



MEN-5410

8-port 10/100/1000Base-T + 2-slot Gigabit SFP
Managed Access Switch

User Manual



COPYRIGHT

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photo copying, recording or otherwise, without the prior written permission of the publisher.

FCC WARNING



This equipment has been tested and found to comply with the limits for a class A device, pursuant to part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial 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 communication. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at the user's own expense.

CE



This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

CAUTION

**RISK OF EXPLOSION IF A BATTERY IS REPLACED BY AN INCORRECT TYPE.
DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.**

Take special care to read and understand all the content in the warning boxes:



Warning

Table of Content

<u>1. ABOUT THIS GUIDE.....</u>	<u>1</u>
1.1. WELCOME	1
1.2. PURPOSE.....	1
1.3. TERMS/ USAGE.....	1
1.4. FEATURES.....	2
1.5. SPECIFICATIONS	1
<u>2. HARDWARE DESCRIPTION.....</u>	<u>3</u>
2.1. CONNECTORS	3
2.2. INSTALLATION	3
2.3. LED INDICATORS	6
<u>3. MANAGEMENT OPTIONS</u>	<u>7</u>
3.1. MANAGEMENT VIA CONSOLE PORT	7
3.2. MANAGEMENT BY TELNET	8
3.3. HOW TO ENTER THE CLI?	8
3.4. CLI COMMAND CONCEPT.....	9
3.5. MANAGEMENT VIA INTERNET BROWSER INTERFACE.....	10
3.6. SYSTEM INFORMATION	11
3.6.1. CLI CONFIGURATION	11
3.6.2. WEB CONFIGURATION.....	11
<u>4. BASIC SETTINGS</u>	<u>13</u>
4.1. GENERAL SETTINGS.....	13
4.1.1. SYSTEM	13
4.1.1.1. CLI CONFIGURATION	13
4.1.1.2. WEB CONFIGURATION.....	14
4.1.2. JUMBO FRAME.....	15
4.1.2.1. CLI CONFIGURATION	15
4.1.2.2. WEB CONFIGURATION.....	15
4.1.3. SNTP.....	15
4.1.3.1. CLI CONFIGURATION	16
4.1.3.1. WEB CONFIGURATION.....	18
4.1.4. MANAGEMENT HOST.....	20
4.1.4.1. CLI CONFIGURATION	20
4.1.4.2. WEB CONFIGURATION.....	20
4.2. MAC MANAGEMENT.....	21
4.2.1. CLI CONFIGURATION	22
4.2.2. WEB CONFIGURATION.....	22
4.2.3. REFUSAL (BLACK-HOLE MAC).....	25
4.2.3.1. CLI CONFIGURATION	25

4.2.3.2.	WEB CONFIGURATION	25
4.3.	PORT MIRROR.....	26
4.3.1.	CLI CONFIGURATION	27
4.3.2.	WEB CONFIGURATION	27
4.4.	PORT SETTINGS.....	28
4.4.1.	CLI CONFIGURATION	30
4.4.2.	WEB CONFIGURATION	31
5.	<u>ADVANCED SETTINGS</u>	<u>33</u>
5.1.	BANDWIDTH CONTROL	33
5.1.1.	QoS	33
5.1.1.1.	CLI CONFIGURATION	38
5.1.1.2.	WEB CONFIGURATION	39
5.1.2.	RATE LIMITATION	43
5.1.2.1.	STORM CONTROL	43
5.1.2.1.1.	CLI CONFIGURATION	43
5.1.2.1.2.	WEB CONFIGURATION	44
5.1.2.2.	RATE LIMITATION	45
5.1.2.2.1.	CLI CONFIGURATION	45
5.1.2.2.2.	WEB CONFIGURATION	45
5.2.	VLAN	46
5.2.1.	MAC-BASED VLAN.....	46
5.2.1.1.	CLI CONFIGURATION	46
5.2.1.2.	WEB CONFIGURATION	47
5.2.2.	PORT ISOLATION	47
5.2.2.1.	CLI CONFIGURATION	48
5.2.2.2.	WEB CONFIGURATION	49
5.2.3.	802.1Q VLAN.....	50
5.2.3.1.	CLI CONFIGURATION	51
5.2.3.2.	WEB CONFIGURATION	52
5.2.4.	GARP/GVRP	55
5.2.4.1.	CLI CONFIGURATION	56
5.2.4.2.	WEB CONFIGURATION	57
5.2.5.	PROTOCOL-BASED VLAN.....	59
5.2.5.1.	CLI CONFIGURATION	59
5.2.5.2.	WEB CONFIGURATION	60
5.2.6.	Q-IN-Q VLAN (VLAN STACKING).....	60
5.2.6.1.	CLI CONFIGURATION	65
5.2.6.2.	WEB CONFIGURATION	67
5.3.	IGMP SNOOPING	69
5.3.1.	IGMP SNOOPING	69
5.3.1.1.	CLI CONFIGURATION	71
5.3.1.2.	WEB CONFIGURATION	73
5.3.2.	MVR.....	75
5.3.2.1.	CLI CONFIGURATION	77
5.3.2.2.	WEB CONFIGURATION	78
5.3.3.	MULTICAST ADDRESS.....	80
5.3.3.1.	CLI CONFIGURATION	81
5.3.3.2.	WEB CONFIGURATION	82

5.4. DHCP RELAY	82
5.4.1. CLI CONFIGURATION	86
5.4.2. WEB CONFIGURATION	87
5.5. DUAL HOMING	87
5.5.1. CLI CONFIGURATION	88
5.5.2. WEB CONFIGURATION	89
5.6. EEE (ENERGY EFFICIENT ETHERNET)	89
5.6.1. CLI CONFIGURATION	90
5.6.2. WEB CONFIGURATION	90
5.7. LINK AGGREGATION.....	91
5.7.1. STATIC TRUNK	91
5.7.1.1. CLI CONFIGURATION	91
5.7.1.2. WEB CONFIGURATION	92
5.7.2. LACP	93
5.7.2.1. CLI CONFIGURATION	94
5.7.2.2. WEB CONFIGURATION	95
5.8. LINK LAYER DISCOVERY PROTOCOL (LLDP).....	97
5.8.1. CLI CONFIGURATION	98
5.8.2. WEB CONFIGURATION	99
5.9. LOOP DETECTION	101
5.9.1. CLI CONFIGURATION	102
5.9.2. WEB CONFIGURATION	103
5.10. STP	104
5.10.1. CLI CONFIGURATION	108
5.10.2. WEB CONFIGURATION	110
5.11. XPRESS RING.....	114
5.11.1. CLI CONFIGURATION.....	115
5.11.2. WEB CONFIGURATION	115
<u>6. SECURITY.....</u>	<u>116</u>
6.1. IP SOURCE GUARD.....	116
6.1.1. DHCP SNOOPING	116
6.1.1.1. CLI CONFIGURATION	119
6.1.1.2. WEB CONFIGURATION	120
6.1.2. ARP INSPECTION	122
6.1.2.1. CLI CONFIGURATION	123
6.1.2.2. WEB CONFIGURATION	123
6.1.3. FILTER TABLE	124
6.1.3.1. CLI CONFIGURATION	125
6.1.3.2. WEB CONFIGURATION	125
6.1.4. BINDING TABLE	126
6.1.4.1. CLI CONFIGURATION	126
6.1.4.2. WEB CONFIGURATION	127
6.1.5. DHCP SERVER SCREENING	129
6.1.5.1. CLI CONFIGURATION	129
6.1.5.2. WEB CONFIGURATION	129
6.2. ACL	130
6.2.1. CLI CONFIGURATION	131
6.2.2. WEB CONFIGURATION	133

