Fast Ring v2 configuration on Switch 2, 3 & 4.

2-1. Connect a computer to Switch 2, 3 & 4 directly; do not connect to Port 5 & 6.

2-2. Login into the Switch 2, 3 & 4 and also go to **Fast Redundancy > Fast Redundancy Setup** for the Fast Ring v2 configuration. Click the **Add Fast Redundancy Entry** button to create a Fast Ring v2.

2-3. Please refer to each column parameter below, set “Group ID” = 1, “Enable” = Enabled, “Protocol” = Fast Ring v2, “Role” = Slave, “1st Redundancy Port” = Port 5 & “2nd Redundancy Port” = Port 6, click **OK** when completing the Fast Ring v2 configuration for Switch 2, 3 & 4.

 Add New Fast Redundancy

Group ID	1 ▾
Enable	Enabled ▾
Description	<input type="text"/>
Protocol	Fast Ring V2 ▾
Role	Slave ▾
1st Redundancy Port	Port 5 ▾
2nd Redundancy Port	Port 6 ▾

Ok

Cancel

NOTE: To avoid the occurrence of loop, please do not connect Switch 1, 2, 3 & 4 together in the ring topology before the end of Fast Ring v2 configuration.

Step 3: Follow the configuration to connect the Switch 1, 2, 3 & 4 together to establish the Fast Ring v2 application.

4.6.1.2 Chain Protocol

CTS's Chain is an advanced software technology that gives network administrators the flexibility to build any type of redundant network topology. It also enables the network to recover in less than 50ms for up to 200 switches if at any time a segment of the chain fails.

When employing a Chain in your network, you first connect the Managed Switches in a chain, and then simply link the two ends of this chain to an Ethernet network. All switches in the chain can be fallen into three parts:

- A Head switch,
- A Tail switch,
- Member switches.

The Head port of the Head switch usually acts as the external port for the entire chain, the Tail port of the Tail switch acts as the blocked port. When the Head port is disconnected, the Tail port will be immediately activated for the data transferring.

The Chain redundancy protocol can be applied to the networks with a complex topology. If the network uses a multi-ring architecture, CTS's Chain can be the best solution to create flexible and scalable topologies with a fast media recovery time.

In the following subsection, we will explain how the backup path is selected for chains configured by the Chain redundancy protocol.

Occupied/Max Entry: 0/2 Add Fast Redundancy Entry Batch Delete

Entry	Group ID	Enable	Description	Protocol	Role	1st Redundancy Port		2nd Redundancy Port		Action
						Port	Role	Port	Role	

Add New Fast Redundancy

Group ID

Enable

Description

Protocol

1st Redundancy Port Role

2nd Redundancy Port Role

Ok Cancel

Occupied/Max Entry: View-only field.

Occupied: This shows the amount of total fast redundancy that have already been created.

Max: This shows the maximum number available for fast redundancy. The maximum number is 2.

Group ID: The group ID of the fast redundancy. Up to 2 group IDs can be supported.

Enable: Enable or disable the chain you configure.

Description: The description of the group.

Protocol: Include “Fast Ring v2” and “Chain” two redundancy protocols. To configure a chain redundancy, pull down the menu of **Protocol** and choose **Chain** as the protocol for the fast redundancy you configure.

1st Redundancy Port: Specify which port of Managed Switch to be acted as the first redundant port. Default value is **Disable**.

Role of 1st Redundancy Port: Include **Head**, **Member** and **Tail** three types of roles.

Head: A role acts as the external port for the entire chain.

Tail: A role acts as the blocked port for the entire chain.


Member: A role acts as an intermediate-connection port between the head port and the tail port.

2nd Redundancy Port: Specify which port of Managed Switch to be acted as the secondary redundant port. Default value is **Disable**.

Role of 2nd Redundancy Port: View-only field. Only **Member** role is allowed.

Click **OK**, the new settings will be taken effect immediately. This entry will be listed on the fast redundancy table.

Click the  icon to modify the settings of a specified fast redundancy.

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

4.6.1.2.1 Configure a Chain Example using the Chain Protocol

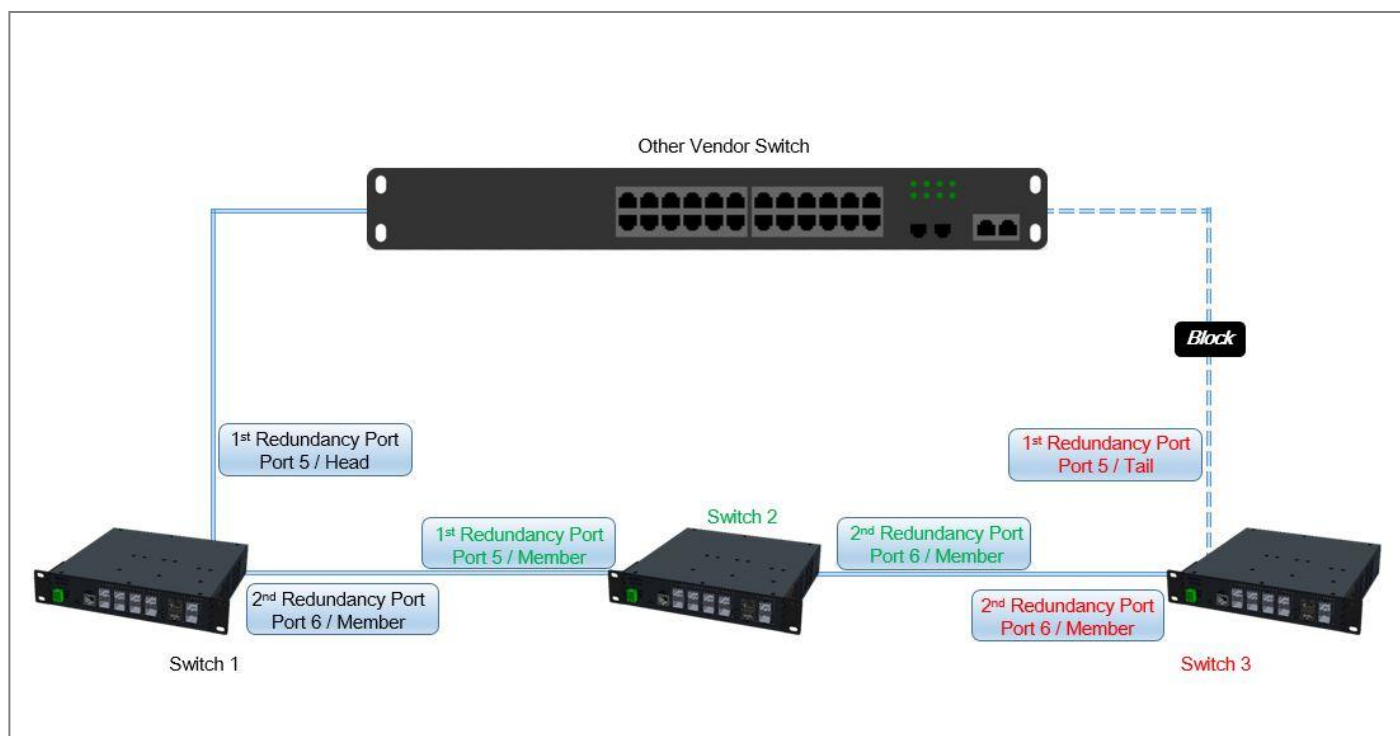


Fig. 4-2 Chain Example Diagram

The above topology often occurs using the Chain protocol and is configured as the following table.

Switch ID	Redundancy Port	Physical Port	Port Role
Switch 1	1 st Redundancy Port	Port 5	Head
	2 nd Redundancy Port	Port 6	Member
Switch 2	1 st Redundancy Port	Port 5	Member
	2 nd Redundancy Port	Port 6	Member
Switch 3	1 st Redundancy Port	Port 5	Tail
	2 nd Redundancy Port	Port 6	Member

Table 4-2 Chain Configuration

The scenario is described as below:

1. Disable DHCP client and set proper static IP address for Switch 1, 2, & 3. In this example, Switch 1 is 192.168.0.101/24; Switch 2 is 192.168.0.102/24 and Switch 3 is 192.168.0.103/24.
2. On Switch 1~3, disable spanning tree protocol to avoid confliction with Chain.

Just follow the procedures listed below for step-by-step instructions to configure a chain as Fig. 4-2 using the Chain protocol.

Step 1: Set up the Chain configuration on Switch 1.

1-1. Connect a computer to Switch 1 directly; do not connect to Port 5 & 6.

1-2. Login into the Switch 1 and go to **Fast Redundancy > Fast Redundancy Setup** for the chain configuration. Click the **Add Fast Redundancy Entry** button to create a chain.


Fast Redundancy » Fast Redundancy Setup

Occupied/Max Entry: 0/2

[Add Fast Redundancy Entry](#) [Batch Delete](#)

Entry	Group ID	Enable	Description	Protocol	Role	1st Redundancy Port		2nd Redundancy Port		Action
						Port	Role	Port	Role	

1-3. Please refer to each column parameter below, set “Group ID” = 1, “Enable” = Enabled, “Protocol” = Chain, “1st Redundancy Port” = Port 5, “1st Redundancy Port / Role” = Head, & “2nd Redundancy Port” = Port 6, click **OK** when completing the chain configuration for Switch 1.

 Add New Fast Redundancy

Group ID:

Enable:

Description:

Protocol:

1st Redundancy Port: Role:

2nd Redundancy Port: Role:


[Ok](#) [Cancel](#)

Step 2: Set up the Chain configuration on Switch 2.

2-1. Connect a computer to Switch 2 directly; do not connect to Port 5 & 6.

2-2. Login into the Switch 2 and also go to **Fast Redundancy > Fast Redundancy Setup** for the chain configuration. Click the **Add Fast Redundancy Entry** button to create a chain.

2-3. Please refer to each column parameter below, set “Group ID” = 1, “Enable” = Enabled, “Protocol” = Chain, “1st Redundancy Port” = Port 5, “1st Redundancy Port / Role” = Member, & “2nd Redundancy Port” = Port 6, click **OK** when completing the chain configuration for Switch 2.

 Add New Fast Redundancy

Group ID

1

Enable

Enabled

Description

Protocol

Chain

1st Redundancy Port

Port 5

Role

Member

2nd Redundancy Port

Port 6

Role

Member

Ok


Cancel

Step 3: Set up the Chain configuration on Switch 3.

3-1. Connect a computer to Switch 3 directly; do not connect to Port 5 & 6.

3-2. Login into the Switch 3 and also go to **Fast Redundancy > Fast Redundancy Setup** for the chain configuration. Click the **Add Fast Redundancy Entry** button to create a chain.

3-3. Please refer to each column parameter below, set “Group ID” = 1, “Enable” = Enabled, “Protocol” = Chain, “1st Redundancy Port” = Port 5, “1st Redundancy Port / Role” = Tail, & “2nd Redundancy Port” = Port 6, click **OK** when completing the chain configuration for Switch 3.

 Add New Fast Redundancy

Group ID

1

Enable

Enabled

Description

Protocol

Chain

1st Redundancy Port

Port 5

Role

Tail

2nd Redundancy Port

Port 6

Role

Member

Ok

Cancel

NOTE: To avoid the occurrence of loop, please do not connect Switch 1, 2, & 3 together in the chain topology before the end of Chain configuration.

Step 4: Follow the configuration to connect the Switch 1, 2, & 3 together to establish Chain application.

4.6.2 Fast Redundancy Status

Fast Redundancy Status allows users to view a list of Fast Redundancy detailed information. This status page is mainly divided into three subdivisions: **Topology Change Status**, allowing users to keep abreast of the dynamic change of the topology wherein the switches operate; **Fast Redundancy Status**, delivering a comprehensive information in exact accordance with the saved-configuration; and **Fast Redundancy Statistics**, offering a real-time Fast Redundancy statistics for efficient troubleshooting and easy monitoring. Please select the option **Fast Redundancy Status** from the **Fast Redundancy** menu and then the following screen page appears.

Fast Redundancy » Fast Redundancy Status

Refresh Page Interval Secs (1-300)

[Start Auto Update](#) [Stop Auto Update](#) [Update](#)

Topology Change Status

Topology Change			Clear Counters
Times	Last Change Time	Elapsed Time	
0	--	--	Clear

Fast Redundancy Status

Entry	Group ID	Enable	Description	Protocol	Role	Status	1st Redundancy Port			2nd Redundancy Port		
							Port	Role	Status	Port	Role	Status

Fast Redundancy Statistics

Entry	Tx		Rx		Clear Counters
	Normal	Failure	Normal	Failure	

Refresh Page Interval: Automatically updates statistics of the Fast Redundancy Status page encompassing three main subdivisions 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 to the next system boot-up. Click **Start/Stop Auto Update** to activate auto-update; click **Update** to manually refresh the event log table once.

Topology Change Status: Includes the following information.

1. **Times:** The total number of times the topology has changed.
2. **Last Change time:** The explicit time when the nearest topology change occurs.
3. **Elapsed Time:** Displays how much time has elapsed since the last change of the topology.
4. **Clear:** This allows users to reset the recorded information.

Fast Redundancy Status: Includes the following information.

1. **Entry:** A designated number as either 1 or 2, which is given according to the sequence of added Fast Redundancy. The maximum number is 2.

2. **Group ID:** The group ID of the fast redundancy.
3. **Description:** The description of the group.
4. **Enable:** The availability of the fast redundancy.
5. **Protocol:** The fast redundancy specified as either “Fast Ring v2” or “Chain.”
6. **Role:** The role assigned to the Managed Switch as either Slave or Master when Fast Ring v2 protocol is chosen. It will show “--” when the Chain protocol is chosen.

Master: A role possesses the ability of blocking or forwarding packets.

Slave: A role possesses the ability of forwarding packets only.

7. **Status:** Signifies the connection status of the fast redundancy you configured, and includes **Healthy**, **Break** and **Signal Fail** 3 types of state. Each state is described as below.

Healthy: Indicates that the connection of the fast redundancy is in normal status.

Break: Indicates that the failure of fast redundancy connection occurs on other switch and its backup link is activated to transmit the data.

Signal Fail: Indicates that the failure of fast redundancy connection occurs on the switch itself and its backup link is activated to transmit the data.

8. **1st/2nd Redundancy Port:** The port of the Managed Switch acts as the first/second interface of the Fast Redundancy.

9. **Role of 1st/2nd Redundancy Port:** Shows the role (Head, Member and Tail) that the port acting as the first/secondary redundant port plays when the Chain protocol is chosen. It will show “--” when the Fast Ring v2 protocol is chosen.

Head: A role acts as the external port for the entire chain.

Member: A role acts as an intermediate-connection port between the head port and the tail port.

Tail: A role acts as the blocked port for the entire chain.

10. **Status of 1st/2nd Redundancy Port:** Shows the connection status of the port that acts as the first/secondary redundant port. Includes **Forwarding**, **Blocked** and **Link down** 3 types of port state. Each state is described as below.

Forwarding: Indicates that the port connection of the fast redundancy is in normal status.

Blocked: Indicates that the port is connected to a backup path and the path is blocked.

Link down: Indicates that no port connection exists.

Fast Redundancy Statistics: Includes the following information.

1. **Entry:** A designated number as either 1 or 2, which given according to the sequence of

the created Fast Redundancy. The maximum number is 2.

2. **TX/RX Source Normal:** The amount of packets successfully transmitted/received.
3. **TX/RX Source Failure:** The amount of packet loss in transmitting/receiving.
4. **Clear:** This allows users to reset the recorded information.

4.7 MAC Address Management

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

Welcome: admin

Link Aggregation ▾

VLAN Setup ▾

Rapid Spanning Tree ▾

Fast Redundancy ▾

MAC Address Management ▾

- MAC Table Learning
- MAC Address Table

MAC Address Management » MAC Table Learning

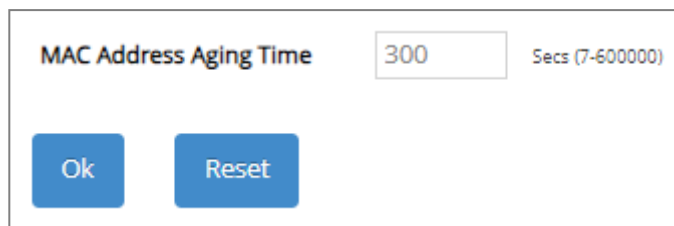
MAC Address Aging Time Secs (7-600000)

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.

4.7.1 MAC Table Learning

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



The image shows a configuration window for MAC Address Aging Time. It has a title bar, a label 'MAC Address Aging Time', a text input field containing '300', and a unit label 'Secs (7-600000)'. Below the input field are two blue buttons: 'Ok' and 'Reset'.

MAC Address Aging Time	<input type="text" value="300"/>	Secs (7-600000)
<div>Ok Reset</div>		

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

4.7.2 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	Multicast
2048	2048	0	0	0	0	0

Clear All

Clear by Port List

1,2,3-6

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

1,2,3-6

Sort by

Port

Search

MAC Address

0 Entries

Index	Type	MAC Address	VID	Port
-------	------	-------------	-----	------

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.8 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 shows a web-based configuration interface for a network switch. On the left is a sidebar menu with the following items: 'Welcome: admin', 'VLAN Setup', 'Rapid Spanning Tree', 'Fast Redundancy', 'MAC Address Management', 'QoS Setup' (highlighted), 'QoS Priority' (sub-item under QoS Setup), 'QoS Remarking', 'QoS Rate Limit', 'Multicast', 'Security Setup', and 'LLDP'. The main content area is titled 'QoS Setup > QoS Priority'. It contains two sections: 'QoS Priority' and 'User Priority'. In the 'QoS Priority' section, there are two dropdown menus: 'Priority Mode' set to 'Disabled' and 'Queue Mode' set to 'Strict'. The 'User Priority' section features a table with 7 columns: 'Port', '1', '2', '3', '4', '5', '6', and 'CPU'. Below the table, there is a row of input boxes labeled 'Priority' with the value '0' entered in each box. At the bottom of the main content area are two buttons: 'Ok' and 'Reset'.

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

1. **QoS Priority:** To set up each port's QoS default class, Priority, Queuing Mode, Queue Weighted, and so on.
2. **QoS Remarking:** To set up QoS 802.1p Remarking and DSCP Remarking.
3. **QoS Rate Limit:** To configure each port's Ingress and Egress Rate.

4.8.1 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.

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 for queues 1 through 4 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 31.

Queue Weight Q0 1 : Q1 2 : Q2 4 : Q3 8 (1-31)

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 Q0 ▾

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”.

4.8.2 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

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 ▾

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) ▾

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) ▼

4.8.3 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.

Quick Select

Select	Port	Ingress			Egress		
		Enabled	Rate (32-1000000 Kbits/Sec)	Unit	Enabled	Rate (32-1000000 Kbits/Sec)	Unit
<input 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"/>	<input type="text" value="500"/>	<input type="text" value="Kbps"/>	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="Kbps"/>
<input type="checkbox"/>	2	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="Kbps"/>	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="Kbps"/>
<input type="checkbox"/>	3	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="Kbps"/>	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="Kbps"/>
<input type="checkbox"/>	4	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="Kbps"/>	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="Kbps"/>
<input type="checkbox"/>	5	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="Kbps"/>	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="Kbps"/>
<input type="checkbox"/>	6	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="Kbps"/>	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="Kbps"/>

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, 3-6) 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 32 ~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.

4.9 Multicast

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

4.9.1 IGMP/MLD Snooping

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

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

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

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

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

Select the subfolder **IGMP/MLD Snooping** and then 9 options will be displayed for your selection.

Welcome: admin

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
 - MLD Group Table

Security Setup

LLDP

Multicast » IGMP/MLD Snooping > IGMP/MLD Setup

IGMP/MLD Snooping: Disabled

IGMPv3/MLDv2 Snooping: Disabled

Query Interval: 125 Secs (1-6000)

Query Response Interval: 100 1/10 Secs (1-255)

Fast Leave: Disabled

Stream Life Time: Disabled

Router Port: ☐ Select All

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☒ 5 ☒ 6

Query interval must be greater than Query Response interval.

Ok Reset

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

4.9.1.1 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.

Multicast » IGMP/MLD Snooping > IGMP/MLD Setup

IGMP/MLD Snooping	Disabled ▾
IGMPv3/MLDv2 Snooping	Disabled ▾
Query Interval	125 <small>Secs (1-6000)</small>
Query Response Interval	100 <small>1/10 Secs (1-255)</small>
Fast Leave	Disabled ▾
Stream Life Time	Disabled ▾
Router Port	<input type="checkbox"/> Select All
	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6

Query interval must be greater than Query Response interval.

Ok Reset

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

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

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

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

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

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

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

4.9.1.2 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	Disabled

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

VID: VID of the specific VLAN.

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

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

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

4.9.1.3 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.



VLAN ID	Querier	Queries Transmitted	Queries Received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
---------	---------	---------------------	------------------	------------	------------	------------	-----------

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

VLAN ID: VID of the specific VLAN.

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

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

Querier: The state of IGMP querier in the VLAN.

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

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

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

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

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

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

4.9.1.4 IGMP Group Table

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

Total Entry		0					Refresh
VLAN ID	Group (MAC)	Port	Last Reporter	Query Response	Report Count	Life Time	

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

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

VLAN ID: The VLAN ID associated with the multicast group.

Group (MAC): The IP address for the multicast group.

Port: The port from which the Managed Switch receives the IGMP join/report message.

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

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

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

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

4.9.1.5 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.



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.

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).

4.9.1.6 MLD Group Table

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

Total Entry		0					Refresh
VLAN ID	Group (MAC)	Port	Last Reporter	Query Response	Report Count	Life Time	

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

VLAN ID: VID of the specific VLAN.

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

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

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

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

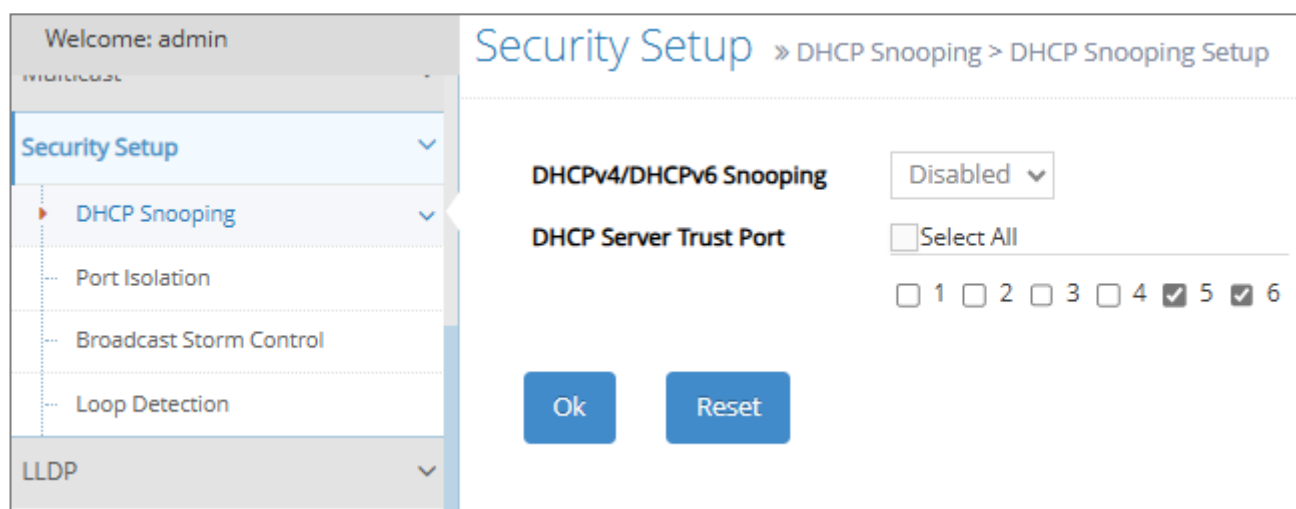
Report Count: A counter of the received MLD join/report message. Upon receiving, the Managed switch will reset Life Time, also a countdown timer yet of the specified Stream Life Time.

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

4.10 Security Setup

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

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



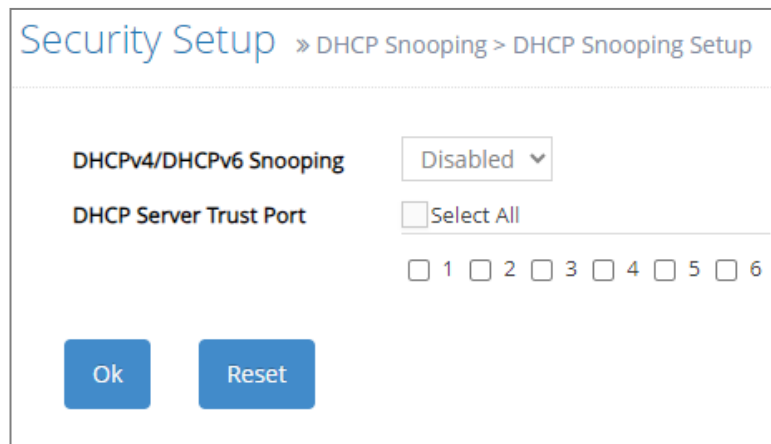
1. **DHCP Snooping:** To set up DHCP Snooping and DHCP server trust ports.
2. **Port Isolation:** Set up port's communication availability that they can only communicate with a given "uplink".
3. **Broadcast Storm Control:** To prevent the Managed Switch from broadcast storm.
4. **Loop Detection:** Enable or disable Loop Detection function, set up Loop Detection configuration and view the Loop Detection status of each port.

4.10.1 DHCP Snooping Configuration

Select the option **DHCP Snooping** from the **Security Setup** folder and then DHCP Snooping Setup will be displayed for your selection.

4.10.1.1 DHCP Snooping Setup

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



The screenshot shows a web-based configuration interface for DHCP Snooping. At the top, a breadcrumb trail reads "Security Setup > DHCP Snooping > DHCP Snooping Setup". Below this, there are two main configuration sections. The first section, "DHCPv4/DHCPv6 Snooping", features a dropdown menu currently set to "Disabled". The second section, "DHCP Server Trust Port", includes a "Select All" checkbox and a row of six individual port checkboxes labeled 1 through 6. At the bottom of the form are two blue buttons: "Ok" and "Reset".

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

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

4.10.2 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

Uplink Port ☐ Select All

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☒ 6

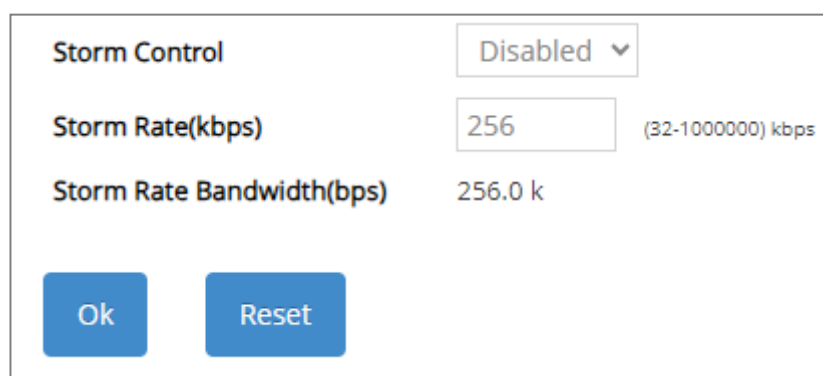
Port Isolation Enable: Enable or disable port isolation function. If port isolation is set to enabled, the ports cannot communicate with each other.

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.

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



The screenshot shows a configuration window for Broadcast Storm Control. It contains three main settings: 'Storm Control' set to 'Disabled' with a dropdown arrow, 'Storm Rate(kbps)' set to '256' with a range '(32-1000000) kbps' in parentheses, and 'Storm Rate Bandwidth(bps)' set to '256.0 k'. At the bottom, there are two blue buttons labeled 'Ok' and 'Reset'.

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

Storm Rate (Kbps): Set up storm rate value. Packets exceeding the value will be dropped.

Storm Rate Bandwidth (bps): Display the current configured storm rate bandwidth.

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

4.10.4 Loop Detection Configuration

In a real network, it is possible for people to misconnect network cables, leading to a loop condition. In the worst-case scenario, this can cause the network to become non-operational. This section provides guidance on configuring the system's Loop Detection function to prevent such loops.

When the Loop Detection function is properly configured, the system detects loop conditions by checking the VLAN and MAC addresses of received packets and comparing them against the MAC address table. Once a loop condition is detected on specific port(s), the system takes the following actions:

1. **Block the affected port(s):** The system stops forwarding all traffic through the looped port(s).
2. **Send an SNMP trap:** This notification informs the network administrator of the detected loop condition.

After the system blocks relevant port, there are two ways to unlock it:

1. **Automatic Unlock:** The system will automatically unlock the blocked port after the configured Unlock Interval (in minutes) has elapsed. The default interval is 1440 minutes.
2. **Manual Unlock:** The network administrator can manually unlock the blocked port.

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

Welcome: admin

MAC Address Management

QoS Setup

Multicast

Security Setup

- DHCP Snooping
 - DHCP Snooping Setup
- Port Isolation
- Broadcast Storm Control
- Loop Detection**

LLDP

Power over Ethernet

Maintenance

Management

Logout

Security Setup » Loop Detection

Loop Detection Enable Disabled

Looped Port Unlock-interval 1440 Mins (1-1440)

Current Status Update

Refresh

Select	Port	Status	Reason of being locked	Unlock
<input type="checkbox"/>	All	--	--	Unlock
<input type="checkbox"/>	1	Unlocked		Unlock
<input type="checkbox"/>	2	Unlocked		Unlock
<input type="checkbox"/>	3	Unlocked		Unlock
<input type="checkbox"/>	4	Unlocked		Unlock
<input type="checkbox"/>	5	Unlocked		Unlock
<input type="checkbox"/>	6	Unlocked		Unlock

Ok Reset

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

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

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

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

Port: The number of each port.

NOTE: *Loop Detection, Fast redundancy and RSTP (Rapid Spanning Tree Protocol) is not allowed to be enabled on the same port at the same time.*

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

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

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

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

4.11 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 a web-based configuration interface for LLDP. On the left is a sidebar menu with the following items: Welcome: admin, LLDP (selected), VLAN Setup, Rapid Spanning Tree, Fast Redundancy, MAC Address Management, QoS Setup, Multicast, Security Setup, LLDP Setup, LLDP Status, Power over Ethernet, Maintenance, Management, and Logout. The main content area is titled 'LLDP » LLDP Setup'. It contains several configuration fields: 'State' is set to 'Enabled'; 'Receiver Hold-Time (TTL)' is 120 seconds (range 1-3600); 'Sending LLDP Packet Interval' is 5 seconds (range 1-180); and 'Sending LLDP Packets Per Discover' is 1 packet (range 1-16). Below these is a section 'Selection of LLDP TLVs to Send' with checkboxes for Port Description, System Name, System Description, System Capabilities, and Management Address, all of which are checked. The next section is 'LLDP Port Configuration', which includes a 'Select All' checkbox and individual checkboxes for ports 1 through 6. At the bottom are 'Ok' and 'Reset' buttons.

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.

4.11.1 LLDP Setup

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

LLDP » LLDP Setup

State: Enabled

Receiver Hold-Time (TTL): 120 (Secs (1-3600))

Sending LLDP Packet Interval: 5 (Secs (1-180))

Sending LLDP Packets Per Discover: 1 (Packet (1-16))

Selection of LLDP TLVs to Send

Port Description: ☒

System Name: ☒

System Description: ☒

System Capabilities: ☒

Management Address: ☒

LLDP Port Configuration

LLDP Port: ☐ Select All

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6

Ok 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.

4.11.2 LLDP Status

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

Refresh										
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.

4.12 Power over Ethernet

PoE (Power Over Ethernet) is the technology that a data-carrying RJ-45 cable can play a role in power supplier. Typically, a PoE switch is deployed at the center of the network for power transmission and supplies electricity to PDs (powered devices) up to 100 meters away through TP ports. PDs can be installed wherever there is a LAN cable rather than AC power source. The user need not be present at powered devices location, which greatly reduces truck rolls. The Managed PoE Switch even supports time-based PoE, defining the time interval when powered devices are desired to be automatically powered on a daily or weekly basis, for budget-conscious users to be more efficient power management.

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

NOTE: The PoE configuration page is accessible only on PoE switch models. This section will not appear on non-PoE devices.

Welcome: admin

System Setup

Port Management

VLAN Setup

MAC Address Management

QoS Setup

Multicast

Security Setup

LLDP

Power over Ethernet

PoE Setup

PoE Status

Maintenance

Management

Logout

Power over Ethernet » PoE Setup

Note !!

1. Once the specify PoE power in is force PoE inline mode, the PoE port will ignore the PoE classification behaviors and directly deliver power over RJ45 cable no matter what Ethernet device is attached, or even there is no Ethernet cable plugged.
2. Please be careful when using force PoE inline mode and make sure the remote device is PoE powered device (PD).
3. Re-enabled PoE interval configuration and Re-enabled button only can configure and enabled when PoE inline mode is force mode.
4. Please set re-enabled PoE interval first when force PoE inline mode has issue and need to re-inject the force PoE power and need to and click Re-enabled button.

PoE

Total PoE Budget (0-300 watts)

PoE Usage Alarm Threshold (285 watts) (1-99%)

PoE Start Up Sequence

PoE Start Up Sequence Interval Secs (3-30)

PoE Start Up Sequence Option

PoE Setting(Port)

Quick Select

Select	Port	State	PoE Inline Mode	Powered Device Name	Priority	Budget	Schedule Action	Schedule Time Range	Re-enabled PoE Interval (Secs, 5-60)	Re-enabled
<input type="checkbox"/>	All	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="button" value="Re-enabled"/>
<input type="checkbox"/>	1	Enable <input type="text" value=""/>	Auto BT <input type="text" value=""/>	<input type="text" value=""/>	Low <input type="text" value=""/>	Auto <input type="text" value=""/>	PoE off <input type="text" value=""/>	<input type="text" value=""/>	10 <input type="text" value=""/>	<input type="button" value="Re-enabled"/>
<input type="checkbox"/>	2	Enable <input type="text" value=""/>	Auto BT <input type="text" value=""/>	<input type="text" value=""/>	Low <input type="text" value=""/>	Auto <input type="text" value=""/>	PoE off <input type="text" value=""/>	<input type="text" value=""/>	10 <input type="text" value=""/>	<input type="button" value="Re-enabled"/>
<input type="checkbox"/>	3	Enable <input type="text" value=""/>	Auto BT <input type="text" value=""/>	<input type="text" value=""/>	Low <input type="text" value=""/>	Auto <input type="text" value=""/>	PoE off <input type="text" value=""/>	<input type="text" value=""/>	10 <input type="text" value=""/>	<input type="button" value="Re-enabled"/>
<input type="checkbox"/>	4	Enable <input type="text" value=""/>	Auto BT <input type="text" value=""/>	<input type="text" value=""/>	Low <input type="text" value=""/>	Auto <input type="text" value=""/>	PoE off <input type="text" value=""/>	<input type="text" value=""/>	10 <input type="text" value=""/>	<input type="button" value="Re-enabled"/>

1. **PoE Setup:** Set up PoE-related attributes.

2. **PoE Status:** View the PoE information of the system and all ports.

4.12.1 PoE Setup

Click the option **PoE Setup** from the **Power over Ethernet** menu and then the following screen page appears.

Power over Ethernet » PoE Setup

Note !!
1. Once the specify PoE power in is force PoE inline mode, the PoE port will ignore the PoE classification behaviors and directly deliver power over RJ45 cable no matter what Ethernet device is attached, or even there is no Ethernet cable plugged.
2. Please be careful when using force PoE inline mode and make sure the remote device is PoE powered device (PD).
3. Re-enabled PoE Interval configuration and Re-enabled button only can configure and enabled when PoE inline mode is force mode.
4. Please set re-enabled PoE interval first when force PoE inline mode has issue and need to re-inject the force PoE power and need to and click Re-enabled button.

PoE

Disabled

Total PoE Budget

300

(0~300 watts)

PoE Usage Alarm Threshold (285 watts)

95

(1~99)%

PoE Start Up Sequence

Disabled

PoE Start Up Sequence Interval

3

Secs (3~30)

PoE Start Up Sequence Option

Port

PoE Setting(Port)

Quick Select 1,2,3-7 Select

Select	Port	State	PoE Inline Mode	Powered Device Name	Priority	Budget	Schedule Action	Schedule Time Range	Re-enabled PoE Interval (Secs, 5-60)	Re-enabled
<input type="checkbox"/>	All									Re-enabled
<input type="checkbox"/>	1	Enable	Auto BT		Low	Auto	PoE off		10	Re-enabled
<input type="checkbox"/>	2	Enable	Auto BT		Low	Auto	PoE off		10	Re-enabled
<input type="checkbox"/>	3	Enable	Auto BT		Low	Auto	PoE off		10	Re-enabled
<input type="checkbox"/>	4	Enable	Auto BT		Low	Auto	PoE off		10	Re-enabled

Ok Reset

PoE: Globally enable or disable PoE function.

Total PoE Budget: View-only field. It shows the total power budget in watt that Switch can provide.

PoE Usage Alarm Threshold: Set up the power usage alarm threshold in percentage. Valid range: 1~99%, and the default value is 95%. The value of the percentage that users entered will be converted to watts and displayed on the left.

PoE Start Up Sequence: Enable or disable the PoE start up sequence function.

PoE Start Up Sequence Interval: Enter the time interval in seconds for the PoE start up sequence.

PoE Start Up Sequence Option: Include **Port** and **Priority** options for the users to set up the PoE start up sequence function. Each option is described below.

Port: Each PoE port will be powered on in sequence according to port number.

Priority: Each PoE port will be powered on in sequence according to assigned port priority.

PoE Setting (Port): Configure PoE-related settings for each port.

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 PoE setting 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.

State: Configure the PoE status of specific port(s). Include **disable**, **enable** and **schedule** 3 options.

Disable: Disable PoE output for specific port(s).

Enable: Enable PoE output for specific port(s).

Schedule: Enable or disable PoE output for specific port according to **Schedule Action** and **Schedule Time Range**.

PoE Inline Mode: Configure the inline mode for a specific port. Include **Auto AF/AT**, **Auto BT**, **Fix** and **Force**. The default inline mode is **Auto BT**.

Auto AF/AT: Under the **Auto AF/AT** mode, the switch will detect the power level class of the connected device and automatically supply the proper power based on the power level class, up to a budget of 30 watts.

Auto BT: Under the **Auto BT** mode, the switch will detect the power level class of the connected device and automatically supply the proper power based on the power level class, up to a budget of 90 watts.

Fix: Under the **Fix** mode, the switch will detect whether the connected device features PoE functionality. If the device supports PoE, the switch will supply power based on the **Budget** that the user has entered. Otherwise, the switch will not supply power.

Force: Under the **Force** mode, the switch will not detect the connected device. Power will be supplied directly based on the **Budget** that the user has entered, even if the device is not a PD.

Powered Device Name: Specify a name for the PD connected to each TP port.

Priority: Assign the priority for the specified ports. If there is insufficient power supply, the power supplied to the TP port will be cut off based on the priority listed below.

Critical: Ports with this priority will be the last to have their power cut off.

High: Ports with this priority will have their power cut off after all ports assigned with the "Low" priority.

Low: Ports with this priority will be the first to have their power cut off.

NOTE: Power will be cut off upon the order of port number (Port4 → Port3 → Port2 → Port1) if ports are assigned with the same priority. For example, When Port2 and Port4 are both the low-priority ports, power supplied by Port4 will be cut off earlier than Port2.

Budget: The power budget for specified port. When PoE inline mode is set to Auto AF/AT or Auto BT, the column will display “Auto”. When the PoE inline mode is set to Fix or Force, users can enter a value from 1.0 to 90.0.

Schedule Action: The action to be performed during the assigned time range.

PoE off: Disable the PoE power supply during the assigned time range.

PoE on: Enable the PoE power supply during the assigned time range.

Schedule Time Range: Assign a time range to the PoE schedule. This defines which previously configured time interval the port should follow. Only one time interval can be applied at a time.

Re-enabled PoE Interval: Enter the time interval in seconds for the PoE Re-enabled function.

Re-enabled: Click “**Re-enabled**” to shut down the PoE power supply of assigned port, it will restart after the configured Re-enabled PoE interval

4.12.2 PoE Status

Click the option **PoE Status** from the **Power over Ethernet** menu and then the following screen page appears.

[Power over Ethernet](#) » PoE Status

Total PoE Budget 300 watts
Total PoE Power Consumption 0.0 watts (0.0%)

Refresh

Port	Powered Device Name	Connection Check	Channel	PoE Budget (W)	Power (W)	Voltage (V)	Current (mA)	Class	Link Status	PoE Inline	PoE Output Status
1		---	---	Auto	---	---	---	---	Down	Auto BT	Manual on
2		---	---	Auto	---	---	---	---	Down	Auto BT	Manual on
3		---	---	Auto	---	---	---	---	Up	Auto BT	Manual on
4		---	---	Auto	---	---	---	---	Down	Auto BT	Manual on

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

Port: View-only field that shows the port number of each PoE port.

Powered Device Name: View-only field that shows the Powered device name entered on the “PoE Setup” page

Connection Check: A view-only field that shows the result of connection check. The column will display **"2-pair," "Single PD,"** or **"Dual PD"** when connected to a device compliant with IEEE 802.3bt and the PoE inline mode is set to **Auto BT** or **Fix**. Otherwise, **"---**" will be displayed.

Channel: View-only field that shows the channel of Dual PD. The column will display **Primary** and **Secondary** when connected a Dual PD and the PoE inline mode is set to **Auto BT** or **Fix**. Otherwise, **"---**" will be displayed.

PoE Budget (W): A view-only field that shows the PoE budget set on the “PoE Setup” page for the specific port.

Power (W): A view-only field that shows the power in watts currently used on the specific port.

Voltage (V): A view-only field that shows the voltage currently used on the specific port.

Current (mA): A view-only field that shows the current in milliamperes currently used on the specific port.

Class: View-only field that shows the power level class of PD.

Link Status: View-only field that shows the current Ethernet network connection status of the specific port.

PoE Inline: View-only field that shows the current PoE Inline mode of the specific port.

PoE Output Status: View-only field that shows the current PoE output status. Each status is described below.

Overload: The power output of the port exceeds the PoE budget.

Searching: The power output of the port has been cut off, the port is not currently connected, or the port is recovering from “**Auto Off**” status.

Manual Off / Schedule Off: The power output has been turned off either due to the time range setting or because it was disabled manually.

Power Denied: The total PoE budget is insufficient, so the power output of the port has been denied.

Detection Fail: Includes situations such as unknown, short circuit, high capacitance, Rlow, Rhigh, open circuit, and FET failure.

Auto Off: The power output of the port has been shut down due to a protection mechanism, while the port remains connected. This status typically appears when the port is connected to a device that is not a PD.

OVLO: The voltage of the port has exceeded the voltage protection range, so the power output has been cut off.

UVLO: The voltage of the port has fallen below the voltage protection range, so the power output has been cut off.

Short: The port has a short circuit.

Thermal Shutdown: The temperature of the port is too high.

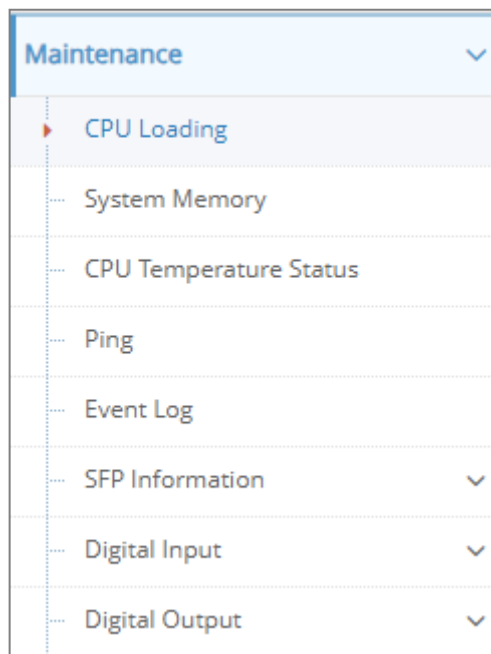
Inrush: The inrush current of the port is too high.

Manual On / Schedule On: The port is delivering power, the power output has been turned on either due to the time range setting or because it was enabled manually.

Request Power: A temporary status indicating that the chipset is still determining whether to deliver power.

4.13 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 8 options within this folder will be displayed for your selection.



1. **CPU Loading:** Manually or automatically update the current loading of CPU as well as the CPU loading record, and configure the CPU loading alarm notification.
2. **System Memory:** Manually or automatically update statistics of Memory and view them.
3. **CPU Temperature Status:** Manually or automatically update the current CPU temperature as well as the CPU temperature record, and configure the cpu-temperature alarm notification.
4. **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.
5. **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.
6. **SFP Information:** View the current port's SFP information, e.g. speed, Vendor ID, Vendor S/N, etc. SFP port state shows current DMI (Diagnostic monitoring interface) temperature, voltage, TX Bias, etc.
7. **Digital Input:** Set up the normal status of the digital input and view the status of digital input.
8. **Digital Output:** Set up the normal status of the digital output, enable or disable the event trigger and configure the output event.

4.13.1 CPU Loading

CPU Loading is to manually or automatically update the current loading of CPU as well as the CPU loading record, and configure the CPU loading alarm notification.

Select the option **CPU Loading** from the **Maintenance** menu and then the following screen page appears.

Maintenance » CPU Loading

Note:
1. Record Frequency of Averages: One entry per 5 seconds.
2. Avg. Record Start is a dynamic time point of the earliest value taken into account for calculating Averages
Since the maximum Averages period is 72 hours, Avg. Record Start will be updated correspondingly.

Refresh Page Interval Secs (1-300)

Notification

Notification

Threshold % (1-99)

Restore % (1-99)

Observation Interval Secs (5-86400)

CPU Statistics

Current (NTP Time)	Not Available
Current (Up Time)	0 day 00:08:35
CPU Loading (%)	29.29
Avg. Record Start (NTP Time)	Not Available
Avg. Record Start (Up Time)	0 day 00:00:22
1 Hour Averages (%)	--
24 Hours Averages (%)	--
72 Hours Averages (%)	--

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

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

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

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

Notification: Enable or disable the CPU loading alarm notification.