6.3. 802.1X	135
6.3.1. CLI CONFIGURATION	137
6.3.2. WEB CONFIGURATION	139
6.4. PORT SECURITY	143
6.4.1. CLI CONFIGURATION	144
6.4.2. WEB CONFIGURATION	144
6.5. SWITCH LOCK.....	145
6.5.1. CLI CONFIGURATIONS	145
6.5.2. WEB CONFIGURATIONS.....	146
<u>7. MONITOR.....</u>	<u>147</u>
7.1. HARDWARE INFORMATION	147
7.1.1. CLI CONFIGURATION	147
7.1.2. WEB CONFIGURATION	148
7.2. PORT UTILIZATION	148
7.2.1. CLI CONFIGURATION	148
7.2.2. WEB CONFIGURATION	148
7.3. RMON STATISTICS	149
7.3.1. CLI CONFIGURATION	149
7.3.2. WEB CONFIGURATION	149
7.4. SFP INFORMATION.....	150
7.4.1. CLI CONFIGURATION	150
7.4.2. WEB CONFIGURATION.....	150
7.5. TRAFFIC MONITOR.....	151
7.5.1. CLI CONFIGURATION	151
7.5.2. WEB CONFIGURATION.....	152
<u>8. MANAGEMENT</u>	<u>154</u>
8.1. AUTO PROVISION	154
8.1.1. CLI CONFIGURATION	155
8.1.2. WEB CONFIGURATION	156
8.2. MAIL ALARM.....	156
8.2.1. REFERENCE	157
8.2.2. CLI CONFIGURATION	157
8.2.3. WEB CONFIGURATION	158
8.3. MAINTENANCE.....	159
8.3.1. CONFIGURATION.....	159
8.3.1.1. CLI CONFIGURATION	159
8.3.1.2. WEB CONFIGURATION	160
8.3.2. FIRMWARE	161
8.3.3. REBOOT	161
8.4. SNMP	162
8.4.1. CLI CONFIGURATION	163
8.4.2. WEB CONFIGURATION	163
8.5. SYSTEM LOG.....	166
8.5.1. CLI CONFIGURATION	166
8.5.2. WEB CONFIGURATION	167

8.6. USER ACCOUNT.....	167
8.6.1. CLI CONFIGURATION	168
8.6.2. WEB CONFIGURATION.....	169
<u>CUSTOMER SUPPORT</u>	<u>170</u>

CONFIDENTIAL

1. About this Guide

1.1. Welcome

The MEN-5410 managed access switch is a compact Gigabit solution designed to provide easy and affordable high-speed network connectivity to home and small offices. Built to fulfill the needs of ever growing bandwidth demands, the MEN-5410 brings the speed Gigabit Ethernet for bandwidth intensive applications without compromising on performance and reliability. Easy-to-use management and monitoring capabilities significantly reduces IT overhead by eliminating the need to manually configure policies on the switch, saving valuable time and effort, and avoids unnecessary OPEX.

Equipped with 8 multi-rate (10/100/1000Mbps) copper ports and 2 Gigabit SFP slots, the MEN-5410 provides you greater flexibility in choosing Standard Ethernet, Fast Ethernet, or Gigabit Ethernet connectivity. The MEN-5410 is capable of providing Gigabit speeds with a total switching capacity of 20Gbps boosts network efficiency and eliminates network congestion. Service providers can take complete advantage of this small but powerful package to offer a truly high-speed network to low density subscriber base with high ARPU.

1.2. Purpose

This guide discusses how to install and configure your Managed Layer 2 Access Switch.

1.3. Terms/ Usage

In this guide, the term “Switch” (first letter upper case) refers to the MEN-5410 Switch, and “switch” (first letter lower case) refers to other switches.

1.4. Features

Network Function

Static link trunking

LACP

STP/RSTP

Support Xpress Ring

Dual Homing

Port based Loop Detection with Auto-recovery timer

IGMP snooping (v1/v2, v3)

MVR

User Security

DHCP Snooping

Access Control List (L2/L3/L4)

Static MAC Forwarding

MAC Limitation

ARP Inspection

Port Authentication

Port Security

Abnormal Traffic Detection

Network Management

SNMP v1/v2c

SNMP Trap

MIB with RMON Group 1,2,3,9

Port-based Mirroring

SNTP

DHCP Client/relay/option 82

Dying Gasp

RS-232 console port

CLI through console

Telnet

Web-based GUI

Status display and event report

Auto-logout timer

Firmware upgrade by TFTP/HTTP/FTP

Configuration backup/restore

Port Management

Loopback Test

User self-defined default configuration

Auto-provisioning

Traffic Management & QoS

802.1Q Tag-based VLAN

Port-based VLAN

Active VLAN support: 4K

Private VLAN

Management VLAN

GARP/GVRP support

802.1p Priority Queues per port

Traffic Classification

Scheduler SP/WRR

Network Storm Control

Rate Limitation

1.5. Specifications

IEEE Standards

IEEE 802.3	10Base-T
IEEE 802.3u	100Base-TX
IEEE 802.3ab	1000Base-T
IEEE 802.3z	1000Base-SX/LX/LHX
IEEE 802.3	Nway Auto-negotiation
IEEE 802.3ad	Link Aggregation
IEEE 802.1d	Spanning Tree Protocol
IEEE 802.1w	Rapid Spanning Tree Protocol
IEEE 802.3x	Flow Control
IEEE 802.1p	Priority Queues
IEEE 802.1q	VLAN Tagging

Performance

Switching fabric	20Gbps
L2 forwarding	14.9Mpps
Packet buffer size	8Mbits
MAC addresses	16K
Throughput	14,880 pps to 10 Mbps ports 148,800 pps to 100 Mbps ports 1,488,000 pps to 1000 Mbps ports
Jumbo frame	10 k

Ports

Uplink ports	2 SFP slots (1000Mbps)
Downlink ports	8 x 10/100/1000Base-T (RJ-45)
1 x RJ-45 Console Port	

Maximum Distances

RJ-45	up to 100 m
SC/SFP	up to 100 km
Console	15 m

Mechanical & Environmental

Operating temperature	0°C to 50°C
Storage temperature	-20°C to 70°C
Operating humidity	10% to 80% RH
Storage humidity	5% to 95% RH

Power

Front access AC power	100-240V AC, 50~60Hz
DC Jack	15V DC input (Optional)
Power consumption	16W (w/o Battery)
Battery Charge	12V, via terminal block

Dimensions & Weight

Dimensions (mm)	268 x 44 x 128 (W x H x D)
Weight	1.2 kg

CONFIDENTIAL

2. Hardware Description

MEN-5410 Front Panel



8-port 10/100/1000Base-T + 2-slot Gigabit SFP
Managed Access Switch with Battery Back-up

2.1. Connectors

The Switch utilizes ports with copper and SFP fiber port connectors functioning under Ethernet/Fast Ethernet/Gigabit Ethernet standards.

10/100/1000Base-T Ports

The 10/100/1000BASE-T ports support network speeds of 10Mbps, 100Mbps or 1000 Mbps, and can operate in half- and full-duplex transfer modes. These ports also offer automatic MDI/MDI-X crossover detection that gives true “plug-n-play” capability – just plug the network cables into the ports and the ports will adjust according to the end-node devices. The following are recommended cabling for the RJ-45 connectors: (1) 10 Mbps – Cat 3 or better; (2) 100 or 1000 Mbps – Cat 5e or better.

SFP Slots for SFP modules

The 2-slot Gigabit SFP are designed to house Gigabit SFP modules that support network speeds of 1000Mbps. For increased bandwidth applications, Switch can provide 2Gbps upstream or downstream traffic rate by trunking skill. In case downstream demand increases, it can provide up to 100Mbps per port to downstream devices or customers in a high flexible package.

2.2. Installation

The location chosen for installing the Switch may greatly affect its performance. When selecting a site, we recommend considering the following rules:

- Install the Switch in an appropriate place. See Technical Specifications for the acceptable temperature and humidity ranges.
- Install the Switch in a location that is not affected by strong electromagnetic field generators (such as motors), vibration, dust, and direct sunlight.
- Leave at least 10cm of space at the front and rear of the unit for ventilation.

- Affix the provided rubber pads to the bottom of the Switch to protect the case from scratching.

Desktop Installation

Follow the instructions listed below to install the Switch in a desktop location:

1. Locate the Switch in a clean, flat and safe position that has convenient access to AC power.
2. Affix the four self-adhesive rubber pads to the underside of the Switch.
3. Apply AC power to the Switch (The green PWR LED on the front panel should light up).
4. Connect cables from the network partner devices to the ports on the front panel (The green LNK LED on the upper right of the port should light).

This Switch can also be mounted on a vertical surface. Simply use the underside of the unit as a template to measure and mark out the position of the holes on to the surface where the unit is to be installed. Then use the two screws provided to mount the Switch firmly in place.

Warning: Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures.

Mounting on a Rack

Attach brackets to each side of the switch and place the brackets in the rack's slots. Insert and tighten two screws to securely attach the bracket to the rack on each side.

Getting Connected

The Switch is capable of connecting up to 8 down-link and 2 up-link network devices employing a combination of twisted-pair and fiber cabling paths at Ethernet, Fast Ethernet, or Gigabit Ethernet speeds.

Powering On the Unit

The Switch uses an AC power supply 100~240V AC, 50~60 Hz, or DC 15V. The Switch's power supply automatically self-adjusts to the local power source and may be powered on without having any or all LAN segment cables connected.

Notes:

- For international use, you may need to change the AC power adapter cord.
- You must use a power cord set that has been approved for the receptacle type and electrical current in your country.

- Check the front-panel LEDs as the device is powered on to verify that the Power LED is lit. If not, check that the power cable is correctly and securely plugged in.

Installing the SFP modules and Fiber Cable

1. Slide the selected SFP module into the selected SFP slot. (Make sure the SFP module is aligned correctly with the inside of the slot):
2. Insert and slide the module into the SFP slot until it clicks into place:
3. Remove any rubber plugs that may be present in the SFP module's mouth.
4. Align the fiber cable's connector with the SFP module's mouth and insert the connector:
5. Slide the connector in until a click is heard:
6. If you want to pull the connector out, first push down the release clip on top of the connector to release the connector from the SFP module.

To properly connect fiber cabling: Check that the fiber terminators are clean. You can clean the cable plugs by wiping them gently with a clean tissue or cotton ball moistened with a little ethanol. Dirty fiber terminators on fiber optic cables will impair the quality of the light transmitted through the cable and lead to degraded performance on the port.

Check the corresponding port LED on the Switch to be sure that the connection is valid. (Refer to the LED chart).

Connecting Copper Cable

1. The 10/100/1000Base-T RJ-45 Ethernet ports fully support auto-sensing and auto-negotiation. Insert one end of a Category 3/4/5/5e (see recommendation above) type twisted pair cable into an available RJ-45 port on the Switch and the other end into the port of the network node.
2. Check the corresponding port LED on the Switch to ensure that the connection is valid. (Refer to LED chart)

Connecting the Console Port Cable

1. Use null modem cable to connect the console port on the Switch and the other end into the COM port of the computer.
2. Insert the RJ-45 side of the (8-pin RJ-45 to DB-9) cable into the RJ-45 console port on the Switch and the other end into the COM port of the computer.
3. Configure by Hyper Terminal, Putty, Tera Term...

Connecting to computers or a LAN

You can use Ethernet cables to connect computers directly to the Switch ports. You can also connect hubs/switches to the switch ports by Ethernet cables. You can use either crossover or straight-through Ethernet cables to connect computers, hubs, or switches.

Attaching the power adapter

Connect the AC power cord to the POWER receptacle on the back of the Switch and plug the other end of the power cord into a wall outlet or a power strip. Check the front LED indicators with the description in the next chapter. If the LEDs light up as described, the Switch's hardware is working properly.

2.3. LED Indicators

This Switch is equipped with Unit LEDs to enable you to determine the status of the Switch, as well as Port LEDs to display what is happening in all your connections. They are as follows:

Unit LEDs		
LED	Condition	Status
POWER (Green)	Illuminated	Power on
	Off	Power off or fail
POST (Green)	Illuminated	System ready to use
	Blinking	Power on self-test
	Off	Power off or test fail
ALARM (Red)	Illuminated	Alarm for over threshold of system temperature or voltage
	Blinking	Alarm for loop detection
	Off	Switch is in normal condition
LNK/ACT (Green) (for 1~8 th 10/100/1000Mbps Copper ports)	Illuminated	Ethernet link-up
	Blinking	Receiving or transmitting data
	Off	Port disconnected or link failed
1000 (Green)	Illuminated	1000Mbps
	Off	10/100Mbps
LNK/ACT (Green) (for 9~10 th ports)	Illuminated	Ethernet link-up
	Blinking	Receiving or transmitting data
	Off	Port disconnected or link failed

3. Management options

This system may be managed out-of-band through the console port on the front panel or in-band by using Telnet. The user may also choose web-based management, accessible through a Web browser.

The management agent is based on SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any PC in the network by using in-band management software.