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

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

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

NOTE: When the alarm notification is enabled,

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

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

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

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

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

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

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

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

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

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

4.13.2 System Memory

System Memory is to manually or automatically update statistics of Memory.

Select the option **System Memory** from the **Maintenance** menu and then the following screen page appears.

Maintenance » System Memory	
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"/>	
Memory Statistics	
Current (NTP Time)	Not Available
Current (Up Time)	0 day 03:27:38
Total Memory (KByte)	57580
Memory Use (KByte)	26328
Memory Free (KByte)	31252

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

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

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

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

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

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

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

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

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

4.13.3 CPU Temperature Status

With the built-in temperature sensor, the Managed Switch is capable of detecting whether CPU temperature is at normal status or not. In addition, by the the notification via trap, syslog and event log, the user can realize the real-time CPU temperature to prevent the device's lifespan from being shorten due to the abnormal operation environment.

The alarm message will be sent in the event of abnormal situations, including CPU temperature is over the temperature threshold, CPU temperature exceeds the range of threshold (from 0 to 95 degrees centigrade), or the temperature sensor fails to detect CPU temperature. A normal message will also be sent to notify the user when CPU temperature higher the threshold returns to the normal status.

Select the option **CPU Temperature Status** from the **Maintenance** menu and then the following screen page appears.

Refresh Page Interval

Secs (1-300)

Start Auto Update

Stop Atuo Update

Update

Notification

High Temperature Threshold

Degrees C (0-95)

Threshold Interval

Secs (120-86400)

Continuous Alarm

CPU Temperature

CPU Temperature (Degrees C)		Elapsed Time
Current	58.5	--
Historical High	58.5	0 day 00:13:02
Historical Low	34.5	0 day 02:53:02

Ok

Reset

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

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

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

Update: Click **Update** to refresh the latest CPU temperature at a time.

High Temperature Threshold: Specify CPU temperature threshold. Valid range: 0~95 degrees centigrade.

If the detected CPU temperature is over the threshold you configure, the alarm message "CPU temperature is over threshold" will be sent based on the configuration in the following **Threshold Interval** and **Continuous Alarm** parameters.

NOTE: Any new changes done on this parameter will be taken effect immediately during the system execution, the temperature sensor will begin to check CPU temperature and decide whether to send the alarm/normal message or not upon the last status. Refer to Table 4-1.

<div>Last Status</div> <div>Detected Status</div>	Normal	Over the Threshold
Normal	No message will be sent.	Send the "CPU temperature is at or under threshold" normal message.
Over the Threshold	Send the "CPU temperature is over threshold" alarm message.	No message will be sent.

Table 4-1

Threshold Interval: Specify the time interval of sending cpu-temperature alarm message in seconds.

NOTE: Any new changes done on this parameter will be taken effect immediately during the system execution, the temperature sensor will begin to check CPU temperature and decide whether to send the alarm/normal message or not upon the last status. Refer to Table 4-2.

<div> <div>Last Status</div> <div>Detected Status</div> </div>	Normal	Over the Threshold
Normal	No message will be sent.	Send the “CPU temperature is at or under threshold” normal message.
Over the Threshold	Send the “CPU temperature is over threshold” alarm message.	Send the “CPU temperature is over threshold” alarm message.

Table 4-2

Continuous Alarm: Enable or disable the continuous alarm message sending function for CPU temperature of the system. Default is “Enabled”.

In case this function is enabled, the alarm message will be sent continuously upon the time interval configured in **Threshold Interval** parameter to notify the user once CPU temperature is at the abnormal status.

In case this function is disabled, the alarm message will be sent only one time to notify the user once CPU temperature is at the abnormal status.

Click **OK**, the new configuration will be taken effect immediately.

Current: Display CPU temperature currently detected by the temperature sensor. It will be shown in red color if the current CPU temperature is higher than the value you configured in the **High Temperature Threshold** parameter, or show “Failed” in red color if the temperature sensor fails.

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

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

Elapsed Time of Historical High: The period of time passed by since the highest CPU temperature has been reached.

Elapsed Time of Historical Low: The period of time passed by since the lowest CPU temperature has been reached.

4.13.4 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.

Ping IPv4/IPv6

192.168.0.1

Count

3

size

64

Start

Stop

Ping State

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.

4.13.5 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 main sections:

- Event Record:** Contains a dropdown menu currently set to 'Disabled' and an 'Ok' button.
- Display Sequence:** Contains a dropdown menu set to 'Newest to oldest', a 'Start from index' field with the value '500', a 'with' dropdown set to '500', and the text 'entries per page'. Below these are navigation buttons: 'First', 'Previous', 'Page 1' (dropdown), '/Page 1', 'Next', and 'Last'.
- Filter:** Contains several configuration options:
 - 'Time Policy' dropdown set to 'All Time'.
 - 'Time Range' dropdown set to 'Up Time'.
 - 'Item Policy' dropdown set to 'Display All'.
 - 'Item List' with a 'Select' button.
 - 'Item Selectd' set to 'None'.
 - 'Search' and 'Clear All' buttons at the bottom.

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.

Time Policy	Include ▾			
Time Range	Up Time ▾			
Start Day	0	Hour	00 ▾	: Minute 00 ▾
End Day	9999	Hour	23 ▾	: Minute 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.

Time Policy	Include ▾					
Time Range	NTP Time ▾					
Start Year	2021	Month	JAN ▾	Day	01 ▾	Hour 00 ▾ : Minute 00 ▾
End Year	2037	Month	DEC ▾	Day	31 ▾	Hour 23 ▾ : Minute 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. Auto backup failed	<input type="checkbox"/> 5. Auto backup succeeded	<input type="checkbox"/> 6. CLI disconnected
<input type="checkbox"/> 7. Cold start	<input type="checkbox"/> 8. CPU loading	<input type="checkbox"/> 9. CPU temperature failed
<input type="checkbox"/> 10. CPU temperature normal	<input type="checkbox"/> 11. CPU temperature overheat	<input type="checkbox"/> 12. Digital input abnormal
<input type="checkbox"/> 13. Digital input normal	<input type="checkbox"/> 14. Digital output abnormal	<input type="checkbox"/> 15. Digital output normal
<input type="checkbox"/> 16. Fast redundancy abnormal	<input type="checkbox"/> 17. Fast redundancy normal	<input type="checkbox"/> 18. Fast redundancy signal fail
<input type="checkbox"/> 19. Link down	<input type="checkbox"/> 20. Link up	<input type="checkbox"/> 21. Login
<input type="checkbox"/> 22. Login failed	<input type="checkbox"/> 23. Logout	<input type="checkbox"/> 24. Loop detection
<input type="checkbox"/> 25. Over PoE Port Budget	<input type="checkbox"/> 26. Over Total PoE Budget Threshold	<input type="checkbox"/> 27. PoE Port Power Off
<input type="checkbox"/> 28. To Denied PoE Port Power Output	<input type="checkbox"/> 29. Over Voltage And Protect PoE Port	<input type="checkbox"/> 30. Under Voltage And Protect PoE Port
<input type="checkbox"/> 31. PoE Port Short	<input type="checkbox"/> 32. PoE Port Thermal Shutdown	<input type="checkbox"/> 33. PoE Port Inrush
<input type="checkbox"/> 34. PoE Port Detection Fail	<input type="checkbox"/> 35. PoE Port Power On	<input type="checkbox"/> 36. PoE Port Power Setting
<input type="checkbox"/> 37. PoE Port Protection Mechanism	<input type="checkbox"/> 38. SFP RX power OK	<input type="checkbox"/> 39. SFP RX power overheat
<input type="checkbox"/> 40. SFP RX power too low	<input type="checkbox"/> 41. SFP temperature ok	<input type="checkbox"/> 42. SFP temperature overheat
<input type="checkbox"/> 43. SFP temperature too low	<input type="checkbox"/> 44. SFP TX power ok	<input type="checkbox"/> 45. SFP TX power overheat
<input type="checkbox"/> 46. SFP TX power too low	<input type="checkbox"/> 47. SFP voltage ok	<input type="checkbox"/> 48. SFP voltage overheat
<input type="checkbox"/> 49. SFP voltage too low	<input type="checkbox"/> 50. System voltage warning	<input type="checkbox"/> 51. Update failed
<input type="checkbox"/> 52. Warm start		

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.

4.13.6 SFP Information

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

Welcome: admin

QoS Setup

Multicast

Security Setup

LLDP

Power over Ethernet

Maintenance

CPU Loading

System Memory

CPU Temperature Status

Ping

Event Log

SFP Information

SFP Port Info

SFP Port State

SFP Port Threshold Configuration

Digital Input

Digital Output

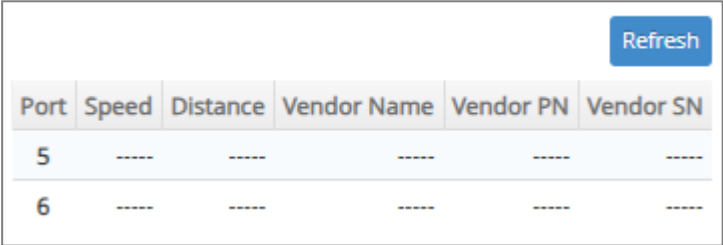
Maintenance » SFP Information > SFP Port Info

Refresh

Port	Speed	Distance	Vendor Name	Vendor PN	Vendor SN
5	----	----	----	----	----
6	----	----	----	----	----

4.13.6.1 SFP Port Info

SFP Port Info displays each port's slide-in SFP/SFP+ Transceiver information e.g. the speed of transmission, the distance of transmission, vendor Name, vendor PN, vendor SN, etc. The following screen page appears if you choose **SFP Port Info** function.



Port	Speed	Distance	Vendor Name	Vendor PN	Vendor SN
5	----	----	----	----	----
6	----	----	----	----	----

Refresh: Click **Refresh** to update the SFP Port Info status.

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

Speed: Data rate of the slide-in SFP/SFP+ Transceiver.

Distance: Transmission distance of the slide-in SFP/SFP+ Transceiver.

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

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

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

4.13.6.2 SFP Port State

SFP Port State displays each port's slide-in SFP/SFP+ Transceiver information e.g. the currently detected temperature, voltage, TX Bias, etc. The following screen page appears if you choose **SFP Port State** function.

						Refresh
Port	Temperature (Degree C)	Voltage (V)	Tx Bias (mA)	Tx Power (dBm)	Rx Power (dBm)	
5	----	----	----	----	----	
6	----	----	----	----	----	

Refresh: Click **Refresh** to update the SFP Port State status.

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

Temperature (Degree C): The operation temperature of slide-in SFP/SFP+ module currently detected.

Voltage (V): The operation voltage of slide-in SFP/SFP+ module currently detected.

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

TX Power (dBm): The optical transmission power of slide-in SFP/SFP+ module currently detected.

RX Power (dBm): The optical receiving power of slide-in SFP/SFP+ module currently detected.

4.13.6.3 SFP Port Threshold Configuration

SFP Port Threshold Configuration function not only displays all SFP ports' current temperature, voltage, current, TX power and RX power information but is capable of detecting whether these SFP ports are at normal status or not.

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

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

The following screen page appears if you choose **SFP Port Threshold Configuration** function.

Maintenance » SFP Information > SFP Port Threshold Configuration

SFP Threshold Enable

Disabled

Ok

Notification

Threshold Interval

600

Secs (120-86400)

Continuous Alarm

Enabled

Interval of Continuous Alarm

120

Secs (60-86400)

SFP Threshold

Display

All

Select	Port	Auto Detect	Current	Temperature Threshold (-40.0 - 120.0 °C)						Current	Voltage Threshold (2.60 - 4.00 V)						
				High			Low				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"/>	5	<input checked="" type="checkbox"/>	--	<input type="checkbox"/>	--	--	<input type="checkbox"/>	--	--	--	<input type="checkbox"/>	--	--	<input type="checkbox"/>	--	--	
<input type="checkbox"/>	6	<input checked="" type="checkbox"/>	--	<input type="checkbox"/>	--	--	<input type="checkbox"/>	--	--	--	<input type="checkbox"/>	--	--	<input type="checkbox"/>	--	--	

Ok

Reset

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

Threshold Interval for Notification: Specify the time interval of sending SFP ports' temperature/current/voltage/TX power/RX power alarm message in seconds. The interval can be set from 120 to 86400 seconds. The default setting is 600 seconds.

Continuous Alarm for Notification: Enable or disable the continuous alarm/warning message sending function for SFP ports' temperature/current/voltage/TX power/RX power. Default is "Enabled".

In case this function is enabled, the alarm/warning message will be sent continuously upon the time interval configured in **Threshold Interval** parameter to notify the user once SFP port's temperature/current/voltage/TX power/RX power is at the abnormal status.

In case this function is disabled, however, the alarm message will be sent only one time to notify the user once SFP port's temperature/current/voltage/TX power/RX power is at the abnormal status.

Interval of Continuous Alarm for Notification: Specify the time interval of sending the alarm message for SFP ports' temperature/current/voltage/TX power/RX power in seconds if the parameter of **Continuous Alarm** is enabled. The system will follow this specified time interval to continually send the alarm message (only for the monitored items of which the values exceed the thresholds) even if the monitored item's state remains as it was. Valid range is 60~86400 seconds. Default is "120" seconds.

Display: Select **All**, **Temperature**, **Voltage**, **Current**, **TX Power**, or **RX Power** from the pull-down menu to configure for the intended monitored item(s) altogether or individually.

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

Port: The number of the SFP port.

Auto Detect: Enable the Auto Detect mode by clicking on the checkbox. Unchecking the checkbox means the Manual mode is applied.

Auto Detection: Switch will auto detect alarm & warning threshold values if the SFP/SFP+ transceiver supports and follows the full SFF-8472. The SFP/SFP+ transceiver has default alarm and warning thresholds, which are fixed and cannot be changed.

Manual: Network manager can set alarm and warning threshold values manually when SFP/SFP+ transceiver doesn't support the full SFF-8472 or customer doesn't trust the threshold value from SFP/SFP+ transceiver (SFF-8472).

Current status of Temperature/Voltage/Current/TX power/RX power Threshold parameter: Display all SFP ports' temperature/Voltage/Current/TX power/RX power currently detected. It will be shown in red color if its current temperature/voltage/current/TX power/RX power is higher than the value in the **High** field or under the value in the **Low** field.

Enable in High & Low fields of Temperature/Voltage/Current/TX power/RX power Threshold parameter: Click on the checkbox of the corresponding port number to respectively enable the

configured threshold for the specific SFP port's alarm/warning notification of temperature /voltage/current/TX power/RX power.

High/Low Value of Temperature Threshold Alarm/Warning parameter: Specify SFP port's temperature Alarm/Warning threshold if the manual mode is applied. Valid range: -40.0 ~ 120.0 degrees centigrade. Default threshold value of Alarm is High: 70, Low: 0; default threshold value of Warning is High: 65, Low: 5.

High/Low Value of Voltage Threshold Alarm/Warning parameter: Specify SFP port's voltage Alarm/Warning threshold if the manual mode is applied. Valid range: 2.60 ~ 4.00 V. Default threshold value of Alarm is High: 3.6, Low: 3; default threshold value of Warning is High: 3.55, Low: 3.05.

High/Low Value of Current Threshold Alarm/Warning parameter: Specify SFP port's current Alarm/Warning threshold if the manual mode is applied. Valid range: 0.0 ~ 150.0 mA. Default threshold value of Alarm is High: 90, Low: 0.1; default threshold value of Warning is High: 80, Low: 0.3.

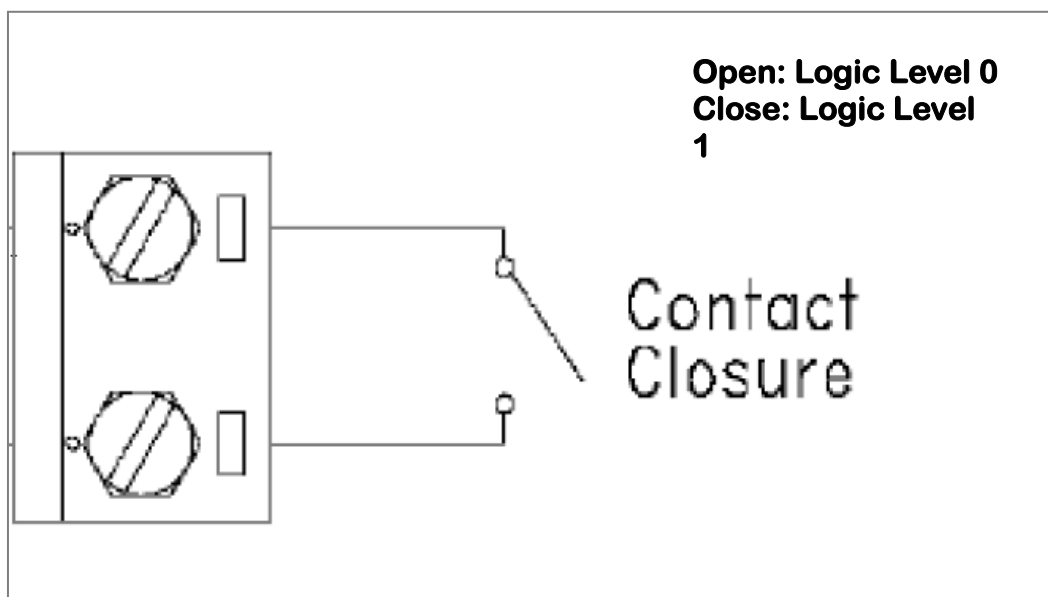
High/Low Value of TX Power Threshold Alarm/Warning parameter: Specify SFP port's TX power Alarm/Warning threshold if the manual mode is applied. Valid range: -30.0 ~ 10.0 dBm. Default threshold value of Alarm is High: 0, Low: -20; default threshold value of Warning is High: -1, Low: -19.

High/Low Value of RX Power Threshold Alarm/Warning parameter: Specify SFP port's RX power Alarm/Warning threshold. Valid range: -40.0 ~ 10.0 dBm. Default threshold value of Alarm is High: -5, Low: -25; default threshold value of Warning is High: -6, Low: -24.

Click **OK**, the new configuration will be taken effect immediately.

4.13.7 Digital Input

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



Select the option **Digital Input** from the **Maintenance** menu and then two functions, including Digital Input Config and Digital Input Status within this subfolder will be displayed.

4.13.7.1 Digital Input Configuration

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

Digital Input 1 Normal Status

Open ▼

Close

Open

Ok Reset

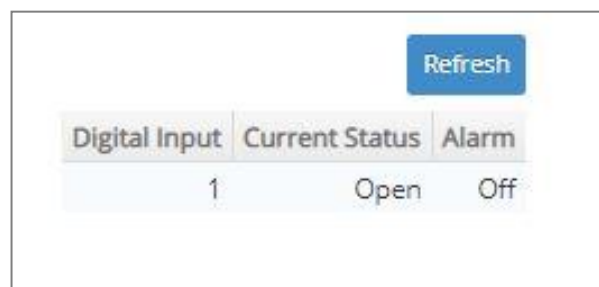
There is one Digital Input Normal Status option shown on the screen page. Normal Status refers to where the contact remains in one state unless actuated. The contact can either be normally open until closed by operation of the switch, or normally closed and opened by the switch action. You may choose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

NOTE: Digital Input event log can be seen both in the Event Log webpage under the Maintenance Menu and SNMP trap (Digital Input Start trap is enabled) if the alarm is activated.

Digital Input 1 Normal Status: Set up the normal status between “Open” or “Close” status for the digital input of the Managed Switch. Click **OK**, the new configuration will be taken effect immediately.

4.13.7.2 Digital Input Status

Select **Digital Input Status** from the **Digital Input** menu and then the following screen page appears.



The screenshot shows a web interface for 'Digital Input Status'. It features a table with three columns: 'Digital Input', 'Current Status', and 'Alarm'. The first row of the table contains the values '1', 'Open', and 'Off'. A blue 'Refresh' button is located in the top right corner of the interface.

Digital Input	Current Status	Alarm
1	Open	Off

Click **Refresh** to update the digital input and alarm status.

Current Status: View-only field that shows the current status of Digital Input 1.

Alarm: View-only field that shows the current alarm status.


4.13.8 Digital Output

Select the option **Digital Output** from the **Maintenance** menu and then two functions, including Digital Output Config and Digital Output Status within this subfolder will be displayed.


4.13.8.1 Digital Output Configuration

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

Digital Output	Config		Event				Action
	Normal	Event Trigger	Digital Input 1	Power 1	Power 2	Port Number	
1	Open	Disabled	Disabled	Disabled	Disabled	None	

Click the  icon in the **Action** field, the configuration section of Digital Output 1 will display on this webpage.

Digital Output 1

 Digital Output Config:

Normal Status

Open

Event Trigger

Disabled


Ok

Reset

Cancel

Normal Status: This is where the contacts remain in one state unless actuated by one of events listed in Digital Output Event. You may choose either Open or Close as normal status of electrical circuit by clicking the **Normal Status** pull-down menu.

Event Trigger: Enable or disable Event Trigger function of Digital Output. Click the **Event Trigger** pull-down menu and select “**Enabled**”, the following Digital Ouput Event list composed of four trigger events appears.

 Digital Output Event:

Digital Input-1

Disabled

Power 1

Disabled

Power 2

Disabled

Port Number

Select All

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6

Ok

Reset

Cancel

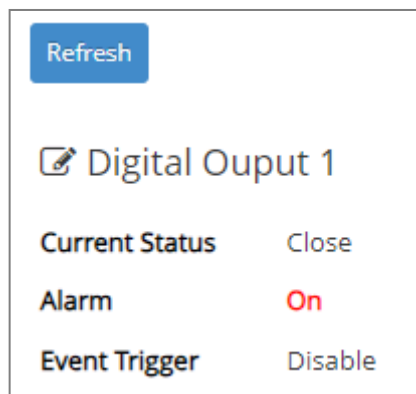
- **Digital Input-1:** Enable or disable the alarm transmission for Digital Input-1 previously mentioned in [Section 4.13.7.1](#).
- **Power 1:** Enable or disable the alarm transmission for Power 1.
- **Power 2:** Enable or disable the alarm transmission for Power 2.
- **Port Number:** Enable the alarm transmission by clicking the corresponding checkbox of Port Number or disable it by unchecking.

Click **OK**, the new settings will be taken effect immediately. Click **Cancel** to undo it, or click the **Reset** button to revert to the settings saved last time.

Digital Output Event	Alarm is triggered when...
Digital Input-1	Normal status and current status are different from each other.
Power 1	Power is disconnected.
Power 2	Power is disconnected.
Port Number	Any checked port is disconnected.
Note: Make sure that the designated event is enabled or checked before triggering alarm.	

4.13.8.2 Digital Output Status

Select **Digital Output Status** from the **Digital Output** menu and then the following screen page appears.



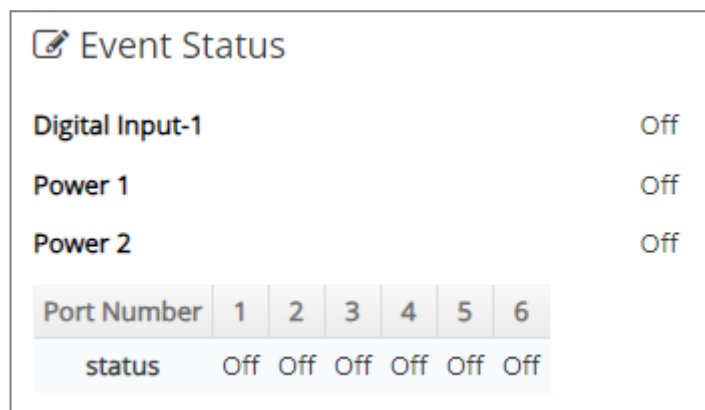
Refresh	
✎ Digital Ouput 1	
Current Status	Close
Alarm	On
Event Trigger	Disable

Click **Refresh** to update the digital Output and alarm status.

Current Status: View-only field that shows the current status of Digital Output 1.

Alarm: View-only field that shows the current alarm status.

Event Trigger: A view-only field that shows whether the Event Trigger function is enabled or disabled. When Event Trigger is enabled, the Event Status section will appear as follows.



✎ Event Status						
Digital Input-1	Off					
Power 1	Off					
Power 2	Off					
Port Number	1	2	3	4	5	6
status	Off	Off	Off	Off	Off	Off

Digital Input-1: A view-only field that shows whether the alarm for Digital Input-1 is triggered.

Power 1: A view-only field that shows whether the alarm for Power 1 is triggered.

Power 2: A view-only field that shows whether the alarm for Power 1 is triggered.

Port Number 1~6: A view-only field that shows whether the alarm for Port 1~6 is triggered.

4.14 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 10 options will be displayed for your selection.

Management » Management Access Setup

Telnet Service	Enabled
SSH Service	Disabled
SNMP Service	Enabled
Web Service	Http
Console Service	Enabled
Baud Rate	9600bps
Stop Bits	1
Parity Check	None
Word Length	8
Flow Control	None
Telnet Port	23 (1-65535)
CLI Time Out	1440 (1-1440) Unit Minutes
Web Time Out	1440 Mins (1-1440)
Console Login Fail Retry Times	3 Number of retries (1-10)
Console Login Fail Block Time	5 Mins (1-120)

Ok Reset

- 1. Management Access Setup:** Enable or disable the specified network services, view the RS-232 serial port setting, specific Telnet and Console services.
- 2. User Account:** View the registered user list, add a new user or remove an existing user.
- 3. RADIUS/TACACS+:** Set up the RADIUS/TACACS+ server authentication method against which a user accessing the Managed Switch can be authenticated.
- 4. Management Authentication:** Set up a planned authentication scheme to be accordingly applied by the Managed Switch authenticating a user's credentials.
- 5. SNMP:** Allow administrator to configure password and encryption method of user accounts generated in User Account for SNMPv3; view the registered SNMP community name list, add a new community name or remove an existing community name; view the registered SNMP trap destination list, add a new trap destination or remove an existing trap destination; view the Managed Switch trap configuration, enable or disable a specific trap.
- 6. Firmware Upgrade:** This allows users to update the latest firmware, save current configuration or restore previous configuration to the Managed Switch.
- 7. 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.

8. **Auto-Backup Setup:** Allows users to set up automatic backups for the managed switch settings.
9. **Save Configuration:** Save all changes to the system.
10. **Reset System:** Reset the Managed Switch.

4.14.1 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	Http	▼
Console Service	Enabled	▼
Baud Rate	9600bps	
Stop Bits	1	
Parity Check	None	
Word Length	8	
Flow Control	None	
Telnet Port	23	(1-65535)
CLI Time Out	1440	(1-1440)
Web Time Out	1440	Mins (1-1440)
Console Login Fail Retry Times	3	Number of retries (1-10)
Console Login Fail Block Time	5	Mins (1-120)

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. Either **Http** or **Https** option can be selected to enable this service. The difference between these two options is as follows:

- When the **Http** option is chosen, the user is allowed to access the Managed Switch only by inputting its IP address with the format of http://192.168.0.1 in URL.
- When the **Https** option is chosen, this communication protocol is encrypted using Transport Layer Security(TLS) or Secure Sockets Layer (SSL) for secure communication over a computer network.
- HTTPS is provided for authentication of the accessed website and protection of the privacy and integrity of the exchanged data while in transit. It protects against attacks by hackers. The user is allowed to access the Managed Switch either by inputting its IP address with

the format of https://192.168.0.1 or http://192.168.0.1 that will be automatically transferred into https://192.168.0.1 in URL.

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

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

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

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

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

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

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

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

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

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

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

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

4.14.2 User Account

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

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

The screenshot shows a web interface for managing user accounts. At the top, there is a section for 'Password Encryption' with a note about password changes and a dropdown menu currently set to 'Disabled'. Below this is the 'User Account' section, which includes a status indicator 'Occupied/Max Entry: 1/10' and two buttons: 'Add User Account' and 'Batch Delete'. A table lists the current user account, 'admin', with details on its state, privilege level, and actions for editing or deleting.

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.

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

AES-128 (Advanced Encryption Standard): An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data. Select “AES-128” from the pull-down menu to enable this password encryption method.

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

Occupied/Max Entry: View-only field.

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

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

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

Add New User Account

Account State Disabled ▾

User Name

Password

Retype Password

Description

Console Level Read Only ▾

Ok Cancel

Account State: Enable or disable this user account.

User Name: Specify the authorized user login name. Up to 32 alphanumeric characters can be accepted.

Password: Enter the desired user password. Up to 32 alphanumeric characters can be accepted.

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

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

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

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

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

Read Only: Allow to view only.

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

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

NOTE:

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

4.14.3 RADIUS/TACACS+

RADIUS and TACACS+ are namely two protocols used in the centralized management over the access into the network mainly for preventing the unauthorized connection, both working under the framework AAA (authentication, authorization, and accounting). The first “A” denotes that a RADIUS/TACACS+ client is required to transmit its username and its password for the authentication against the RADIUS/TACACS+ server. If the credentials are valid, the access-accept message will then be sent, and the client at this point will gain the approval of access into the Managed Switch, which in return delivers effective protection against unauthorized operation from malicious users.

To configure RADIUS/TACACS+, select the option **RADIUS/TACACS+** from the **Management** menu and then the following screen page shows up.

RADIUS

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 [Ok]

RADIUS Retry Times: 0 (0-3)

RADIUS Timeout: 3 Secs (1-3)

Index	Enable	Server IP	Server Port	Secret Key	Retype Secret Key
RADIUS 1	<input type="checkbox"/>	0.0.0.0	1812	***	***
RADIUS 2	<input type="checkbox"/>	0.0.0.0	1812	***	***

TACACS+

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 [Ok]

TACACS+ Retry Times: 0 (0-3)

TACACS+ Timeout: 3 Secs (1-3)

Index	Enable	Server IP	Server Port	Secret Key	Retype Secret Key
TACACS+ 1	<input type="checkbox"/>	0.0.0.0	49	***	***
TACACS+ 2	<input type="checkbox"/>	0.0.0.0	49	***	***

[Ok]

RADIUS: Configure the RADIUS server authentication method.

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

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

AES-128 (Advanced Encryption Standard): An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data. Select “AES-128” from the pull-down menu to enable the secret key encryption method.

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

2. RADIUS Timeout: The amount of time (second) that the Managed Switch will wait if the RADIUS server is not responding. Valid values are 1 through 3.

- 3. Index:** The entry of the RADIUS servers. Up to 2 servers can be configured as the RADIUS authentication server.
- 4. Enable:** Click the checkbox of the intended RADIUS server to enable RADIUS authentication. Once it's enabled, the user login will be upon those settings on the RADIUS server.
- 5. Server IP:** The IPv4/IPv6 address of the RADIUS server.
- 6. Server Port:** The RADIUS service port on the RADIUS server. Valid values are 1025 through 65535.
- 7. Secret Key:** The secret key for the RADIUS server; it is used to validate communications with the RADIUS server. Up to 32 alphanumeric characters can be set up.
- 8. Retype Secret Key:** Enter the secret key again for double-checking.

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

TACACS+: Configure the TACACS+ server authentication method.

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

None: Disable the secret key encryption function. Select "None" from the pull-down menu to disable it.

AES-128 (Advanced Encryption Standard): An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data. Select "AES-128" from the pull-down menu to enable the secret key encryption method.

- 1. TACACS+ Retry Times:** The maximum number of attempts to reconnect if the TACACS+ server is not reachable. Valid values are 0 through 3.
- 2. TACACS+ Timeout:** The amount of time (second) that the Managed Switch will wait if the TACACS+ server is not responding. Valid values are 1 through 3.
- 3. Index:** The entry of the TACACS+ servers. Up to 2 servers can be configured as the TACACS+ authentication server.
- 4. Enable:** Click the checkbox of the intended TACACS+ server to enable TACACS+ authentication. Once it's enabled, the user login will be upon those settings on the RADIUS server.
- 5. Server IP:** The IPv4/IPv6 address of the TACACS+ server.
- 6. Server Port:** The TACACS+ service port on the TACACS+ server. Valid values are 49, and 1025 through 65535.
- 7. Secret Key:** The secret key for the TACACS+ server; it is used to validate communications with the TACACS+ server. Up to 32 alphanumeric characters can be set up.
- 8. Retype Secret Key:** Enter the secret key again for double-checking.

4.14.4 Management Authentication

Management Authentication makes possible the versatile approaches to authentication on the Managed Switch. Network administrators can opt for multiple authentication methods and prioritize them in accordance with their most desired plan. This function brings not only enhanced flexibility to the authentication management, but also a smart countermeasure for an unexpected user authentication failure.

To configure the authentication method, select the option **Management Authentication** from the **Management** menu and then the following screen page shows up.

Service	Method 1	Method 2	Method 3	Method 4	Method 5
All	Local ▼	Disable ▼	Disable ▼	Disable ▼	Disable ▼
Telnet	Local ▼	Disable ▼	Disable ▼	Disable ▼	Disable ▼
SSH	Local ▼	Disable ▼	Disable ▼	Disable ▼	Disable ▼
Web	Local ▼	Disable ▼	Disable ▼	Disable ▼	Disable ▼
Console	Local ▼	Disable ▼	Disable ▼	Disable ▼	Disable ▼

Continue To Next Method When Authentication Fail Enabled ▼

Ok

Service: The interfaces via which the user accesses the Managed Switch, including **All**, **Telnet**, **SSH**, **Web** and **Console**.

All: Every user accessing the Managed Switch will be authenticated against the same authentication method scheme, regardless of the interface adopted by the user.

Method 1-5: Select **Local**, **RADIUS 1**, **RADIUS 2**, **TACACS+ 1**, **TACACS+ 2**, or **Disable** from each Method's pull-down menu to form a chain of authentication methods. However, **Local** must be set after **RADIUS** and **TACACS+** servers throughout the specified method scheme, and the 1st method cannot be configured as **Disable**.

Local: The user information stored in the Managed Switch against which the user will be authenticated when accessing the Managed Switch.

RADIUS 1/2: The RADIUS server against which the user will be authenticated when accessing the Managed Switch.

TACACS+ 1/2: The TACACS+ server against which the user will be authenticated when accessing the Managed Switch.

Continue To Next Method When Authentication Fail: Select **Enabled** or **Disabled** from the pull-down menu to enable or disable the function.

Note:

1. Once this function is enabled, the Managed Switch will continue to the next method if Method 1 fails, say, due to invalid client credentials. It indeed delivers extra flexibility for an

ought-to-be-authenticated user, yet at the expense of network security. To fully protect against malicious users, it's recommended to set this function disabled.

2. Disabling this function means the device will only apply Method 1. Access to the Managed Switch will be denied to those who fail the authentication with Method 1.

4.14.5 SNMP

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

4.14.5.1 SNMPv3 USM User

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


Note: The SNMPv3 user account is generated from “User Account”. (Refer to [Section 4.14.2](#))

Password Encryption

Disabled

Ok

Occupied/Max Entry: 1/10

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.

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

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

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

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

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

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

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

Retype Authentication-Password: Enter again the passwords specified in the **Authentication-Password** field.

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

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

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

AES-128 (Advanced Encryption Standard): An encryption algorithm uses key and block sizes of 128 bits to secure against malicious attacks on sensitive or private data. Select “AES-128” from the pull-down menu to enable it.

Private-Password: Specify the passwords if “DES” or “AES-128” is chosen. Up to 20 characters can be accepted.

Retype Private-Password: Enter again the passwords specified in the **Private-Password** field.

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.

4.14.5.2 Device Community

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

Occupied/Max Entry: 2/10

Add Device Community

Batch Delete

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.

Occupied/Max Entry: 2/10

Add Device Community

Batch Delete

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.

4.14.5.3 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	

Ok

Reset

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.

4.14.5.4 Trap Setup

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

Management » SNMP > Trap Setup	
Cold Start Trap	Enabled ▼
Warm Start Trap	Enabled ▼
Authentication Failure Trap	Enabled ▼
PoE Trap	Enabled ▼
Port Link Up/Down Trap	Enabled ▼
System Power Down Trap (1st Destination Only)	Enabled ▼
CPU Loading Trap	Enabled ▼
Digital I/O Start Trap	Enabled ▼
Auto Backup Trap	Enabled ▼
Console Port Link Up/Down Trap	Enabled ▼
CPU Temperature Trap	Enabled ▼
Fast Redundancy Trap	Enabled ▼
SFP Threshold Trap	Enabled ▼
<div>Ok Reset</div>	

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.

PoE Trap: Enable or disable the Managed Switch to send a trap when specified PoE events occur, such as system power exceeding the threshold or port power exceeding the budget.

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

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

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

Digital I/O Start Trap: Enable or disable the Managed Switch to send a trap when the status of digital input/output changes (e.g., alarm trigger or return to normal status).

Auto Backup Trap: Enable or disable the Managed Switch to send a trap whether the Auto Backup is successful or fail.

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

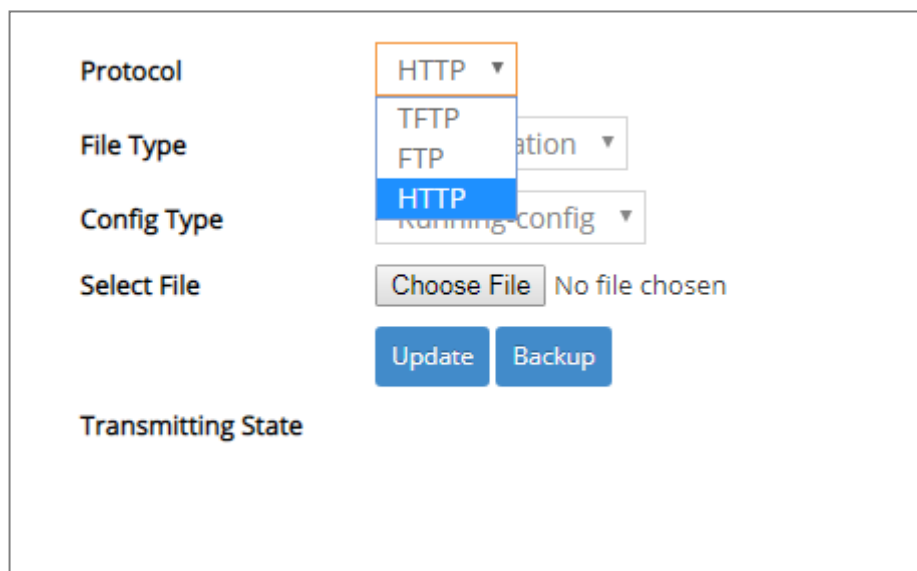
CPU Temperature Trap: Enable or disable the Managed Switch to send a trap when CPU temperature is over the parameter of **High Temperature Threshold** value, CPU temperature returns to the normal status (at or under the parameter of **High Temperature Threshold** value), CPU temperature exceeds the range of threshold (0~95 degrees centigrade), or the temperature sensor fails to detect CPU temperature.

Fast Redundancy Trap: Enable or disable Managed Switch to send a trap when any specified redundancy port in fast redundancy links up or links down.

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

4.14.6 Firmware Upgrade

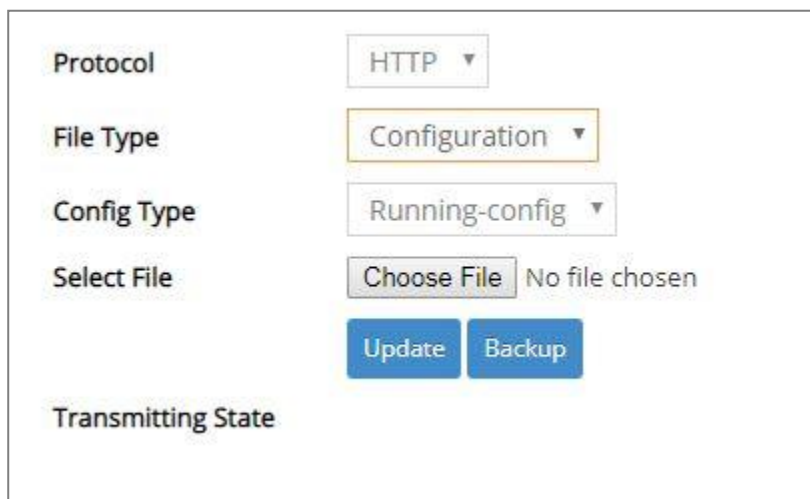
The Managed Switch offers three methods, including HTTP, FTP and TFTP to back up/restore the configuration and update the firmware. To do this, please select the option **Firmware Upgrade** from the **Management** menu and then the following screen page appears.



The screenshot shows a web interface for firmware upgrade. It includes a 'Protocol' dropdown menu which is open, showing options 'HTTP', 'TFTP', and 'FTP'. The 'HTTP' option is highlighted in blue. Other fields include 'File Type' (set to 'Configuration'), 'Config Type' (set to 'Running-config'), 'Select File' (with a 'Choose File' button and 'No file chosen' text), 'Update' and 'Backup' buttons, and a 'Transmitting State' label.

4.14.6.1 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.



This screenshot shows the same interface as the previous one, but with the 'File Type' dropdown set to 'Configuration' and the 'Config Type' dropdown set to 'Running-config'. The 'Protocol' remains 'HTTP'. The 'Update' and 'Backup' buttons are visible at the bottom.

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.

4.14.6.2 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.

Protocol	HTTP ▾
File Type	Firmware ▾
Upgrade Image Option	Image-2 ▾ (Current Boot Image: Image-1)
Select File	Choose File No file chosen
	<input type="button" value="Update"/>
Transmitting State	

Upgrade Image Option: Display the image that will be upgraded.

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

4.14.6.3 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 includes several dropdown menus and text input fields. The 'Protocol' dropdown is set to 'FTP'. The 'File Type' dropdown is set to 'Configuration'. The 'Config Type' dropdown is set to 'Running-config'. Below these are text input fields for 'Server IPv4/IPv6 Address', 'User Name', 'Password', and 'File Location'. At the bottom of the form are two blue buttons: 'Update' and 'Backup'. Below the buttons is a label 'Transmitting State'.

Protocol	FTP ▼
File Type	Configuration ▼
Config Type	Running-config ▼
Server IPv4/IPv6 Address	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password"/>
File Location	<input type="text"/>
<input type="button" value="Update"/> <input type="button" value="Backup"/>	
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.

4.14.6.4 Firmware Upgrade via FTP/TFTP

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

Protocol	<div>FTP ▾</div>
File Type	<div>Firmware ▾</div>
Upgrade Image Option	<div>Image-2 ▾ (Current Boot Image: Image-1)</div>
Server IPv4/IPv6 Address	<div></div>
User Name	<div></div>
Password	<div></div>
File Location	<div></div>
	<div>Update</div>
Transmitting State	

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

Upgrade Image Option: Display the image that will be upgraded.

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.

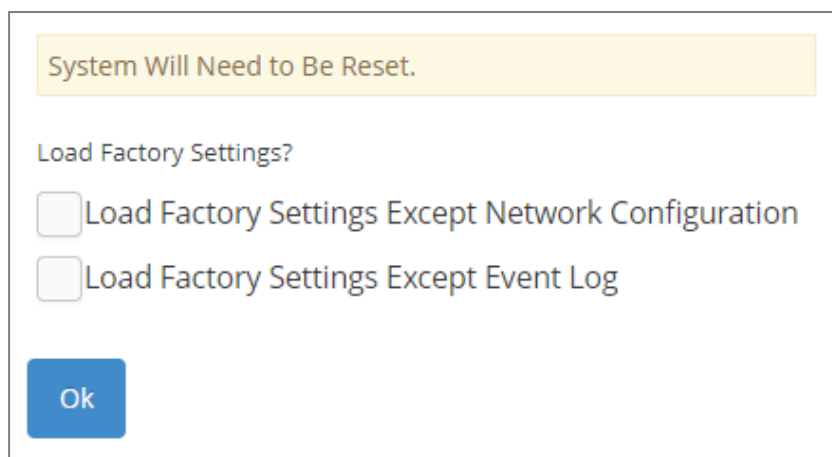
File Location: Enter the specific path and filename within the FTP/TFTP file server.

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.

4.14.7 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 checkboxes: the first is labeled "Load Factory Settings Except Network Configuration" and the second is labeled "Load Factory Settings Except Event Log". At the bottom left of the dialog box is a blue button labeled "Ok".

System Will Need to Be Reset.

Load Factory Settings?

☐ Load Factory Settings Except Network Configuration

☐ Load Factory Settings Except Event Log

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. (Refer to [Section 4.13.5](#) "Event Log" for the configuration of the Event Record function.)

Click **OK** to start loading factory settings. Or click the checkbox in front of **Load Factory Settings Except Network Configuration** and then click **OK** to start loading factory settings except network configuration.

4.14.8 Auto-Backup Setup

In the Managed Switch, the forementioned **HTTP Upgrade** and **FTP/TFTP Upgrade** functions are offered for the users to do the manual backup of the start-up configuration. Alternatively, you can choose the **Auto-Backup Setup** function to do this backup automatically and periodically. It is useful to prevent the loss of users' important configuration if they forget to do the backup, or help do the file comparison if any error occurs. Please note that the device's NTP function must be enabled as well in order to obtain the correct local time.

To initiate this function, please select **Auto-Backup Setup** from the **Management** menu, the following screen shows up.

The screenshot shows the 'Auto-Backup Setup' configuration page. At the top, the breadcrumb 'Management » Auto-Backup Setup' is visible. A light blue note box states: 'Note: In order for the Auto Backup function to work properly, the NTP function must be enabled for the device to acquire local time information.' Below this, the configuration fields are as follows:

NTP Status	Disable
Auto Backup	Disabled ▼
Backup Time	0 ▼ o'clock
Protocol	FTP ▼
File Type	Configuration
Server IPv4/IPv6 Address	0.0.0.0
User Name	anonymous
Password	
File Directory	/
File Name	
Backup State	

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

NTP Status: Display the current state of NTP server. Include Disable, Inactive and active 3 states.

Disable: NTP server is disabled.

Inactive: NTP server is enabled, but the Managed Switch does not obtain the local time from NTP server.

Active: NTP server is enabled, and the Managed Switch obtains the local time from NTP server.

Auto Backup: Enable/Disable the auto-backup function for the start-up configuration files of the device.

Backup Time: Set up the time when the backup of the start-up configuration files will start every day for the system.