The switch gives you the flexibility to access and manage it by using any or all of the methods described. The administration console and web browser interfaces are embedded in the Switch software and can be used immediately after setup.

3.1. Management via console port

Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using an out-of-band connection or the BOOTP protocol.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network or via the internet. The onboard configuration program can be accessed using Telnet from any computer attached to the network. It can also be managed from any computer using a Web browser.

Access the Switch via a terminal emulator (such as Hyper Terminal) attached to the console port. The console port is set at the factory with the following default COM port properties. Configure your own terminal to match the following:

Setting	Default Value
Terminal Emulation	VT100
Baud Rate	38400
Parity	None
Data Bits	8
Stop Bits	1
Flow Control	None

Note: Ensure that the terminal or PC you are using to make this connection is configured to match the above settings. Otherwise the connection will not work.

Then press [ENTER] to open the login screen with the "Default Value" for Username and Password as "admin".

3.2. Management by Telnet

Activate your workstation's command prompt program and access your Switch via the Internet by typing in the correct IP address (factory default IP address is 192.168.0.254 - connect directly via console port to configure a unique IP address). Your command prompt program will allow use of the Telnet protocol.

1. Connect your computer to one of the Ethernet ports.
2. Open a Telnet session to the Switch's IP address. If this is your first login, use the default values.

Setting	Default Value
IP Address	192.168.0.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Management VLAN	1
Default Username	admin
Default Password	admin

3. Make sure your computer IP address is in the same subnet, unless you are accessing the Switch through one or more routers.

3.3. How to enter the CLI?

Press [Enter] key to enter the login command prompt when below message is displayed on the screen.

Please press Enter to activate this console

Input "*admin*" to enter the CLI mode when below message is displayed on the screen.

L2SWITCH login:

You can execute a few limited commands when CLI prompt is displayed as below.

L2SWITCH>

If you want to execute more powerful commands, you must enter the privileged mode.

Input command "*enable*"

L2SWITCH>enable

Input a valid username and password when below prompt are displayed.

user:admin

password:admin

L2SWITCH#

3.4. CLI command concept

Node	Command	Description
enable	show hostname	This command displays the system's network name.
configure	reboot	This command reboots the system.
eth0	ip address A.B.C.D/M	This command configures a static IP and subnet mask for the system.
interface	show	This command displays the current port configurations.
acl	show	This command displays the current access control profile.
vlan	show	This command displays the current VLAN configurations.

The Node type:

- enable
Its command prompt is "**L2SWITCH#**".
It means these commands can be executed in this command prompt.
- configure
Its command prompt is "**L2SWITCH(config)#**".
It means these commands can be executed in this command prompt.
In *Enable* code, executing command "**configure terminal**" enter the configure node.
L2SWITCH# configure terminal
- eth0
Its command prompt is "**L2SWITCH(config-if)#**".
It means these commands can be executed in this command prompt.
In *Configure* code, executing command "**interface eth0**" enter the eth0 interface node.
L2SWITCH(config)#interface eth0
L2SWITCH(config-if)#
- interface
Its command prompt is "**L2SWITCH(config-if)#**".
It means these commands can be executed in this command prompt.
In *Configure* code, executing command "**interface gig Ethernet1/0/5**" enter the interface port 5 node.
Or
In *Configure* code, executing command "**interface fast Ethernet1/0/5**" enter the interface port 5 node.
Note: depend on your port speed, gig Ethernet1/0/5 for gigabit Ethernet ports and fast Ethernet1/0/5 for fast Ethernet ports.

L2SWITCH(config)#interface gig Ethernet1/0/5

L2SWITCH(config-if)#

- **vlan**
 Its command prompt is “*L2SWITCH(config-vlan)#*”.
 It means these commands can be executed in this command prompt.
 In **Configure** code, executing command “*vlan 2*” enter the vlan 2 node.
 Note: where the “2” is the vlan ID.

L2SWITCH(config)#vlan 2
L2SWITCH(config-vlan)#

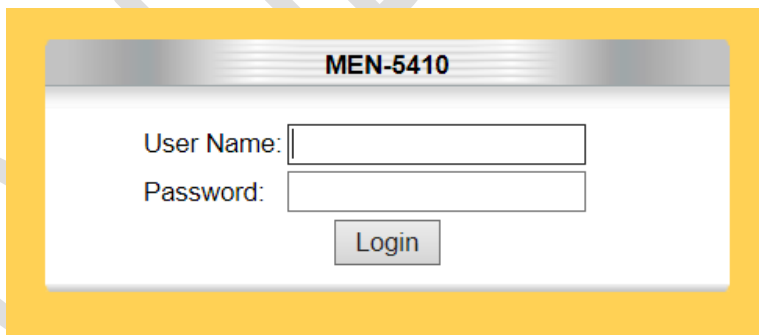
- **acl**
 Its command prompt is “*L2SWITCH(config-acl)#*”.
 It means these commands can be executed in this command prompt.
 In **Configure** code, executing command “*access-list test*” enter the access-list test node.
 Note: where the “*test*” is the profile name.

L2SWITCH(config)#access-list test
L2SWITCH(config-acl)#

3.5. Management via Internet Browser Interface

From a PC, open your Web browser, type the following in the Web address (or location) box: <http://192.168.0.254> and then press <Enter>.

This is the factory default IP address for the switch. A login dialog is displayed, as shown in the figure:



Enter your user name and password, and then click OK.

Use the defaults the first time you log into the program. You can change the password at any time through CLI interface.

Default:

User name: admin,

Password: admin.

3.6. System Information

The System Information window appears each time you log into the program. Alternatively, this window can be accessed by clicking System Status > System Information

3.6.1. CLI Configuration

Node	Command	Description
enable	show hostname	This command displays the system's network name.
enable	show interface eth0	This command displays the current Eth0 configurations.
enable	show model	This command displays the system information.
enable	show running-config	This command displays the current operating configurations.
enable	show system-info	This command displays the system's CPU loading and memory information.
enable	show uptime	This command displays the system up time.

3.6.2. Web Configuration

System Information

System Information

Model Name	MEN-5410
Host Name	L2SWITCH
Boot Code Version	5410-000-1.0.0.S0
Firmware Version	5410-000-1.0.2.b1
Built Date	Tue Nov 12 11:52:42 CST 2013
DHCP Client	Disabled
IP Address	192.168.202.37
Subnet Mask	255.255.255.0
Default Gateway	192.168.202.1
MAC Address	00:50:43:ae:65:b8
Serial Number	A000000000001
Management VLAN	1
CPU Loading	0 %
Memory Information	Total: 54124 KB, Free: 29720 KB, Usage: 45.09 %
Current Time	1970-1-1, 3:2:12

Parameter	Description
Model Name	This field displays the model name of your Switch.
Host name	This field displays the name of your Switch.
Boot Code Version	This field displays the boot code version.
Firmware Version	This field displays the version number of the currently installed

	firmware.
Built Date	This field displays the built date of the currently installed firmware.
DHCP Client	This field displays whether the DHCP client feature is enabled.
IP Address	This field indicates the IP address of the Switch.
Subnet Mask	This field indicates the subnet mask of the Switch.
Default Gateway	This field indicates the default gateway of the Switch.
MAC Address	This field displays the MAC (Media Access Control) address of the Switch.
Serial Number	The serial number, the unique code assigned by manufacture for identification of a single unit.
Management VLAN	This field displays the VLAN ID that is used for the Switch management purposes.
CPU Loading	This field displays the percentage of your Switch's system load.
Memory Information	This field displays the total memory the Switch has and the memory which is currently available (Free) and occupied (Usage).
Current Time	This field displays current date (yyyy-mm-dd) and time (hh:mm:ss).
Refresh	Click this to update the information in this screen.

CONFIDENTIAL

4. Basic Settings

4.1. General Settings

4.1.1. System

Management VLAN

To specify a VLAN group which can access the Switch.

- The valid VLAN range is from 1 to 4094.
- If you want to configure a management VLAN, the management VLAN should be created first and the management VLAN should have at least one member port.

Host Name

The **hostname** is same as the SNMP system name. Its length is up to 64 characters. The first 16 characters of the hostname will be configured as the CLI prompt.

Default Settings

- The default Hostname is L2SWITCH
- The default DHCP client is disabled.
- The default Static IP is 192.168.0.254
- Subnet Mask is 255.255.255.0
- Default Gateway is 0.0.0.0
- Management VLAN is 1.

4.1.1.1. CLI Configuration

Node	Command	Description
configure	reboot	This command reboots the system.
configure	hostname STRINGS	This command sets the system's network name.
configure	interface eth0	This command enters the eth0 interface node to configure the system IP.
eth0	ip address A.B.C.D/M	This command configures a static IP and subnet mask for the system.
eth0	ip address default-gateway A.B.C.D	This command configures the system default gateway.
eth0	ip dhcp client (disable enable renew)	This command configures a DHCP client function for the system. Disable: Use a static IP address on the switch. Enable & Renew: Use DHCP client to get an IP address from DHCP server.
eth0	management vlan VLAN_ID	This command configures the management vlan.

4.1.1.2. Web Configuration

General Settings

System
Jumbo Frame
SNTP
Management Host

System Settings

Hostname:

DHCP Client: Enable

Static IP Address:

Subnet Mask:

Default Gateway:

Management VLAN:

Parameter	Description
Hostname	Enter up to 64 alphanumeric characters for the name of your Switch. The hostname should be the combination of the digit or the alphabet or hyphens (-) or underscores (_).
DHCP Client	Select Enable to allow the Switch to automatically get an IP address from a DHCP server. Click Renew to have the Switch re-get an IP address from the DHCP server. Select Disable if you want to configure the Switch's IP address manually.
Static IP Address	Enter the IP address of your Switch in dotted decimal notation. For example, 192.168.0.254.
Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.1.
Management VLAN	Enter a VLAN ID used for Switch management purposes.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

4.1.2. Jumbo Frame

Jumbo frames are Ethernet frames with a payload greater than 1500 bytes. Jumbo frames can enhance data transmission efficiency in a network. The jumbo frame settings will apply to all ports.

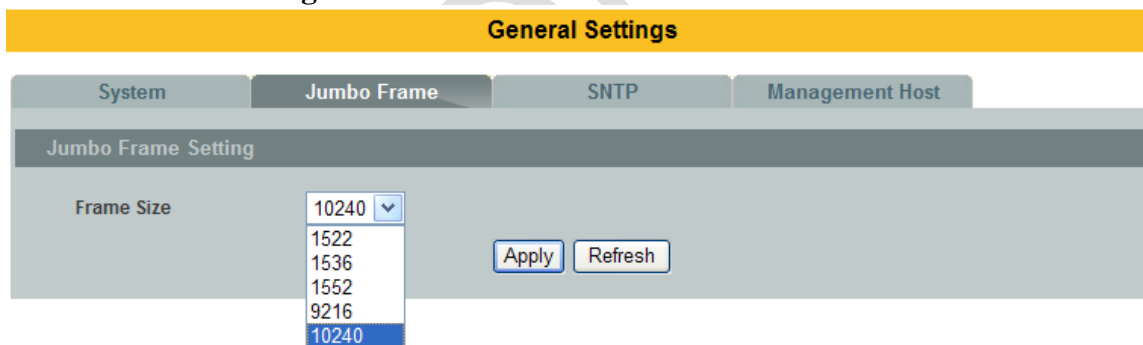
Note: If the size of a packet exceeds the jumbo frame size, the packet will be dropped. The available values are 1522,1536,1552,9216,10240.

Default Setting: The default jumbo frame is 10240 bytes.

4.1.2.1. CLI Configuration

Node	Command	Description
enable	show jumboframe	This command displays the current jumbo frame settings.
configure	jumboframe (10240 1522 1536 1552 9216)	This command configures the maximum number of bytes of a jumbo frame for all ports. The bigger the frame size, the better the performance.

4.1.2.2. Web Configuration



Parameter	Description
Frame Size	Select the maximum number of bytes of a jumbo frame for all ports. The bigger the frame size, the better the performance.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

4.1.3. SNTP

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. A less complex implementation of NTP, using the same protocol but without requiring the storage of state over extended periods of time is known as the **Simple Network Time Protocol (SNTP)**. NTP provides Coordinated Universal Time (UTC). No information about time zones or

daylight saving time is transmitted; this information is outside its scope and must be obtained separately.

UDP Port: 123.

Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.

Note:

1. The SNTP server always replies the UTC current time.
2. When the Switch receives the SNTP reply time, the Switch will adjust the time with the time zone configuration and then configure the time to the Switch.
3. If the time server's IP address is not configured, the Switch will not send any SNTP request packets.
4. If no SNTP reply packets, the Switch will retry every 20 seconds forever.
5. If the Switch has received SNTP reply, the Switch will re-get the time from NTP server every one hour.
6. If the time zone and time NTP server have been changed, the Switch will repeat the query process.
7. No default SNTP server.

Default Settings

Current Time:

 Time: 0:3:51 (UTC)
 Date: 1970-1-1

Time Server Configuration:

 Time Zone : +00:00
 IP Address: 0.0.0.0

DayLight Saving Time Configuration:

 State : disabled
 Start Date: None.
 End Date : None.