Protocol: Either FTP or TFTP server can be selected to backup the start-up configuration files.

File Type: Display the type of files that will be backed up.

Server IPv4/IPv6 Address: Set up the IPv4/IPv6 address of FTP/TFTP server.

User Name and Password: Input the required username as well as password for authentication if FTP is chosen in the Protocol field.

File Directory: Assign the back-up path where the start-up configuration files will be placed on FTP or TFTP server.

File Name: The filename assigned to the auto- backup configuration files. The format of filename generated automatically is as follows:

ip address_Device Name_yyyyMMdd-HHmm.txt , for example, 192.168.0.3_SRS-3106_20240829-1600.txt

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

4.14.9 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.

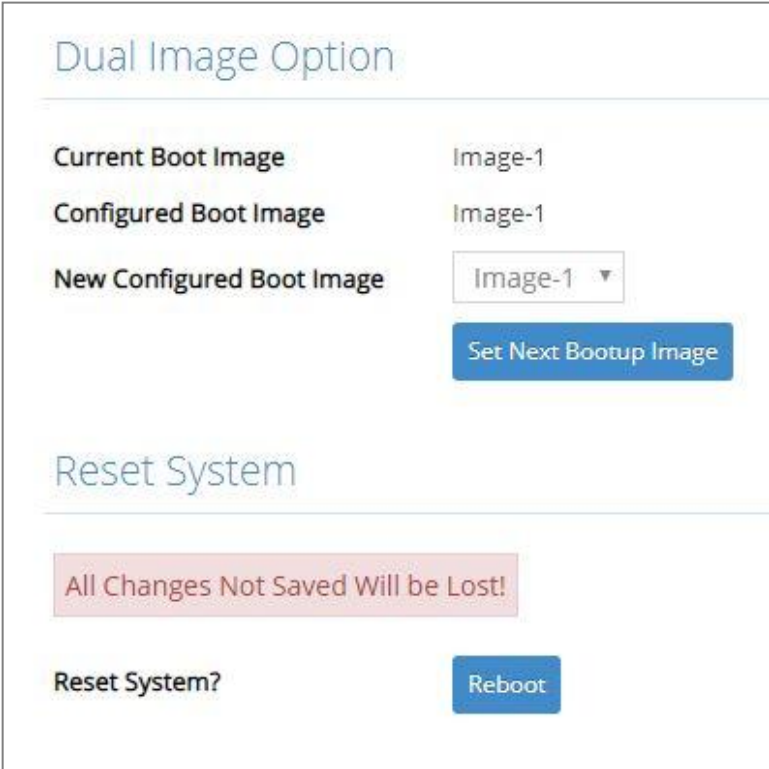


A dialog box with a white background and a thin grey border. It contains the text "Save All Changes to Flash?" in a standard black font. To the right of the text is a blue button with the word "Ok" in white.

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.

4.14.10 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 screen is divided into two main sections. The top section, titled "Dual Image Option", contains three labels on the left: "Current Boot Image", "Configured Boot Image", and "New Configured Boot Image". To the right of these labels are the values "Image-1", "Image-1", and a dropdown menu showing "Image-1" with a downward arrow. Below the dropdown is a blue button labeled "Set Next Bootup Image". The bottom section, titled "Reset System", features a red warning box with the text "All Changes Not Saved Will be Lost!". Below this is a label "Reset System?" and a blue button labeled "Reboot".

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-Jacobson-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

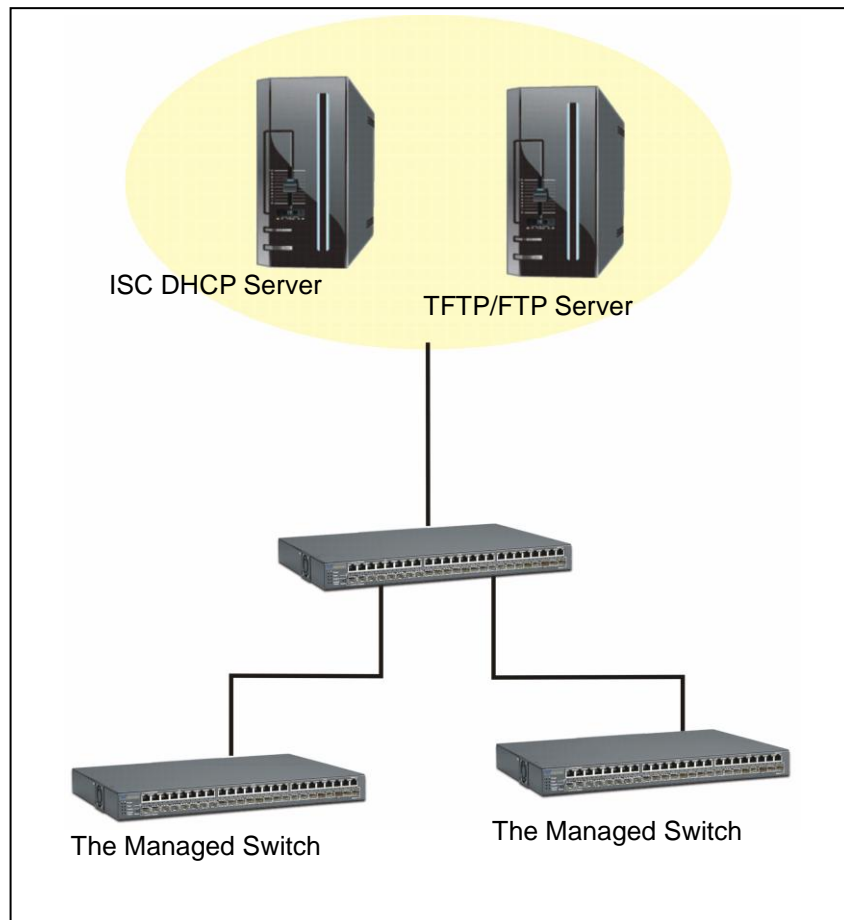
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the Managed Switch that you purchased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

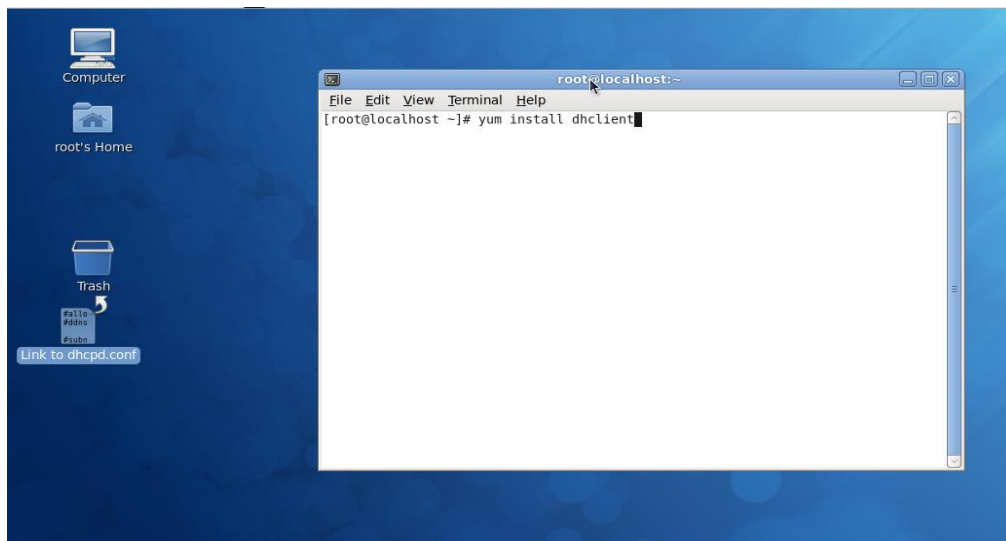
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Topology Example

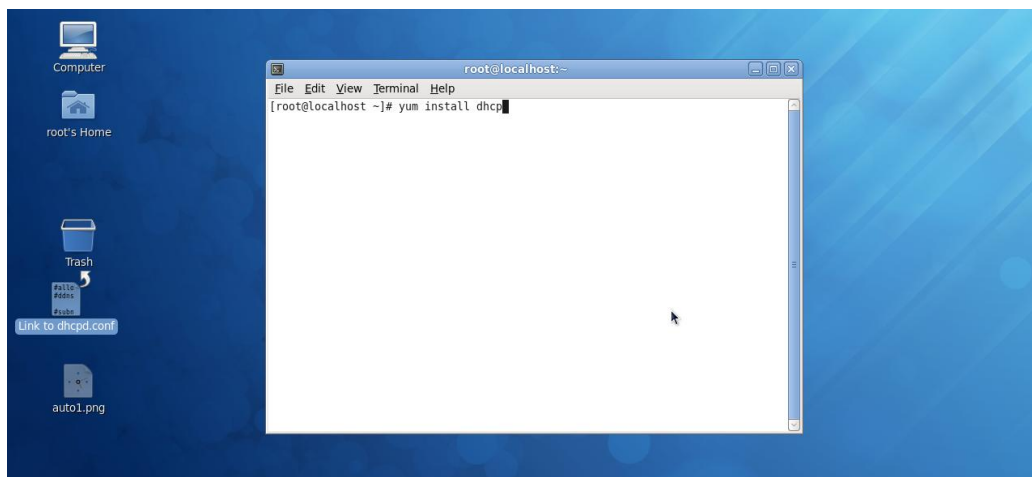
Step 2. Set up Auto Provision Server

● Update DHCP Client



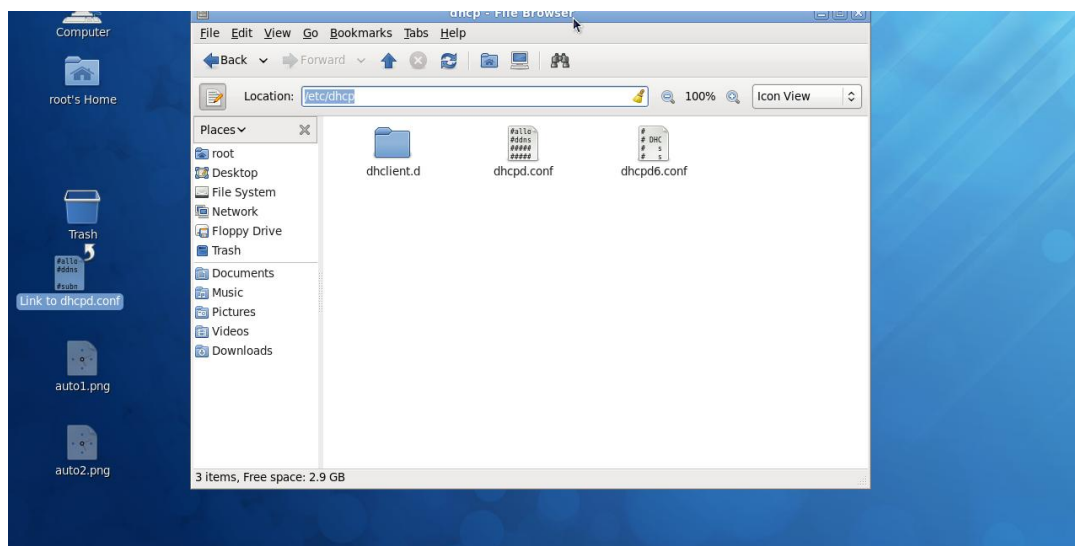
Linux Fedora 12 supports “yum” function by default. First of all, update DHCP client function by issuing “yum install dhclient” command.

● Install DHCP Server



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

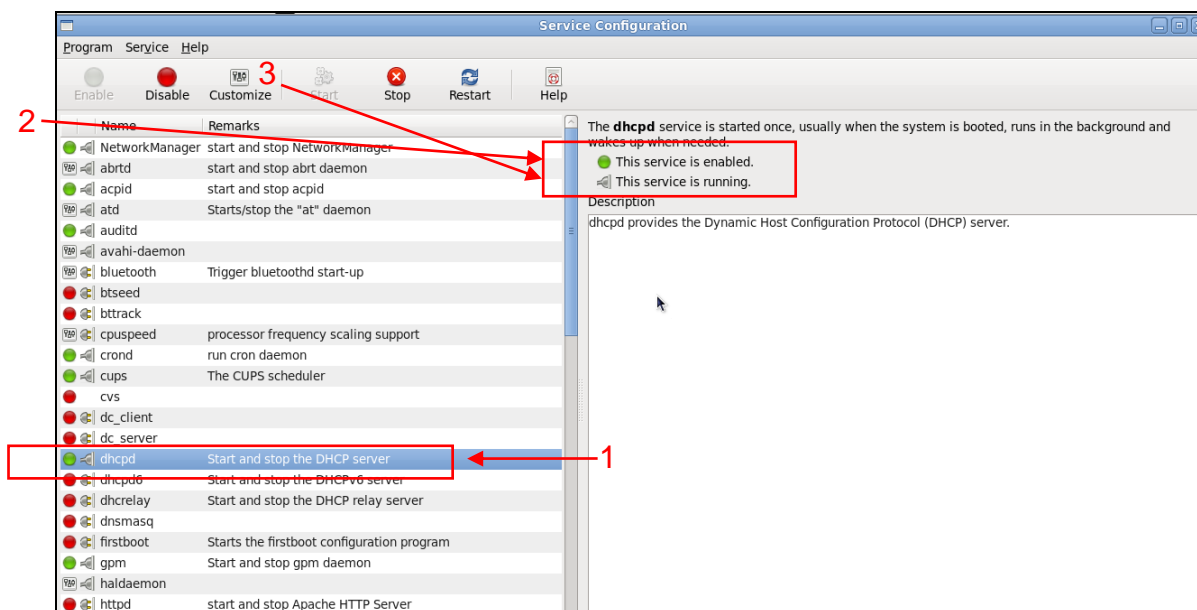
- **Copy dhcpd.conf to /etc/dhcp/ directory**



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

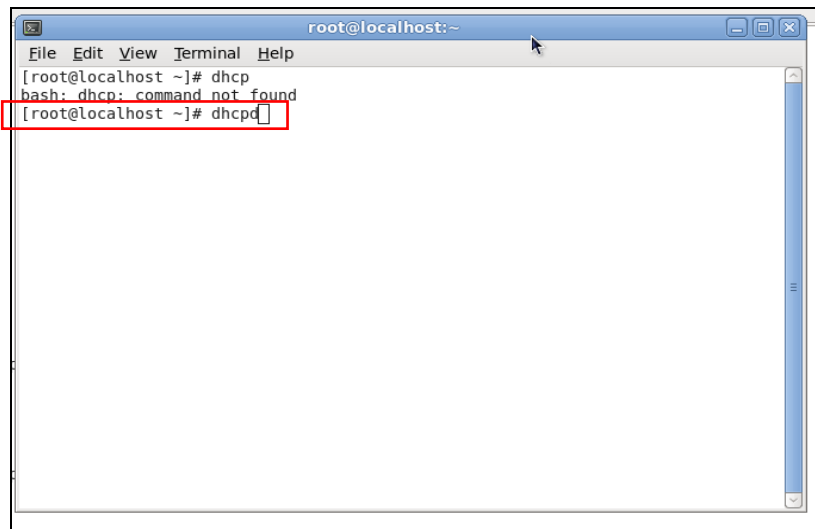
Please note that each vendor has their own way to define auto provisioning. Make sure to use the file provided by the vendor.

- **Enable and run DHCP service**



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

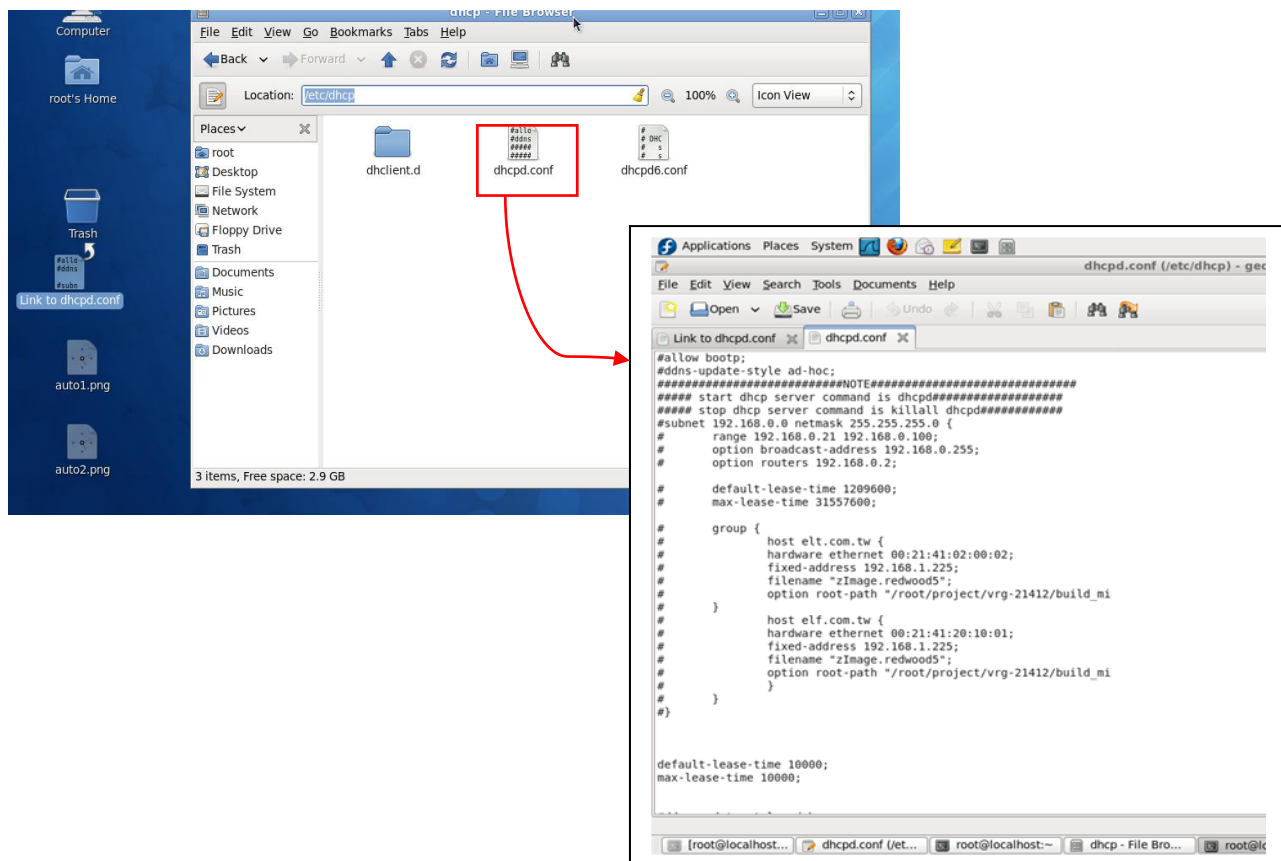
NOTE: DHCP service can also be enabled by CLI. Issue “dhcpd” command to enable DHCP service.



```
root@localhost:~  
File Edit View Terminal Help  
[root@localhost ~]# dhcp  
bash: dhcp: command not found  
[root@localhost ~]# dhcpd
```

Step 3. Modify dhcpd.conf file

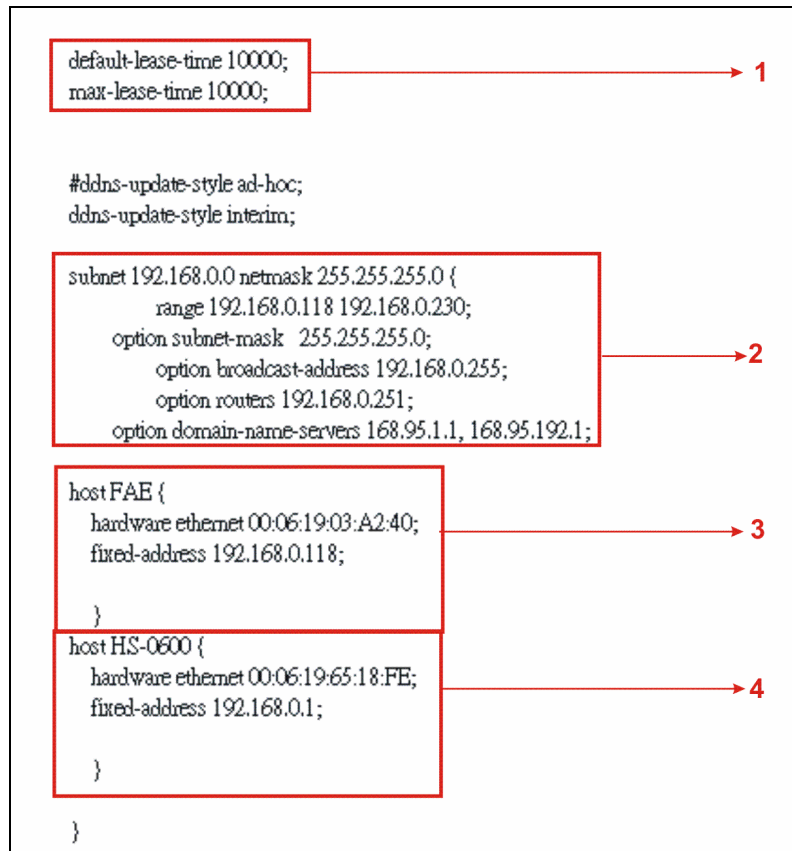
- Open dhcpd.conf file in /etc/dhcp/ directory



Double-click dhcpd.conf placed in /etc/dhcp/ directory to open it.

● Modify dhcpd.conf file

The following marked areas in dhcpd.conf file can be modified with values that work with your networking environment.