4.1.3.1. CLI Configuration

Node	Command	Description
enable	show time	This command displays current time and time configurations.
configure	time HOUR:MINUTE:SECOND	Sets the current time on the Switch. <i>hour:</i> 0-23 <i>min:</i> 0-59 <i>sec:</i> 0-59

		Note: If you configure Daylight Saving Time after you configure the time, the Switch will apply Daylight Saving Time.
configure	time date YEAR/MONTH/DAY	Sets the current date on the Switch. <i>year:</i> 1970- <i>month:</i> 1-12 <i>day:</i> 1-31
configure	time daylight-saving-time	This command enables the daylight saving time.
configure	time daylight-saving-time start-date (first second third fourth last) (Sunday Monday Tuesday Wednesday Thursday Friday Saturday) MONTH HOUR	This command sets the start time of the Daylight Saving Time.
configure	time daylight-saving-time end-date (first second third fourth last) (Sunday Monday Tuesday Wednesday Thursday Friday Saturday) MONTH HOUR	This command sets the end time of the Daylight Saving Time.
configure	no time daylight-saving-time	This command disables daylight saving on the Switch.
configure	time ntp-server (disable enable)	This command disables / enables the NTP server state.
configure	time ntp-server IP_ADDRESS	This command sets the IP address of your time server.
configure	time timezone STRING	Configures the time difference between UTC (formerly known as GMT) and your time zone. Valid Range: -1200 ~ +1200.

Example:

```
L2SWITCH(config)#time ntp-server 192.5.41.41
L2SWITCH(config)#time timezone +0800
L2SWITCH(config)#time ntp-server enable
L2SWITCH(config)#time daylight-saving-time start-date first Monday 6 0
L2SWITCH(config)#time daylight-saving-time end-date last Saturday 10 0
```

4.1.3.1. Web Configuration

General Settings

System	Jumbo Frame	SNTP	Management Host
Current Time and Date			
Current Time	00:38:21 (UTC)		
Current Date	2014-01-01		
Time and Date Settings			
<input checked="" type="radio"/> Manual			
New Time	<input type="text" value="2014"/> . <input type="text" value="1"/> . <input type="text" value="1"/> / <input type="text" value="0"/> : <input type="text" value="38"/> : <input type="text" value="21"/> (yyyy.mm.dd / hh:mm:ss)		
<input type="radio"/> Enable Network Time Protocol			
NTP Server	<input checked="" type="radio"/> 192.5.41.41 - North America		
	<input type="radio"/> <input type="text"/>		
Time Zone	<input type="text" value="+0000"/>		
Daylight Saving Settings			
State	<input type="text" value="Disable"/>		
Start Date	<input type="text" value="First"/> of <input type="text" value="Sunday"/> of <input type="text" value="January"/> at <input type="text" value="0"/> o'clock		
End Date	<input type="text" value="First"/> of <input type="text" value="Sunday"/> of <input type="text" value="January"/> at <input type="text" value="0"/> o'clock		
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>			

Parameter	Description
Current Time and Date	
Current Time	This field displays the time you open / refresh this menu.
Current Date	This field displays the date you open / refresh this menu.
Time and Date Setting	
Manual	Select this option if you want to enter the system date and time manually.
New Time	Enter the new date in year, month and day format and time in hour, minute and second format. The new date and time then appear in the Current Date and Current Time fields after you click Apply .
Enable Network Time Protocol	Select this option to use Network Time Protocol (NTP) for the time service.
NTP Server	Select a pre-designated time server or type the IP address of your time server. The Switch searches for the timeserver for up to 60 seconds.

Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone.
Daylight Saving Settings	
State	Select Enable if you want to use Daylight Saving Time. Otherwise, select Disable to turn it off.
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving Time. The time is displayed in the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, 3(March) and 2:00.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, 3(March) and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
End Date	<p>Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving Time. The time field uses the 24 hour format.</p> <p>Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, 11(November) and 2:00.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, 10(October) and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

4.1.4. Management Host

The feature limits the hosts which can manage the Switch. The default has no management host. That is, any hosts can manage the Switch via **telnet** or **web browser**. If user has configured one or more management host, the Switch can be managed by these hosts only. The feature allow user to configure management IP up to 3 entries.

Default Settings

This feature allows user to configure management host up to 3 entries. The default is none, any host can manage the Switch via telnet or web browser.

4.1.4.1. CLI Configuration

Node	Command	Description
enable	show interface eth0	The command displays the all of the interface <i>eth0</i> configurations.
eth0	show	The command displays the all of the interface <i>eth0</i> configurations.
eth0	management host A.B.C.D	The command adds a management host address.
eth0	no management host A.B.C.D	The command deletes a management host address.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#interface eth0
L2SWITCH(config-if)#management host 192.168.200.106
```

4.1.4.2. Web Configuration

General Settings

System
Jumbo Frame
SNTP
Management Host

Management Host Settings

Management Host

Management Host List

No.	Management Host	Action
1	192.168.200.12	<input type="button" value="Delete"/>

Parameter	Description
Management Host	This field configures the management host.
Apply	Click Apply to take effect the settings.

Refresh	Click Refresh to begin configuring this screen afresh.
No.	This field displays a sequential number for each management host.
Management Host	This field displays the management host.
Action	Click Delete to remove the specified entry.

4.2. MAC Management

Dynamic Address:

The MAC addresses are learnt by the switch. When the switch receives frames, it will record the source MAC, the received port and the VLAN in the address table with an age time. When the age time is expired, the address entry will be removed from the address table.

Static Address:

The MAC addresses are configured by users. The static addresses will not be aged out by the switch. The static address can be removed by user only. The maximum static address entry is up to 256.

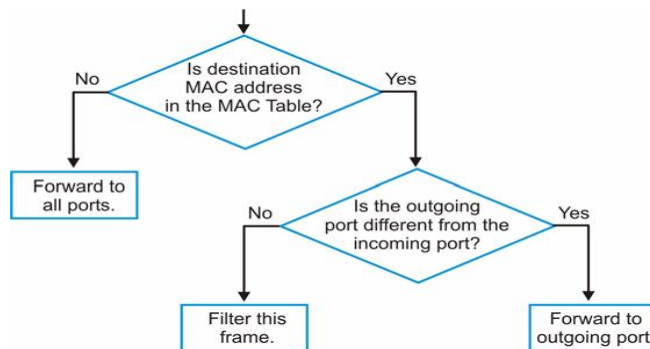
The switch supports up to 16K address table. The static address and the dynamic address share the same table.

The **MAC Table** (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the MAC address of the device is shown on the Switch's MAC Table. It also shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered).

The Switch uses the **MAC Table** to determine how to forward frames. See the following figure.

1. The Switch examines a received frame and learns the port from which this source MAC address came.
2. The Switch checks to see if the frame's destination MAC address matches a source MAC address already learnt in the **MAC Table**.
 - If the Switch has already learnt the port for this MAC address, then it forwards the frame to that port.
 - If the Switch has not already learnt the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
 - If the Switch has already learnt the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

Figure MAC Table Flowchart



Default Settings

The default MAC address table age time is 300 seconds.
 The Maximum static address entry is 256.

4.2.1. CLI Configuration

Node	Command	Description
enable	show mac-address-table aging-time	This command displays the current MAC address table age time.
enable	show mac-address-table (static dynamic)	This command displays the current static/dynamic unicast address entries.
enable	show mac-address-table port PORT_ID	This command displays the current unicast address entries learnt by the specific port.
configure	mac-address-table static MACADDR vlan VLAN_ID port PORT_ID	This command configures a static unicast entry.
configure	no mac-address-table static MACADDR vlan VLAN_ID	This command removes a static unicast entry from the address table.

Example:

L2SWITCH(config)#mac-address-table static 00:11:22:33:44:55 vlan 1 port 1

4.2.2. Web Configuration

Static MAC

A static Media Access Control (MAC) address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

MAC Address Management

Static MAC Settings MAC Table Age Time Setting Refusal MAC Settings

Static MAC Settings

MAC Address	VLAN ID	Port
<input type="text"/>	<input type="text"/>	1 <input type="button" value="v"/>

Static MAC Table

MAC Address	VLAN ID	Port	Action
00:0b:04:11:dc:ec	1	CPU	

Total counts : 1

Parameter	Description
Static MAC Settings	
MAC Address	Enter the MAC address of a computer or device that you want to add to the MAC address table. Valid format is hh:hh:hh:hh:hh:hh.
VLAN ID	Enter the VLAN ID to apply to the computer or device.
Port	Enter the port number to which the computer or device is connected.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Static MAC Table	
MAC Address	This field displays the MAC address of a manually entered MAC address entry.
VLAN ID	This field displays the VID of a manually entered MAC address entry.
Port	This field displays the port number of a manually entered MAC address entry. The MAC address with port CPU means the Switch's MAC addresses itself.
Action	Click Delete to remove this manually entered MAC address entry from the MAC address table. You cannot delete the Switch's MAC address from the static MAC address table.

MAC Table

MAC Address Management

Static MAC Settings **MAC Table** Age Time Setting Refusal MAC Settings

MAC Table

Show Type: All

MAC	Type	VLAN ID	Port/Trunk ID
00:30:00:00:00:00	Dynamic	1	1
00:50:43:4a:62:96	Static	1	CPU
00:1d:7d:e6:ab:cf	Dynamic	1	1

Total counts : 3

 Page:1/1 Page:

Parameter	Description
Show Type Apply	Select All, Static, Dynamic or Port and then click Apply to display the corresponding MAC address entries on this screen.
Refresh	Click this to update the information in the MAC table.
MAC Address	This field displays a MAC address.
Type	This field displays whether this entry was entered manually (Static) or whether it was learned by the Switch (Dynamic).
VLAN ID	This field displays the VLAN ID of the MAC address entry.
Port	This field displays the port number the MAC address entry is associated. It displays CPU if it is the entry for the Switch itself. The CPU means that it is the Switch's MAC.
Total Counts	This field displays the total entries in the MAC table.

Age Time Settings

MAC Address Management

Static MAC Settings MAC Table **Age Time Setting** Refusal MAC Settings

Age Time Setting

Age Time: (sec) (Range:20-500)

Parameter	Description
-----------	-------------

Age Time	Configure the age time; the valid range is from 20 to 500 seconds. The default value is 300 seconds.
Apply	Click Apply to take effect the settings.
Refresh	Click this to update the information in the MAC table.

4.2.3. Refusal (Black-hole MAC)

This type of MAC address entries are configured manually. A switch discards the packets destined for or originated from the MAC addresses contained in blackhole MAC address entries. Blackhole entries are configured for filtering out frames with specific source or destination MAC addresses

Notice: User can configure up to 20 entries.

4.2.3.1. CLI Configuration

Node	Command	Description
enable	show mac-address-table refusal	This command displays the current refusal MAC address only.
configure	mac-address-table refusal MACADDR vlan VLAN_ID	This command configures a refusal MAC on a specific VLAN.
configure	mac-address-table refusal MACADDR	This command configures a refusal MAC.

4.2.3.2. Web Configuration

MAC Address Management

Static MAC Settings
MAC Table
Age Time Setting
Refusal MAC Settings

Refusal MAC Settings

MAC Address	VLAN ID
<input type="text"/>	Any <input type="button" value="v"/> <input type="text"/>

Refusal MAC Table

MAC Address	VLAN ID	Action
00:11:22:33:44:55	1	<input type="button" value="Delete"/>
00:22:33:44:55:66	Any	<input type="button" value="Delete"/>

Total counts : 2

Parameter	Description
MAC Address	Enter the MAC address of a computer or device that you want to refusal. Valid format is hh:hh:hh:hh:hh:hh.
VLAN ID	Enter the VLAN ID to apply to the computer or device.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
MAC Address	This field displays a MAC address.
VLAN ID	This field displays the VLAN ID of the MAC address entry.
Action	Click Delete to remove this manually entered MAC address entry from the refusal MAC address table.
Total Counts	This field displays the total entries in the refusal MAC table.

4.3. Port Mirror

Port-based Mirroring

The Port-Based Mirroring is used on a network switch to send a copy of network packets sent/received on one or a range of switch ports to a network monitoring connection on another switch port (**Monitor-to Port**). This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system.

Port Mirroring, together with a network traffic analyzer, helps to monitor network traffic. Users can monitor the selected ports (**Source Ports**) for egress and/or ingress packets.

Source Mode:

- Ingress : The received packets will be copied to the monitor port.
- Egress : The transmitted packets will be copied to the monitor port.
- Both : The received and transmitted packets will be copied to the monitor port.

Note:

1. The monitor port cannot be a trunk member port.
2. The monitor port cannot be ingress or egress port.
3. If the Port Mirror function is enabled, the Monitor-to Port can receive mirrored packets only.
4. If a port has been configured as a source port and then user configures the port as a destination port, the port will be removed from the source ports automatically.

Default Settings

Mirror Configurations:

State : Disable

Monitor port : 1
 Ingress port(s) : None
 Egress port(s) : None

4.3.1. CLI Configuration

Node	Command	Description
enable	show mirror	This command displays the current port mirroring configurations.
configure	mirror (disable enable)	This command disables / enables the port mirroring on the switch.
configure	mirror destination port PORT_ID	This command specifies the monitor port for the port mirroring.
configure	mirror source ports PORT_LIST mode (both ingress/egress)	This command adds a port or a range of ports as the source ports of the port mirroring.
configure	no mirror source ports PORT_LIST	This command removes a port or a range of ports from the source ports of the port mirroring.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#mirror enable
L2SWITCH(config)#mirror destination port 2
L2SWITCH(config)#mirror source ports 3-11 mode both
```

4.3.2. Web Configuration

Port Mirroring

Port Mirroring Settings

State: Disable ▾

Monitor to Port: 1 ▾

All Ports: - ▾

Source Port	Mirror Mode	Source Port	Mirror Mode
1	Disable ▾	2	Disable ▾
3	Disable ▾	4	Disable ▾
5	Disable ▾	6	Disable ▾

Apply
Refresh

Parameter	Description
State	Select Enable to turn on port mirroring or select Disable to turn it off.

Monitor Port	to	Select the port which connects to a network traffic analyzer.
All Ports		Settings in this field apply to all ports. Use this field only if you want to make some settings the same for all ports. Use this field first to set the common settings and then make adjustments on a port-by-port basis.
Source Port		This field displays the number of a port.
Mirror Mode		Select Ingress , Egress or Both to only copy the ingress (incoming), egress (outgoing) or both (incoming and outgoing) traffic from the specified source ports to the monitor port. Select Disable to not copy any traffic from the specified source ports to the monitor port.
Apply		Click Apply to take effect the settings.
Refresh		Click Refresh to begin configuring this screen afresh.