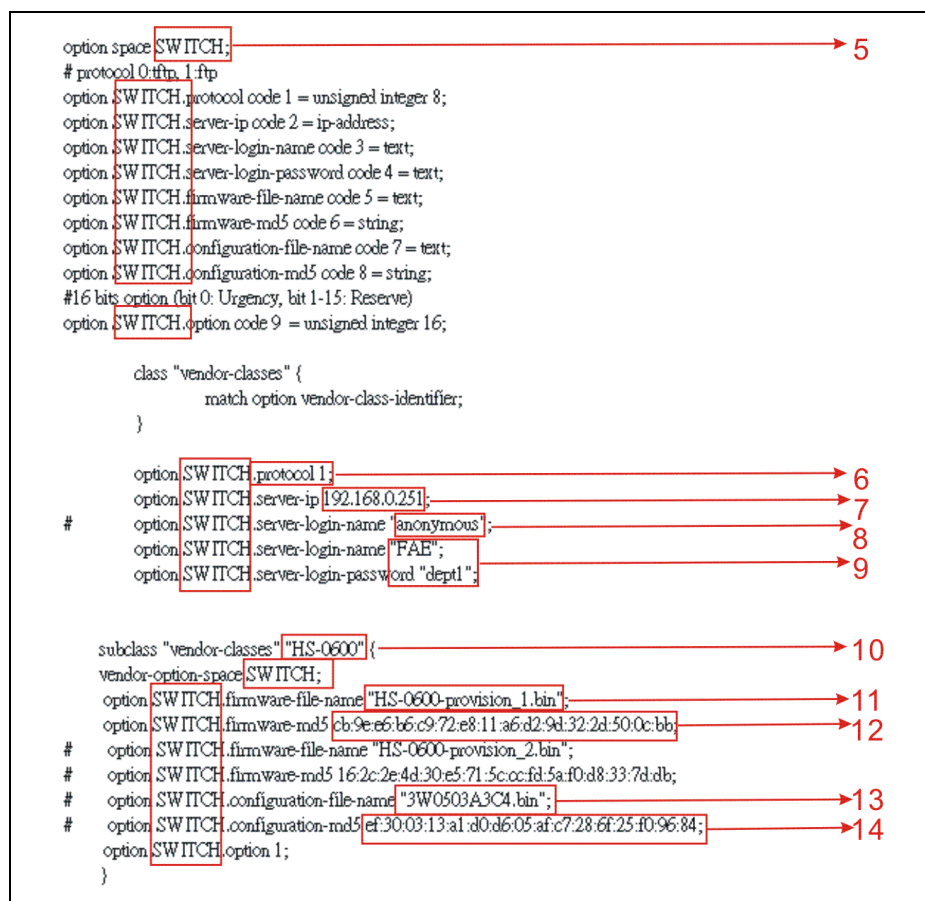


1. Define DHCP default and maximum lease time in seconds.

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

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

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



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

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

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

```
dhcpcd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Link to dhcpcd.conf x dhcpcd.conf x
option space SWITCH;
# protocol 0 tftp, 1 tftp;
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 c972e811a6d29d322d500cbb;
    # option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
    # option SWITCH.firmware-md5 162c2e4d30e5715cccf85af0d8337dab;
    # option SWITCH.configuration-file-name "3W0503A3C4 bin";
    # option SWITCH.configuration-md5 ef300313a1d0d605afc7286f25f09684;
    option SWITCH.option 1;
}

root@localhost:~# md5sum HS-0600-provision_2.bin
162c2e4d30e5715cccf85af0d8337dab HS-0600-provision_2.bin
root@localhost:~#
```

● Restart DHCP service

```
dhcpcd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Link to dhcpcd.conf x dhcpcd.conf x
option space SWITCH;
# protocol 0 tftp, 1 tftp;
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 c972e811a6d29d322d500cbb;
    # option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
    # option SWITCH.firmware-md5 162c2e4d30e5715cccf85af0d8337dab;
    # option SWITCH.configuration-file-name "3W0503A3C4 bin";
    # option SWITCH.configuration-md5 ef300313a1d0d605afc7286f25f09684;
    option SWITCH.option 1;
}

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:~#
```

```
dhcpcd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Link to dhcpcd.conf x dhcpcd.conf x
option space SWITCH;
# protocol 0 tftp, 1 tftp;
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 c972e811a6d29d322d500cbb;
    # option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
    # option SWITCH.firmware-md5 162c2e4d30e5715cccf85af0d8337dab;
    # option SWITCH.configuration-file-name "3W0503A3C4 bin";
    # option SWITCH.configuration-md5 ef300313a1d0d605afc7286f25f09684;
    option SWITCH.option 1;
}

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

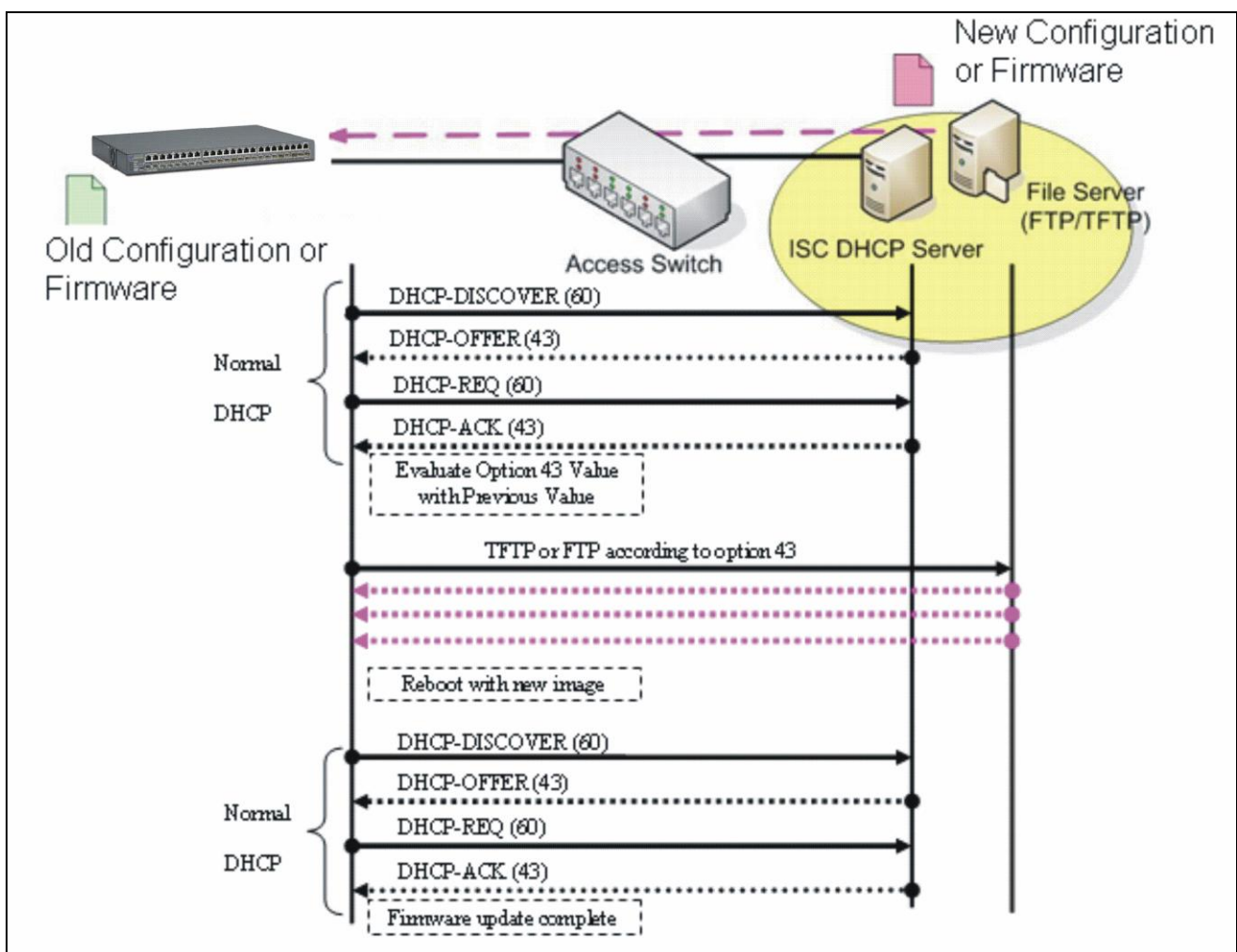
The TFTP/FTP File server should include the following items:

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.



APPENDIX C: VLAN Application Note

Overview

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

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

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

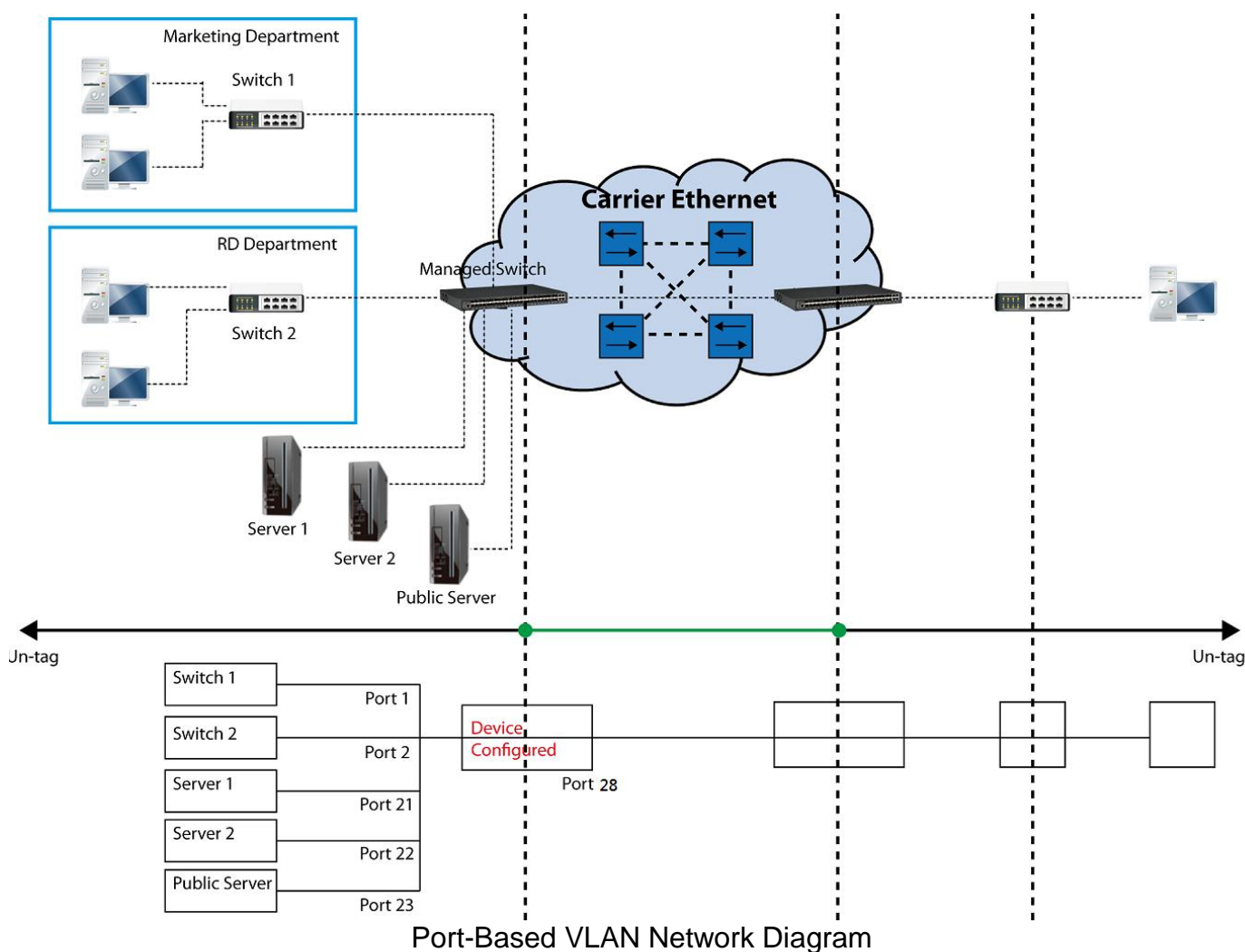
While this application note can not cover all of the real-life applications that are possible on this Managed Switch, it does provide the most common applications largely deployed in most situations. In particular, this application note provides a couple of network examples to help users implement Port-Based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

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

I. Port-Based VLAN

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

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



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

VLAN Name	Member ports
Marketing	1, 21, 23, 28
RD	2, 22, 23, 28

CLI Configuration:

Steps...	Commands...								
1. Enter Global Configuration mode.	Switch> enable Password: Switch#config Switch(config)#								
2. Create port-based VLANs “Marketing” and “RD”	Switch(config)# vlan port-based Marketing OK ! Switch(config)# vlan port-based RD OK !								
3. Select port 1, 21, 23 and 28 to configure.	Switch(config)# interface 1,21,23,28 Switch(config-if-1,21,23,28)#								
4. Assign the ports to the port-based VLAN “Marketing”.	Switch(config-if-1,21,23,28)# vlan port-based Marketing OK !								
5. Return to Global Configuration mode, and select port 2, 22, 23 and 28 to configure.	Switch(config-if-1,21,23,28)# exit Switch(config)# interface 2,22,23,28 Switch(config-if-2,22,23,28)#								
6. Assign the ports to the port-based VLAN “RD”.	Switch(config-if-2,22,23,28)# vlan port-based RD OK !								
7. Return to Global Configuration mode, and show currently configured port-based VLAN membership.	Switch(config-if-2,22,23,28)# exit Switch(config)# show vlan port-based When you enable Port Isolation, Port Based VLAN is automatically invalid. =====								
	Port Based VLAN : =====								
	<table> <thead> <tr> <th>Name</th><th>Port Member</th></tr> </thead> <tbody> <tr> <td>Default_VLAN</td><td>1-28,CPU</td></tr> <tr> <td>Marketing</td><td>1,21,23,28</td></tr> <tr> <td>RD</td><td>2,22,23,28</td></tr> </tbody> </table>	Name	Port Member	Default_VLAN	1-28,CPU	Marketing	1,21,23,28	RD	2,22,23,28
Name	Port Member								
Default_VLAN	1-28,CPU								
Marketing	1,21,23,28								
RD	2,22,23,28								
	<p><i>Note: By default, all ports are member ports of the Default_VLAN. Before removing the Default_VLAN from the VLAN table, make sure you have correct management VLAN and VLAN mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.</i></p>								

Web Management Configuration:

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

VLAN Setup > Port Based VLAN

The screenshot shows the web management interface. On the left, the 'VLAN Setup' menu is expanded, and 'Port Based VLAN' is selected. The main area displays the 'Port Based VLAN' configuration page. At the top, it shows 'Occupied/Max Entry: 1/28'. Below this is a table with 16 columns labeled 'Name' and '1' through '16'. The 'Name' column contains 'Default_VLAN' and the '1' column contains a checkmark. Below the table, there is a note: 'Note: When you enable Port Isolation, Port Based VLAN is automatic'.

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

Occupied/Max Entry: 1/28

[Add Port Based VLAN](#)
[Batch Delete](#)

Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	CPU	Action	
Default_VLAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

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

3. Add Port 1, 21, 23 and 28 in a group and name it to “Marketing”.
VLAN Setup>Port Based VLAN>Add Port Based VLAN

Occupied/Max Entry: 1/28

[Add Port Based VLAN](#)
[Batch Delete](#)

Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	CPU	Action	
Marketing	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Default_VLAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Click to apply the new settings when completing.

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

Occupied/Max Entry: 2/28

[Add Port Based VLAN](#)
[Batch Delete](#)

Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	CPU	Action	
Default_VLAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Marketing	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

5. Add Port 2, 22, 23 and 28 in a group and name it to “RD”.

VLAN Setup>Port Based VLAN>Add Port Based VLAN

Occupied/Max Entry: 2/28 Add Port Based VLAN Batch Delete

Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	CPU	Action
RD	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Default_VLAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Marketing	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Click  to apply the new settings when completing.

6. Check Port-Based VLAN settings.

VLAN Setup>Port Based VLAN

Occupied/Max Entry: 3/28 Add Port Based VLAN Batch Delete

Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	CPU	Action
Default_VLAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Marketing	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
RD	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

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

Treatments of packets:

1. A untagged packet arrives at Port 1

Untagged packets received on the Managed Switch will be forwarded out untagged. Therefore, in this example, the Managed Switch will look at the Port-Based forwarding table for Port 1 and forward untagged packets to member port 21, 23, and 28.

2. A untagged packet arrives at Port 2

Untagged packets received on the Managed Switch will be forwarded out untagged. Therefore, in this example, the Managed Switch will look at the Port-Based forwarding table for Port 2 and forward untagged packets to member port 22, 23, and 28.

3. A tagged packet with any permissible VID arrives at Port 1

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

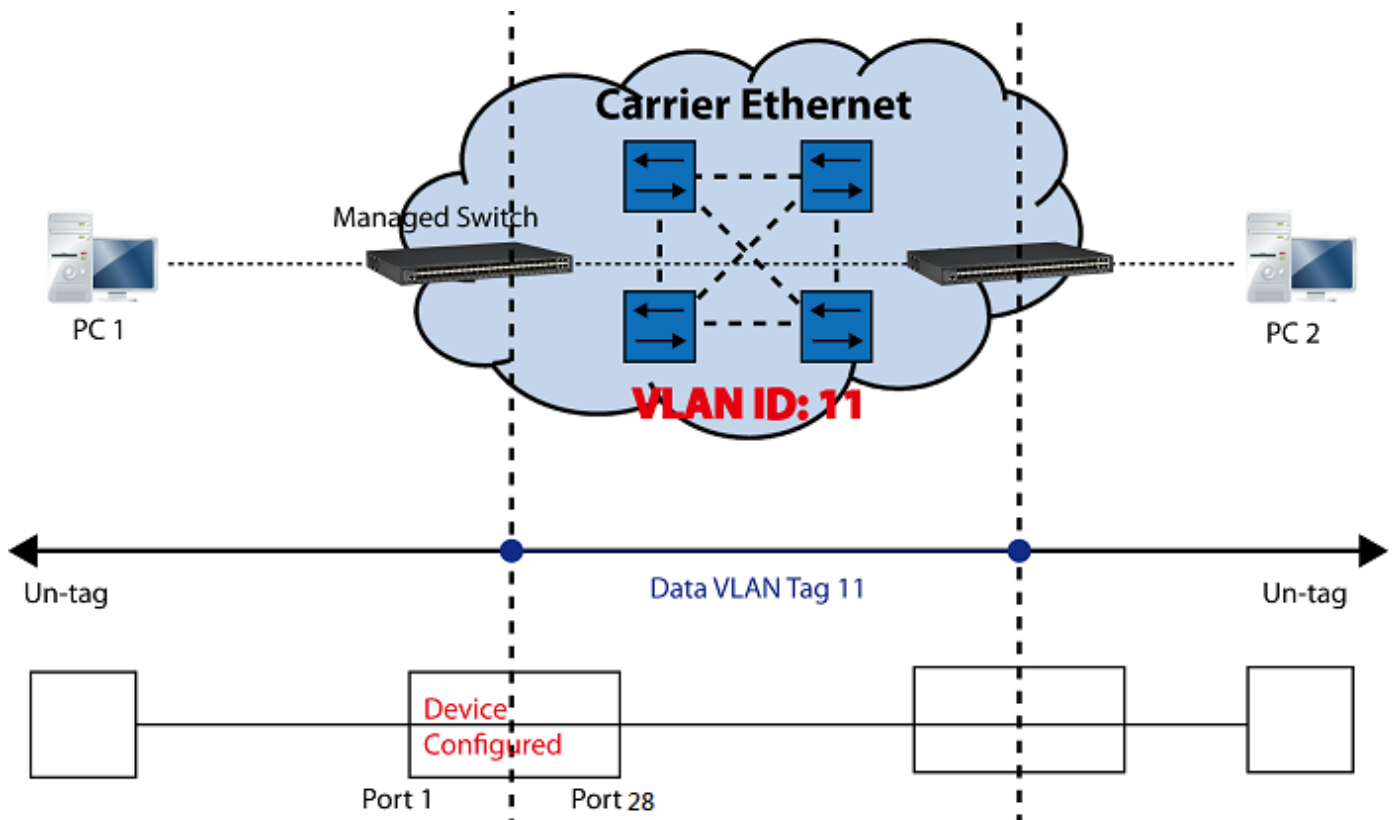
4. A tagged packet with any permissible VID arrives at Port 2

Tagged packets received on the Managed Switch will be forwarded out tagged. Therefore, in this example, the Managed Switch will look at the Port-Based forwarding table for Port 2 and forward tagged packets to member port 22, 23, and 28.

II. Data VLAN

In networking environment, VLANs can carry various types of network traffic. The most common network traffic carried in a VLAN could be voice-based traffic, management traffic and data traffic. In practice, it is common to separate voice and management traffic from data traffic such as files, emails. Data traffic only carries user-generated traffic which is sometimes referred to a user VLAN and usually untagged when received on the Managed Switch.

In the network diagram provided, it depicts a data VLAN network where PC1 wants to ping PC2 in a remote network. Thus, it sends out untagged packets to the Managed Switch to be routed in Carrier Ethernet. For this example, IEEE 802.1Q tagging mechanism can be used to forward data from the Managed Switch to the destination PC.



Data VLAN Network Diagram

CLI Configuration:

Steps...	Commands...
1. Enter Global Configuration mode.	Switch> enable Password: Switch#config Switch(config)#
2. Create VLAN 11 and assign Port 1 and Port 28 to VLAN 11.	Switch(config)# interface 1,28 Switch(config-if-1,28)# vlan dot1q-vlan trunk-vlan 11 OK ! Switch(config-if-1,28)# exit
3. Name VLAN 11 as "DataVLAN".	Switch(config)# vlan dot1q-vlan 11 Switch(config-vlan-11)# name DataVLAN OK ! Switch(config-vlan-11)# exit

4. Set Port 28 to trunk mode.	Switch(config)# interface 28 Switch(config-if-28)# vlan dot1q-vlan mode trunk OK ! Switch(config-if-28)# exit
5. Change Port 1's Access VLAN ID into "11".	Switch(config)# interface 1 Switch(config-if-1)# vlan dot1q-vlan pvid 11 OK ! Switch(config-if-1)# exit
6. Show currently configured VLAN tag settings.	Switch(config)# show vlan interface =====
	IEEE 802.1q Tag VLAN Interface =====
	CPU VLAN ID : 1 Dot1q-Tunnel EtherType : 0x9100
	Port P-Bit Port VLAN Mode PVID Trunk-vlan

	1 0 access 11 1,11
	2 0 access 1 1
	3 0 access 1 1.
	.
	26 0 access 1 1
	27 0 access 1 1
	28 0 trunk 1 1,11

Web Management Configuration:

1. Select "VLAN Interface" option in IEEE 802.1q Tag VLAN menu.

VLAN Setup>IEEE 802.1q Tag VLAN>VLAN Interface

The screenshot displays the Web Management Configuration interface. On the left, the 'VLAN Setup' menu is expanded, showing 'IEEE 802.1q Tag VLAN' and 'VLAN Interface' (highlighted with a red box). The main area shows a table for configuring VLANs.


Select	Port	Mode	PVID	Trunk-VLAN
<input type="checkbox"/>	All			
<input type="checkbox"/>	1	ACCESS	1	1
<input type="checkbox"/>	2	ACCESS	1	1
<input type="checkbox"/>	3	ACCESS	1	1
<input type="checkbox"/>	4	ACCESS	1	1
<input type="checkbox"/>	5	ACCESS	1	1
<input type="checkbox"/>	6	ACCESS	1	1
<input type="checkbox"/>	7	ACCESS	1	1
<input type="checkbox"/>	8	ACCESS	1	1

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

CPU VLAN ID	<input type="text" value="1"/>	(1-4094)
Dot1q-Tunnel EtherType	<input type="text" value="9100"/>	(0000-FFFF)

Select	Port	Mode	PVID	Trunk-VLAN
<input type="checkbox"/>	All			
<input type="checkbox"/>	1	ACCESS	1	<input type="text" value="1,11"/>
<input type="checkbox"/>	2	ACCESS	1	1
<input type="checkbox"/>	3	ACCESS	1	1
<input type="checkbox"/>	4	ACCESS	1	1
<input type="checkbox"/>	5	ACCESS	1	1
⋮				
<input type="checkbox"/>	25	ACCESS	1	1
<input type="checkbox"/>	26	ACCESS	1	1
<input type="checkbox"/>	27	ACCESS	1	1
<input type="checkbox"/>	28	TRUNK	1	<input type="text" value="1,11"/>

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

3. Click  icon belonging to the new Trunk VLAN 11 named VLAN0011, and the following screen shows up. Rename this new Trunk VLAN 11 as “DataVLAN” that includes Port 1 and 28 as member ports.
VLAN Setup>IEEE 802.1q Tag VLAN>Trunk VLAN Setup

Occupied/Max Entry: 2/2077
Add Trunk VLAN
Batch Delete

VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	CPU	Action
Default_VLAN	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	 	
DataVLAN	11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>	

Click  to apply the new settings when completing.


4. Check Trunk VLAN 11 settings.

VLAN Setup>IEEE 802.1q Tag VLAN>Trunk VLAN Setup

Occupied/Max Entry: 2/2077

Add Trunk VLAN

Batch Delete

VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	CPU	Action
Default_VLAN	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	 
DataVLAN	11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	 

5. Change Port 1's Access VLAN ID into 11, and set Port 28 to trunk mode.

VLAN Setup>IEEE 802.1q Tag VLAN>VLAN Interface

CPU VLAN ID	<input type="text" value="1"/>	(1-4094)		
Dot1q-Tunnel EtherType	<input type="text" value="9100"/>	(0000-FFFF)		
Select	Port	Mode	PVID	Trunk-VLAN
<input type="checkbox"/>	All			
<input type="checkbox"/>	1	ACCESS	<input type="text" value="11"/>	1,11
<input type="checkbox"/>	2	ACCESS	<input type="text" value="1"/>	1
<input type="checkbox"/>	3	ACCESS	<input type="text" value="1"/>	1
<input type="checkbox"/>	4	ACCESS	<input type="text" value="1"/>	1
<input type="checkbox"/>	5	ACCESS	<input type="text" value="1"/>	1

::
::

<input type="checkbox"/>	25	ACCESS	<input type="text" value="1"/>	<input type="text" value="1"/>
<input type="checkbox"/>	26	ACCESS	<input type="text" value="1"/>	<input type="text" value="1"/>
<input type="checkbox"/>	27	ACCESS	<input type="text" value="1"/>	<input type="text" value="1"/>
<input type="checkbox"/>	28	TRUNK	<input type="text" value="1"/>	<input type="text" value="1,11"/>

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

Treatments of Packets:

1. A untagged packet arrives at Port 1

When an untagged packet arrives at Port 1, Port 1's Port VLAN ID (11) will be added to the original port. Because Port 28 is configured as a trunk port, it will forward the packet with tag 11 out to the Carrier Ethernet.

2. A tagged packet arrives at Port 1

In most situations, data VLAN will receive untagged packets sent from the client PC or workstation. If tagged packets are received (possibly sent by malicious attackers), they will be dropped.

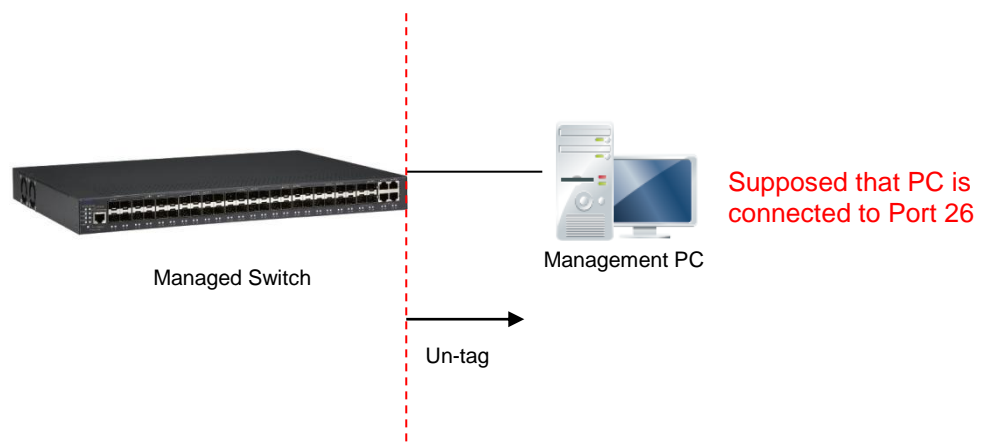
III. Management VLAN

For security and performance reasons, it is best to separate user traffic and management traffic. When Management VLAN is set up, only a host or hosts that is/are in this Management VLAN can manage the device; thus, broadcasts that the device receives or traffic (e.g. multicast) directed to the management port will be minimized.

Web Management Configuration (Access Mode):

Supposed that we have the default Management VLAN whose VLAN ID is 1 for all ports, we can create new Management VLANs as required. This example is to demonstrate how to set up Management VLAN from 15 to 20 on specified ports under Access mode.

In **Management VLAN Network Diagram**, the management PC on the right would like to manage the Managed Switch on the left directly. You can follow the steps described below to set up the Management VLAN.



Management VLAN Network Diagram

1. Change the Management default VLAN 1 into VLAN 15 that includes Port 25, 26, 27 and 28 under the Access mode.

VLAN Setup>IEEE 802.1q Tag VLAN>VLAN Interface

CPU VLAN ID: 15 (1-4094)

Dot1q-Tunnel EtherType: 8100 (0000-FFFF)

Select	Port	Mode	PVID	Trunk-VLAN
<input type="checkbox"/>	All			
<input type="checkbox"/>	1	ACCESS	1	1
<input type="checkbox"/>	2	ACCESS	1	1
<input type="checkbox"/>	3	ACCESS	1	1
<input type="checkbox"/>	4	ACCESS	1	1
<input type="checkbox"/>	5	ACCESS	1	1
<input type="checkbox"/>	6	ACCESS	1	1
<input type="checkbox"/>	7	ACCESS	1	1
<input type="checkbox"/>	8	ACCESS	1	1
<input type="checkbox"/>	9	ACCESS	1	1
<input type="checkbox"/>	10	ACCESS	1	1
<input type="checkbox"/>	11	ACCESS	1	1
<input type="checkbox"/>	12	ACCESS	1	1
<input type="checkbox"/>	13	ACCESS	1	1
<input type="checkbox"/>	14	ACCESS	1	1
<input type="checkbox"/>	15	ACCESS	1	1
<input type="checkbox"/>	16	ACCESS	1	1
<input type="checkbox"/>	17	ACCESS	1	1
<input type="checkbox"/>	18	ACCESS	1	1
<input type="checkbox"/>	19	ACCESS	1	1
<input type="checkbox"/>	20	ACCESS	1	1
<input type="checkbox"/>	21	ACCESS	1	1
<input type="checkbox"/>	22	ACCESS	1	1
<input type="checkbox"/>	23	ACCESS	1	1
<input type="checkbox"/>	24	ACCESS	1	1
<input type="checkbox"/>	25	ACCESS	15	1
<input type="checkbox"/>	26	ACCESS	15	1
<input type="checkbox"/>	27	ACCESS	15	1
<input type="checkbox"/>	28	ACCESS	15	1

Ok Reset

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

Note1: Make sure you have correct management VLAN and VLAN Mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you click **OK** to apply.

Note2: To check the current status of Management VLAN, please refer to **VLAN Table**.

VLAN Setup » IEEE 802.1q Tag VLAN > VLAN Table

Note:

When the VLAN of specified port has already changed VLAN by Server with 802.1x Assigned-VLAN feature, please check current assigned VLAN status on page 802.1X Setup > 802.1X Port Status.

U: Untagged T: Tagged D: Dot1q-Tunnel V: Member -: Not Member

VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	CPU
Default_VLAN	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	-	-	-	-	-
VLAN0015	15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	U	U	U	U	V

2. Now, change the Management VLAN 15 into VLAN 20 and includes Port 25, 26 and 27 under Access mode (It's necessary to include Port 26 to prevent the disconnection.)
VLAN Setup>IEEE 802.1q Tag VLAN>VLAN Interface

CPU VLAN ID		20	(1-4094)	
Dot1q-Tunnel EtherType		9100	(0000-FFFF)	
Select	Port	Mode	PVID	Trunk-VLAN
<input type="checkbox"/>	All	▼		
<input type="checkbox"/>	1	ACCESS ▼	1	1
<input type="checkbox"/>	2	ACCESS ▼	1	1
<input type="checkbox"/>	3	ACCESS ▼	1	1
<input type="checkbox"/>	4	ACCESS ▼	1	1
<input type="checkbox"/>	5	ACCESS ▼	1	1
<input type="checkbox"/>	6	ACCESS ▼	1	1
<input type="checkbox"/>	7	ACCESS ▼	1	1
<input type="checkbox"/>	8	ACCESS ▼	1	1
<input type="checkbox"/>	9	ACCESS ▼	1	1
<input type="checkbox"/>	10	ACCESS ▼	1	1
<input type="checkbox"/>	11	ACCESS ▼	1	1
<input type="checkbox"/>	12	ACCESS ▼	1	1
<input type="checkbox"/>	13	ACCESS ▼	1	1
<input type="checkbox"/>	14	ACCESS ▼	1	1
<input type="checkbox"/>	15	ACCESS ▼	1	1
<input type="checkbox"/>	16	ACCESS ▼	1	1
<input type="checkbox"/>	17	ACCESS ▼	1	1
<input type="checkbox"/>	18	ACCESS ▼	1	1
<input type="checkbox"/>	19	ACCESS ▼	1	1
<input type="checkbox"/>	20	ACCESS ▼	1	1
<input type="checkbox"/>	21	ACCESS ▼	1	1
<input type="checkbox"/>	22	ACCESS ▼	1	1
<input type="checkbox"/>	23	ACCESS ▼	1	1
<input type="checkbox"/>	24	ACCESS ▼	1	1
<input type="checkbox"/>	25	ACCESS ▼	20	1
<input type="checkbox"/>	26	ACCESS ▼	20	1
<input type="checkbox"/>	27	ACCESS ▼	20	1
<input type="checkbox"/>	28	ACCESS ▼	15	1
<div>Ok Reset</div>				

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

Note: To check the current status of Management VLAN, please refer to **VLAN Table**.

VLAN Setup » IEEE 802.1q Tag VLAN > VLAN Table

Note:

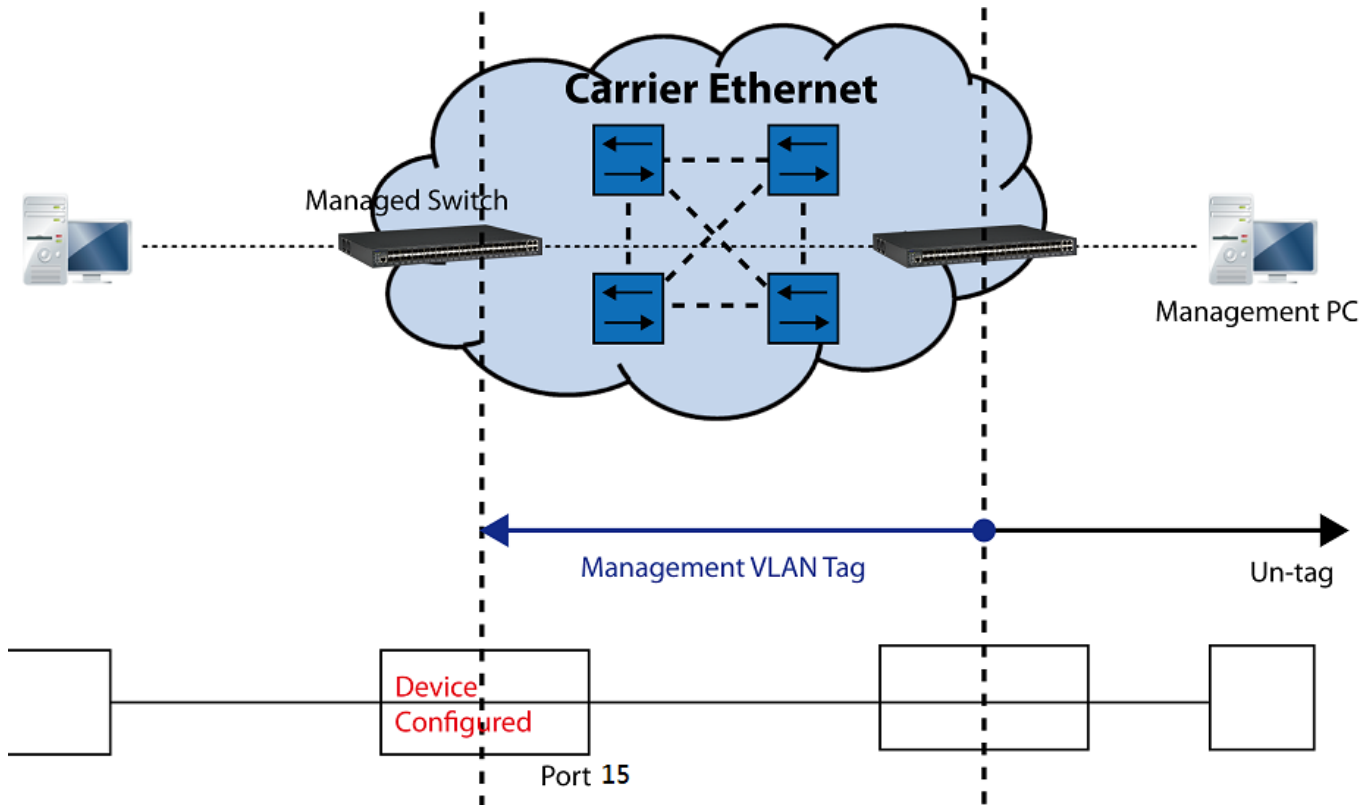
When the VLAN of specified port has already changed VLAN by Server with 802.1x Assigned-VLAN feature, please check current assigned VLAN status on page 802.1X Setup > 802.1X Port Status.

U: Untagged T: Tagged D: Dot1q-Tunnel V: Member -: Not Member

VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	CPU
Default_VLAN	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	-	-	-	-	-	
VLAN0015	15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	U	-
VLAN0020	20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	U	U	U	-	V

Web Management Configuration (Trunk Mode):

In **Management VLAN Network Diagram** shown below, the management PC on the right would like to manage the Managed Switch on the left remotely. You can follow the steps described below to set up the Management VLAN.



Management VLAN Network Diagram

Supposed that the Management PC is remotely connected to Managed Switch Port 15 as shown above while we have a variety of existing trunk vlan and the Management VLAN 15 is set on Port 25,26,27,28 and CPU as shown below. We can create new Management VLAN 20 as required. This part is to demonstrate how to set up from Management VLAN 15 to VLAN 20 on specified ports under Trunk mode.

VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	CPU
Default_VLAN	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	-	U	U	U	U	U	U	U	U	-	-	-	-	-	-
VLAN0015	15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	U	-	-	-	-	-	-	-	-	-	T	T	T	T	V

IEEE 802.1q Tag VLAN Table

1. Change the Management VLAN 15 into VLAN 20 that includes Port 25, 26, 27 under Trunk mode.

CPU VLAN ID: 20 (1-4094)

Dot1q-Tunnel EtherType: 8100 (0000-FFFF)

Select	Port	Mode	PVID	Trunk-VLAN
<input type="checkbox"/>	All			
<input type="checkbox"/>	1	ACCESS	1	1
<input type="checkbox"/>	2	ACCESS	1	1
<input type="checkbox"/>	3	ACCESS	1	1
<input type="checkbox"/>	4	ACCESS	1	1
<input type="checkbox"/>	5	ACCESS	1	1
<input type="checkbox"/>	6	ACCESS	1	1
<input type="checkbox"/>	7	ACCESS	1	1
<input type="checkbox"/>	8	ACCESS	1	1
<input type="checkbox"/>	9	ACCESS	1	1
<input type="checkbox"/>	10	ACCESS	1	1
<input type="checkbox"/>	11	ACCESS	1	1
<input type="checkbox"/>	12	ACCESS	1	1
<input type="checkbox"/>	13	ACCESS	1	1
<input type="checkbox"/>	14	ACCESS	1	1
<input type="checkbox"/>	15	ACCESS	20	1
<input type="checkbox"/>	16	ACCESS	1	1
<input type="checkbox"/>	17	ACCESS	1	1
<input type="checkbox"/>	18	ACCESS	1	1
<input type="checkbox"/>	19	ACCESS	1	1
<input type="checkbox"/>	20	ACCESS	1	1
<input type="checkbox"/>	21	ACCESS	1	1
<input type="checkbox"/>	22	ACCESS	1	1
<input type="checkbox"/>	23	ACCESS	1	1
<input type="checkbox"/>	24	ACCESS	1	1
<input type="checkbox"/>	25	TRUNK	1	20
<input type="checkbox"/>	26	TRUNK	1	20
<input type="checkbox"/>	27	TRUNK	1	20
<input type="checkbox"/>	28	TRUNK	1	15

Ok Reset

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

Note1: Make sure you have correct management VLAN and VLAN Mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you click **OK** to apply.

Note2: To check the current status of Management VLAN, please refer to **VLAN Table**.

Then, Management VLAN has been changed into VLAN 20.

VLAN Setup » IEEE 802.1q Tag VLAN > VLAN Table

Note:
When the VLAN of specified port has already changed VLAN by Server with 802.1x Assigned-VLAN feature, please check current assigned VLAN status on page 802.1X Setup > 802.1X Port Status.

U: Untagged T: Tagged D: Dot1q-Tunnel V: Member -: Not Member

VLAN Name	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	CPU
Default_VLAN	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	-	U	U	U	U	U	U	U	U	-	-	-	-	-	
VLAN0015	15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	T	-	
VLAN0020	20	-	-	-	-	-	-	-	-	-	-	-	-	-	U	-	-	-	-	-	-	-	-	-	T	T	T	-	V	

CLI Configuration (Access Mode):

Supposed that we have the default Management VLAN whose VLAN ID is 1 for all ports, we can create new Management VLANs as required. This example is to demonstrate how to set up Management VLAN 15 and then change VLAN 15 into VLAN 20 on specified ports under Access mode. Here, we supposed that the Management PC is remotely connected to Managed Switch Port 26.

1. Change the Management default VLAN 1 into VLAN 15 that includes Port 25, 26, 27 and 28 under Access mode.

Steps...	Commands...																																	
1. Enter Global Configuration mode.	Switch> enable Password: Switch# configure Switch(config)#																																	
2. Assign VLAN 15 to Management VLAN and Port 25-28 to Management port.	Switch(config)# vlan management-vlan 15 management-port 25-28 mode access OK ! NOTE: Make sure you have correct management VLAN and VLAN mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.																																	
3. Show currently configured dot1q settings and check CPU has been a member port in Management VLAN 15.	Switch(config)# show vlan =====	IEEE 802.1q VLAN Table =====	CPU VLAN ID : 15 Management Priority : 0 U: untagged port, T: tagged port, D: dot1q-tunnel port, V: member port	<table><tr><th>VLAN Name</th><th>VLAN</th><th>1</th><th>8</th><th>9</th><th>16</th><th>17</th><th>24</th><th>2528</th><th>CPU</th></tr><tr><td>Default_VLAN</td><td>1</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>-</td></tr><tr><td>VLAN0015</td><td>15</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>V</td></tr></table>	VLAN Name	VLAN	1	8	9	16	17	24	2528	CPU	Default_VLAN	1	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	-	VLAN0015	15	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	V
VLAN Name	VLAN	1	8	9	16	17	24	2528	CPU																									
Default_VLAN	1	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	-																									
VLAN0015	15	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	V																									

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

Steps...	Commands...																																								
1. Enter Global Configuration mode.	Switch> enable Password: Switch# configure Switch(config)#																																								
2. Assign VLAN 20 to Management VLAN and Port 25-27 to Management port.	Switch(config)# vlan management-vlan 20 management-port 25-27 mode access OK ! NOTE: Make sure you have correct management VLAN and VLAN mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.																																								
3. Show currently configured dot1q settings and check CPU has been a member port in Management VLAN 20.	Switch(config)# show vlan =====	IEEE 802.1q VLAN Table =====																																							
	CPU VLAN ID : 20 Management Priority : 0																																								
	U: untagged port, T: tagged port, D: dot1q-tunnel port, V: member port																																								
	=====																																								
	<table><tr><th>VLAN Name</th><th>VLAN</th><th>1</th><th>8</th><th>9</th><th>16</th><th>17</th><th>24</th><th>2528</th><th>CPU</th></tr><tr><td>Default_VLAN</td><td>1</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td></tr><tr><td>VLAN0015</td><td>15</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td></tr><tr><td>VLAN0020</td><td>20</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td><td>UUUUUUUU</td></tr></table>	VLAN Name	VLAN	1	8	9	16	17	24	2528	CPU	Default_VLAN	1	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	VLAN0015	15	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	VLAN0020	20	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU
VLAN Name	VLAN	1	8	9	16	17	24	2528	CPU																																
Default_VLAN	1	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU																																
VLAN0015	15	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU																																
VLAN0020	20	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU	UUUUUUUU																																

CLI Configuration(Trunk Mode):

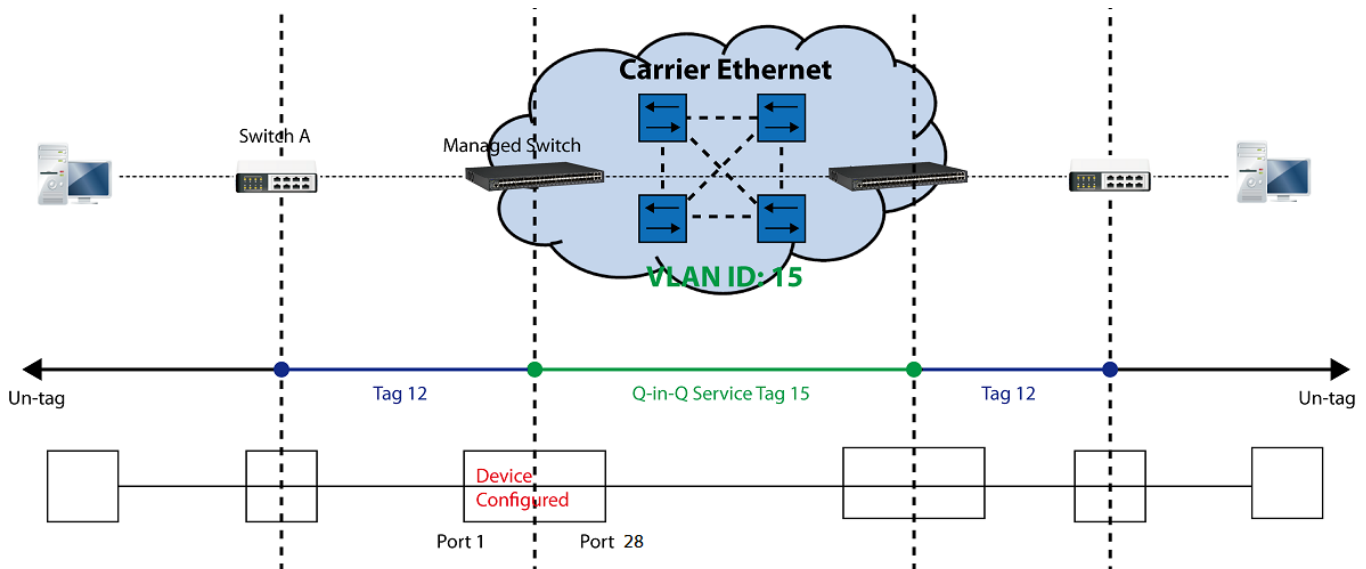
This part is to demonstrate how to change Management VLAN 15 into VLAN 20 on specified ports under Trunk mode. Supposed that we have the existing Management VLAN 15 on Port 25,26,27,28 and CPU, we can create new Management VLAN 20 as required. Here, we supposed that the Management PC is remotely connected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

1. Change the Management VLAN 15 into VLAN 20 that includes Port 25, 26, 27 under Trunk mode.

Steps...	Commands...																																								
1. Enter Global Configuration mode.	Switch> enable Password: Switch# configure Switch(config)#																																								
2. Assign VLAN 20 to Management VLAN and Port 15 to Management port for the access of the Managed Switch.	Switch(config)# vlan management-vlan 20 management-port 15 mode access OK ! NOTE: Make sure you have correct management VLAN and VLAN mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.																																								
3. Assign VLAN 20 to Management VLAN and Port 25-27 to Management port.	Switch(config)# vlan management-vlan 20 management-port 25-27 mode trunk OK ! NOTE: Make sure you have correct management VLAN and VLAN mode configurations, otherwise, incorrect configurations may disconnect your management PC to the Managed Switch immediately when you enter the command.																																								
4. Show currently configured dot1q settings and check CPU has been a member port in Management VLAN 20.	Switch(config)# show vlan ===== IEEE 802.1q VLAN Table ===== CPU VLAN ID : 20 Management Priority : 0 U: untagged port, T: tagged port, D: dot1q-tunnel port, V: member port <table><tr><th>VLAN Name</th><th>VLAN</th><th>1</th><th>8</th><th>9</th><th>16</th><th>17</th><th>24</th><th>2528</th><th>CPU</th></tr><tr><td>Default VLAN</td><td>1</td><td>UUUUUUUU</td><td>UUUUUUU-U</td><td>UUUUUUUU</td><td>----</td><td>-</td><td></td><td></td><td></td></tr><tr><td>VLAN0015</td><td>15</td><td>-----</td><td>-----</td><td>-----</td><td>---</td><td>T</td><td>-</td><td></td><td></td></tr><tr><td>VLAN0020</td><td>20</td><td>-----</td><td>-----</td><td>-U-</td><td>-----</td><td>TTT-</td><td>V</td><td></td><td></td></tr></table>	VLAN Name	VLAN	1	8	9	16	17	24	2528	CPU	Default VLAN	1	UUUUUUUU	UUUUUUU-U	UUUUUUUU	----	-				VLAN0015	15	-----	-----	-----	---	T	-			VLAN0020	20	-----	-----	-U-	-----	TTT-	V		
VLAN Name	VLAN	1	8	9	16	17	24	2528	CPU																																
Default VLAN	1	UUUUUUUU	UUUUUUU-U	UUUUUUUU	----	-																																			
VLAN0015	15	-----	-----	-----	---	T	-																																		
VLAN0020	20	-----	-----	-U-	-----	TTT-	V																																		

IV. Q-in-Q

The IEEE 802.1Q double tagging VLAN is also referred to Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1q VLAN space by tagging the inner tagged packets. In this way, a “double-tagged” frame is created so as to separate customer traffic within a service provider network. As shown below, the network diagram depicts the Switch A (on the left) carries a Customer tag 12. When tagged packets are received on the Managed Switch, they should be tagged with an outer Service Provider tag 15. To set up the network as provided, you can follow the steps described below.



Q-in-Q VLAN Network Diagram

CLI Configuration:

Steps...	Commands...
1. Enter Global Configuration mode.	<pre>Switch> enable Password: Switch#config Switch(config)#</pre>
2. Create S-Tag 15 on Port 1.	<pre>Switch(config)# interface 1 Switch(config-if-1)# vlan dot1q-vlan mode dot1q- tunnel OK ! Switch(config-if-1)# vlan dot1q-vlan pvid 15 OK ! Switch(config-if-1)# exit</pre>
3. Create Port 28 to trunk port with 15 VLAN ID.	<pre>Switch(config)# interface 28 Switch(config-if-28)# vlan dot1q-vlan mode trunk OK ! Switch(config-if-28)# vlan dot1q-vlan trunk-vlan 15 OK ! Switch(config-if-28)# no vlan dot1q-vlan trunk-vlan 1 OK ! Switch(config-if-28)# exit</pre>
4. Show currently configured dot1q VLAN membership.	<pre>Switch(config)# show vlan interface ===== IEEE 802.1q Tag VLAN Interface ===== CPU VLAN ID : 1 Dot1q-Tunnel EtherType : 0x9100 Port P-Bit Port VLAN Mode PVID Trunk-vlan ----- 1 0 dot1q tunnel 15 1</pre>

	2	0	access	1	1
	27	0	access	1	1
	28	0	trunk	1	15

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

Web Management Configuration:

1. Select “VLAN Interface” option in IEEE 802.1Q Tag VLAN menu.
VLAN Setup>IEEE 802.1q Tag VLAN>VLAN Interface

VLAN Setup » IEEE 802.1q Tag VLAN > VLAN Interface

CPU VLAN ID (1-4094)

Dot1q-Tunnel EtherType (0000-FFFF)

Select	Port	Mode	PVID	Trunk-VLAN
<input type="checkbox"/>	All			
<input type="checkbox"/>	1	DOT1Q-TUNNEL	15	1
<input type="checkbox"/>	2	ACCESS	1	1
⋮				
<input type="checkbox"/>	26	ACCESS	1	1
<input type="checkbox"/>	27	ACCESS	1	1
<input type="checkbox"/>	28	TRUNK	1	15

Check the VLAN status. Supposed that Port 1 carries dot1q-tunnel VLAN 15 while Port 28 trunk VLAN 15.

Treatments of Packets:

1. A tagged packet arrives at Port 1

When a packet with a tag 12 arrives at Port 1, the original tag will be kept intact and then added an outer tag 15 by Port 1, which is set as a tunnel port. When this packet is forwarded to Port 28, two tags will be forwarded out because Port 28 is set as a trunk port.

2. A untagged packet arrives at Port 1

If an untagged packet is received, it will also be added a tag 15. However, Q-in-Q function will not work.

APPENDIX D: SFP/SFP+ Port Threshold

Command & Configuration Guide

Version 1.0

Chapter 1. SFP/SFP+ Port Threshold

1.1 Introduction

The Managed Switch supports alarm and warning thresholds for temperature (degrees C), voltage (V), current (mA), TX power (dBm) and RX power (dbm) commands that is easy troubleshooting for network manager when SFP/SFP+ transceiver has issue or prevent issue in advance.

It supports two alarm and warning threshold method:

1. Auto Detection: Switch will auto detect alarm & warning threshold value if the SFP/SFP+ transceiver supports and follow the full SFF-8472. The SFP/SFP+ transceiver has default alarm and warning thresholds, which are fixed and cannot be changed.
2. Manual: network manager can set alarm and warning threshold value manually when SFP/SFP+ transceiver doesn't support the full SFF-8472 or customer doesn't trust the threshold value from SFP/SFP+ transceiver (SFF-8472).

When the temperature (degrees C), voltage (V), current (mA), TX power (dBm) or RX power (dbm) of SFP/SFP+ transceiver exceeds the alarm/warning threshold, an alarm or warning is generated, indicating that the SFP/SFP+ transceiver may be faulty, and switch will auto send message for network manager if network manager already enable SFP/SFP+ port threshold function. When message of alarm and warning threshold is generated, check the SFP/SFP+ transceiver, operating temperature and connected fibers first.

Chapter 2. Configuration Command

2.1 Configuring SFP/SFP+ Port Threshold Global Parameters

To configure the SFP/SFP+ port threshold global parameters, perform this task:

	Command or Action	Purpose
Step 1	Switch# configure	Enters global configuration mode.
Step 2	Switch (config)# sfp threshold	Enables global SFP threshold on the switch. The " no sfp threshold " command disables the global SFP threshold function.
Step 3	Switch (config)# sfp threshold notification continuous-alarm	Enables global notification continuous alarm of SFP threshold on the switch. The " no sfp threshold notification continuous-alarm " command disables the global notification continuous alarm of SFP threshold function. Default value is enabled.
Step 4	Switch (config)# sfp threshold notification continuous-alarm interval [60-86400]	(Optional) Configures specifies continuous alarm interval for notification. The " no sfp threshold notification continuous-alarm interval " command reset alarm interval time in default parameter, the default alarm interval time is 120 seconds.
Step 5	Switch (config)# sfp threshold notification interval [120-86400]	(Optional) Configures specifies interval for notification. The " no sfp threshold notification interval " command reset interval time in default parameter, the default interval time is 600 seconds.
Step 6	Switch (config)# exit	Returns to privileged EXEC mode.
Step 7	Switch# write	(Optional) Save the configuration.

This example shows how to enable global SFP threshold; and set specify notification continuous alarm interval and notification interval time:

```
Switch (config)# sfp threshold
Switch (config)# sfp threshold notification continuous-alarm
Switch (config)# sfp threshold notification continuous-alarm interval 100
Switch (config)# sfp threshold notification interval 180
Switch (config)# exit
Switch# write
```

2.2 Configuring Auto Detection SFP/SFP+ Port Threshold Interface Parameters

To configure the auto detection SFP/SFP+ port threshold parameters, perform this task:

	Command or Action	Purpose
Step 1	Switch# configure	Enters global configuration mode.
Step 2	Switch(config)# interface <i>interface-id</i>	Specifies the Layer 2 port to configure, and enters interface configuration mode.
Step 3	Switch (config-if-interface-id)# sfp threshold detect	(Optional) Enable auto detect alarm and warning threshold for specific port. Default value is enabled.
Step 4	Switch (config-if-interface-id)# sfp threshold current [<i>high</i> <i>low</i>]	Enable to check high/low current threshold for specific port. The “ no sfp threshold current [<i>high</i> <i>low</i>]” command reset high/low current threshold in default parameter.
Step 5	Switch (config-if-interface-id)# sfp threshold rx-power [<i>high</i> <i>low</i>]	Enable to check high/low RX power threshold for specific port. The “ no sfp threshold rx-power [<i>high</i> <i>low</i>]” command reset high/low RX power threshold in default parameter.
Step 6	Switch (config-if-interface-id)# sfp threshold temperature [<i>high</i> <i>low</i>]	Enable to check high/low temperature threshold for specific port. The “ no sfp threshold temperature [<i>high</i> <i>low</i>]” command reset high/low temperature threshold in default parameter.
Step 7	Switch (config-if-interface-id)# sfp threshold tx-power [<i>high</i> <i>low</i>]	Enable to check high/low TX power threshold for specific port. The “ no sfp threshold tx-power [<i>high</i> <i>low</i>]” command reset high/low TX power threshold in default parameter.
Step 8	Switch (config-if-interface-id)# sfp threshold voltage [<i>high</i> <i>low</i>]	Enable to check high/low voltage threshold for specific port. The “ no sfp threshold voltage [<i>high</i> <i>low</i>]” command reset high/low voltage threshold in default parameter.
Step 9	Switch (config-if-interface-id)# exit	Returns global configuration mode.
Step 10	Switch (config)# exit	Returns to privileged EXEC mode.
Step 11	Switch# write	(Optional) Save the configuration.

This example shows how to enable auto detection SFP threshold:

```
Switch (config)# interface 25-28
Switch (config-if-25-28)# sfp threshold detect
Switch (config-if-25-28)# sfp threshold current high
Switch (config-if-25-28)# sfp threshold current low
Switch (config-if-25-28)# sfp threshold rx-power high
Switch (config-if-25-28)# sfp threshold rx-power low
Switch (config-if-25-28)# sfp threshold temperature high
Switch (config-if-25-28)# sfp threshold temperature low
Switch (config-if-25-28)# sfp threshold tx-power high
Switch (config-if-25-28)# sfp threshold tx-power low
Switch (config-if-25-28)# sfp threshold voltage high
Switch (config-if-25-28)# sfp threshold voltage low
Switch (config-if-25-28)# exit
Switch (config)# exit
Switch# write
```

2.3 Configuring manual SFP/SFP+ Port Threshold Interface Parameters

To configure the manual SFP/SFP+ port threshold parameters, perform this task:

	Command or Action	Purpose
Step 1	Switch# configure	Enters global configuration mode.
Step 2	Switch(config)# interface <i>interface-id</i>	Specifies the Layer 2 port to configure, and enters interface configuration mode.
Step 3	Switch (config-if-interface-id)# no sfp threshold detect	Disable auto detect alarm and warning threshold for specific port.
Step 4	Switch (config-if-interface-id)# sfp threshold current [<i>high</i> <i>low</i>]	Enable to check high/low current threshold for specific port. The “ no sfp threshold current [<i>high</i> <i>low</i>]” command reset high/low current threshold in

		default parameter.
Step 5	Switch (config-if-interface-id)# sfp threshold current [high low] value [0-1500]	To set specific value for high/low alarm/warning current threshold for specific port. This command can set high/low alarm and warning current threshold at the same time; and use the same specific value, the value range is 0~1500 (Unit is 1/10mA). The “ no sfp threshold current [high low] value” command reset value for high/low alarm and warning current threshold in default parameter. Note: The value of low threshold cannot at or over high threshold.
Step 6	Switch (config-if-interface-id)# sfp threshold current [high low] value [alarm warning] [0-1500]	To set specific value for high/low alarm/warning current threshold for specific port. This command can set high/low alarm or warning current threshold, the value range is 0~1500 (Unit is 1/10mA). The “ no sfp threshold current [high low] value [alarm warning]” command reset value for high/low alarm or warning current threshold in default parameter. Note: 1. The value of low alarm threshold cannot over low warning threshold; 2. The value of low warning threshold cannot at or over high warning threshold; 3. The value of high warning threshold cannot over high alarm threshold. Please don't use step 5 and 6 at the same time.
Step 7	Switch (config-if-interface-id)# sfp threshold rx-power [high low]	Enable to check high/low RX power threshold for specific port. The “ no sfp threshold rx-power [high low]” command reset high/low RX power threshold in default parameter.
Step 8	Switch (config-if-interface-id)# sfp threshold rx-power [high low] value [-400~100]	To set specific value for high/low alarm/warning RX power threshold for specific port. This command can set high/low alarm and warning RX power threshold at the same time; and use the same specific value, the value range is -400~100 (Unit is 1/10dBm). The “ no sfp threshold rx-power [high low] value” command reset value for high/low alarm and warning RX power threshold in default parameter. Note: The value of low threshold cannot at or over high threshold.
Step 9	Switch (config-if-interface-id)# sfp threshold rx-power [high low] value [alarm warning] [-400~100]	To set specific value for high/low alarm/warning RX power threshold for specific port. This command can set high/low alarm or warning RX power threshold, the value range is -400~100 (Unit is 1/10dBm). The “ no sfp threshold rx-power [high low] value [alarm warning]” command reset value for high/low alarm or warning RX power threshold in default parameter. Note: 1. The value of low alarm threshold cannot over low warning threshold; 2. The value of low warning threshold cannot at or over high warning threshold; 3. The value of high warning threshold cannot over high alarm threshold. Please don't use step 8 and 9 at the same time.
Step 10	Switch (config-if-interface-id)# sfp threshold temperature [high low]	Enable to check high/low temperature threshold for specific port. The “ no sfp threshold temperature [high low]” command reset high/low temperature threshold in default parameter.
Step 11	Switch (config-if-interface-id)# sfp threshold temperature [high low] value [-400~1200]	To set specific value for high/low alarm/warning temperature threshold for specific port. This command can set high/low alarm and warning temperature threshold at the same time; and use the same specific value, the value range is -400~1200 (Unit is 1/10 degrees C). The “ no sfp threshold temperature [high low] value” command reset value for high/low alarm and warning temperature

		threshold in default parameter. Note: The value of low threshold cannot at or over high threshold.
Step 12	Switch (config-if-interface-id)# sfp threshold temperature [high low] value [alarm warning] [-400~1200]	To set specific value for high/low alarm/warning temperature threshold for specific port. This command can set high/low alarm or warning temperature threshold, the value range is -400~1200 (Unit is 1/10 degrees C). The “ no sfp threshold temperature [high low] value [alarm warning]” command reset value for high/low alarm or warning temperature threshold in default parameter. Note: 1. The value of low alarm threshold cannot over low warning threshold; 2. The value of low warning threshold cannot at or over high warning threshold; 3. The value of high warning threshold cannot over high alarm threshold. Please don't use step 11 and 12 at the same time.
Step 13	Switch (config-if-interface-id)# sfp threshold tx-power [high low]	Enable to check high/low TX power threshold for specific port. The “ no sfp threshold tx-power [high low]” command reset high/low tx-power threshold in default parameter.
Step 14	Switch (config-if-interface-id)# sfp threshold tx-power [high low] value [-300~100]	To set specific value for high/low alarm/warning TX power threshold for specific port. This command can set high/low alarm and warning TX power threshold at the same time; and use the same specific value, the value range is -300~100 (Unit is 1/10dBm). The “ no sfp threshold tx-power [high low] value ” command reset value for high/low alarm and warning tx-power threshold in default parameter. Note: The value of low threshold cannot at or over high threshold.
Step 15	Switch (config-if-interface-id)# sfp threshold tx-power [high low] value [alarm warning] [-300~100]	To set specific value for high/low alarm/warning TX power threshold for specific port. This command can set high/low alarm or warning TX power threshold, the value range is -300~100 (Unit is 1/10dBm). The “ no sfp threshold tx-power [high low] value [alarm warning]” command reset value for high/low alarm or warning tx-power threshold in default parameter. Note: 1. The value of low alarm threshold cannot over low warning threshold; 2. The value of low warning threshold cannot at or over high warning threshold; 3. The value of high warning threshold cannot over high alarm threshold. Please don't use step 14 and 15 at the same time.
Step 16	Switch (config-if-interface-id)# sfp threshold voltage [high low]	Enable to check high/low voltage threshold for specific port. The “ no sfp threshold voltage [high low]” command reset high/low voltage threshold in default parameter.
Step 17	Switch (config-if-interface-id)# sfp threshold voltage [high low] value [260~400]	To set specific value for high/low alarm/warning voltage threshold for specific port. This command can set high/low alarm and warning voltage threshold at the same time; and use the same specific value, the value range is 260~400 (Unit is 1/100V). The “ no sfp threshold t voltage [high low] value ” command reset value for high/low alarm and warning voltage threshold in default parameter. Note: The value of low threshold cannot at or over high threshold.
Step 18	Switch (config-if-interface-id)# sfp threshold voltage [high low] value [alarm warning] [260~400]	To set specific value for high/low alarm/warning voltage threshold for specific port. This command can set high/low alarm or warning voltage threshold, the value range is 260~400 (Unit is 1/100V). The “ no sfp threshold voltage [high low] value [alarm warning]” command reset value for high/low alarm or warning voltage threshold in default

	parameter. Note: 1. The value of low alarm threshold cannot over low warning threshold; 2. The value of low warning threshold cannot at or over high warning threshold; 3. The value of high warning threshold cannot over high alarm threshold. Please don't use step 14 and 15 at the same time.
Switch (config-if-interface-id)# exit	Returns global configuration mode.
Switch (config)# exit	Returns to privileged EXEC mode.
Switch# write	(Optional) Save the configuration.

This example shows how to enable manual SFP threshold parameters:

```
Switch (config)# interface 25-28
Switch (config-if-25-28)# no sfp threshold detect
Switch (config-if-25-28)# sfp threshold current high
Switch (config-if-25-28)# sfp threshold current high value alarm 1100
Switch (config-if-25-28)# sfp threshold current high value warning 900
Switch (config-if-25-28)# sfp threshold current low
Switch (config-if-25-28)# sfp threshold current low value alarm 50
Switch (config-if-25-28)# sfp threshold current low value warning 100
Switch (config-if-25-28)# sfp threshold rx-power high
Switch (config-if-25-28)# sfp threshold rx-power high value alarm -10
Switch (config-if-25-28)# sfp threshold rx-power high value warning -20
Switch (config-if-25-28)# sfp threshold rx-power low
Switch (config-if-25-28)# sfp threshold rx-power low value alarm -220
Switch (config-if-25-28)# sfp threshold rx-power low value warning -210
Switch (config-if-25-28)# sfp threshold temperature high
Switch (config-if-25-28)# sfp threshold temperature high value alarm 800
Switch (config-if-25-28)# sfp threshold temperature high value warning 750
Switch (config-if-25-28)# sfp threshold temperature low
Switch (config-if-25-28)# sfp threshold temperature low value alarm -150
Switch (config-if-25-28)# sfp threshold temperature low value warning -100
Switch (config-if-25-28)# sfp threshold tx-power high
Switch (config-if-25-28)# sfp threshold tx-power high value alarm -20
Switch (config-if-25-28)# sfp threshold tx-power high value warning -30
Switch (config-if-25-28)# sfp threshold tx-power low
Switch (config-if-25-28)# sfp threshold tx-power low value alarm -110
Switch (config-if-25-28)# sfp threshold tx-power low value warning -100
Switch (config-if-25-28)# sfp threshold voltage high
Switch (config-if-25-28)# sfp threshold voltage high value alarm 365
Switch (config-if-25-28)# sfp threshold voltage high value warning 350
Switch (config-if-25-28)# sfp threshold voltage low
Switch (config-if-25-28)# sfp threshold voltage low value alarm 310
Switch (config-if-25-28)# sfp threshold voltage low value warning 320
Switch (config-if-25-28)# exit
Switch (config)# exit
Switch# write
```

2.4 Configuring SNMP Trap for SFP/SFP+ Port Threshold Parameters

To configure the SNMP trap for SFP/SFP+ port threshold parameters, perform this task:

	Command or Action	Purpose
Step 1	Switch# configure	Enters global configuration mode.
Step 2	Switch(config)# snmp-server trap-type sfp-threshold	Enable SNMP trap for SFP threshold when SFP status changes from normal to abnormal or abnormal to normal. The " no snmp-server trap-type sfp-threshold " command disable SNMP trap for SFP threshold. Default value is enabled.
Step 3	Switch (config)# exit	Returns to privileged EXEC mode.
Step 4	Switch# write	(Optional) Save the configuration.

Chapter 3. Show Command

3.1 Display SFP/SFP+ Port Threshold Information

You can display SFP/SFP+ Port Threshold configuration and information of the monitored items on the specified port of the switch by performing the following tasks:

Command	Purpose
Switch# show sfp threshold <i>interface-id</i>	Display all interface, single interface or interface range of temperature (degrees C), voltage (V), current (mA), TX power (dBm) and RX power (dBm) information that include SFP current status, high alarm, high warning, low warning and low alarm threshold.
Switch# show sfp threshold current <i>interface-id</i>	Display all interface, single interface or interface range of current (mA) information that include SFP current status, high alarm, high warning, low warning and low alarm threshold.
Switch# show sfp threshold rx-power <i>interface-id</i>	Display all interface, single interface or interface range of RX power (dBm) information that include SFP current status, high alarm, high warning, low warning and low alarm threshold.
Switch# show sfp threshold temperature <i>interface-id</i>	Display all interface, single interface or interface range of temperature (degrees C) information that include SFP current status, high alarm, high warning, low warning and low alarm threshold.
Switch# show sfp threshold tx-power <i>interface-id</i>	Display all interface, single interface or interface range of TX power (dBm) information that include SFP current status, high alarm, high warning, low warning and low alarm threshold.
Switch# show sfp threshold voltage <i>interface-id</i>	Display all interface, single interface or interface range of voltage (V) information that include SFP current status, high alarm, high warning, low warning and low alarm threshold.

This page is intentionally left blank.