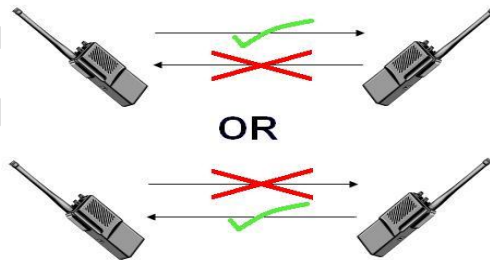
4.4. Port Settings

- Duplex mode

A **duplex** communication system is a system composed of two connected parties or devices that can communicate with one another in both directions.

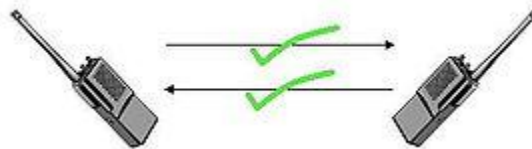
Half Duplex:

A *half-duplex* system provides for communication in both directions, but only one direction at a time (not simultaneously). Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting, before replying.



Full Duplex:

A *full-duplex*, or sometimes *double-duplex* system, allows communication in both directions, and, unlike half-duplex, allows this to happen simultaneously. Land-line telephone networks are full-duplex, since they allow both callers to speak and be heard at the same time.



- Loopback Test

A loopback test is a test in which a signal is sent from a communications device and returned (looped back) to it as a way to determine whether the device is working right or as a way to pin down a failing node in a network. One type of loopback test is performed using a special plug, called a **wrap plug** that is inserted in a port on a communications device. The effect of a wrap plug is to cause transmitted (output) data to be returned as received (input) data, simulating a complete communications circuit using a single computer.

- Auto MDI-MDIX

Auto-MDIX (automatic medium-dependent interface crossover) is a computer networking technology that automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately, thereby removing the need for crossover cables to interconnect switches or connecting PCs peer-to-peer. When it is enabled, either type of cable can be used or the interface automatically corrects any incorrect cabling. For Auto-MDIX to operate correctly, the speed on the interface and duplex setting must be set to "auto". Auto-MDIX was developed by HP engineers Dan Dove and Bruce Melvin.

The original "HP Auto-MDIX" invention was spawned one day when Bruce was looking for a cross-over cable in the lab. His efforts were being hampered and out of frustration he asked Dan "Can't you invent a way so I don't need these "cross-over cables" His inspiration led Dan to develop the method which utilizes a pseudo-random number generator to decide whether or not a network port will attach its transmitter, or its receiver to each of the twisted pairs used to Auto-Negotiate the link.

Subsequently, Dan went on to promote Auto-MDIX within the IEEE-802.3ab (1000BASE-T) standard and also develop patented algorithms for "**Forced Mode Auto-MDIX**" which allows a link to be automatically established even if the port does not auto-negotiate.

- Auto Negotiation

Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode.

If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using **half duplex** mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.

- Flow Control

A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port.

The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode.

IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.

Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.

Note: 1000 Base-T doesn't support force mode.

Default Settings

The default port Speed & Duplex is auto for all ports.

The default port Flow Control is Off for all ports.

4.4.1. CLI Configuration

Node	Command	Description
enable	show interface IFNAME	This command displays the current port configurations.
interface	show	This command displays the current port configurations.
interface	loopback (none phy)	This command specifies the loopback mode of operation for the specific port.
interface	flowcontrol (off on)	This command disables / enables the flow control for the port.
interface	speed (auto 10-full 10-half 100-full 100-half)	This command configures the speed and duplex for the port.
interface	shutdown	This command disables the specific port.
interface	no shutdown	This command enables the specific port.
interface	loopback (none mac)	This command tests the transmission or transportation infrastructure.

Example :

```
L2SWITCH#configure terminal
L2SWITCH(config)#interface gi1/0/1
L2SWITCH(config-if)#speed auto
```

4.4.2. Web Configuration

Port Settings

Port Settings

Port	State	Speed/Duplex	Flow Control
From: 1 <input type="button" value="v"/> To: 1 <input type="button" value="v"/>	Enable <input type="button" value="v"/>	Auto <input type="button" value="v"/>	Off <input type="button" value="v"/>

Port Status

Port	State	Speed/Duplex	Flow Control	Link Status
1	Enabled	Auto	Off	Link Down
2	Enabled	Auto	Off	Link Down
3	Enabled	Auto	Off	Link Down
4	Enabled	Auto	Off	Link Down
5	Enabled	Auto	Off	Link Down
6	Enabled	Auto	Off	Link Down

Parameter	Description
Port	Select a port number you want to configure on this screen.
State	Select Enable to activate the port or Disable to deactivate the port.
Speed/Duplex	Select the speed and duplex mode of the port. The choices are: <ul style="list-style-type: none"> • Auto • 10 Mbps / Full Duplex • 10 Mbps / Half Duplex • 100 Mbps / Full Duplex • 100 Mbps / Half Duplex • 1000 Mbps / Full Duplex
Flow Control	Select On to enable access to buffering resources for the port thus ensuring lossless operation across network switches. Otherwise, select Off to disable it.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Port	This field displays the port number.
State	This field displays whether the port is enabled or disabled.
Speed/Duplex	This field displays the speed either 10M , 100M or 1000M and the duplex mode Full or Half .

Flow Control	This field displays whether the port's flow control is On or Off .
Link Status	This field displays the link status of the port. If the port is up, it displays the port's speed, duplex and flow control setting. Otherwise, it displays Link Down if the port is disabled or not connected to any device.

CONFIDENTIAL

5. Advanced Settings

5.1. Bandwidth Control

5.1.1. QoS

Each egress port can support up to 8 transmit queues. Each egress transmit queue contains a list specifying the packet transmission order. Every incoming frame is forwarded to one of the 8 egress transmit queues of the assigned egress port, based on its priority. The egress port transmits packets from each of the 8 transmit queues according to a configurable scheduling algorithm, which can be a combination of Strict Priority (SP) and/or Weighted Round Robin (WRR).

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to give preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The Switch supports 802.1p priority queuing. The Switch has 8 priority queues. These priority queues are numbered from 7 (Class 7) — the highest priority queue — to 0 (Class 0) — the lowest priority queue.

The eight priority tags specified in

IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

Priority	: 0	1	2	3	4	5	6	7
Queue	: 2	0	1	3	4	5	6	7

Priority scheduling is implemented by the priority queues stated above. The Switch will empty the four hardware priority queues in order, beginning with the highest priority queue, 7, to the lowest priority queue, 0. Each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue will begin transmitting any packets it may have received.

QoS Enhancement

You can configure the Switch to prioritize traffic even if the incoming packets are not marked with IEEE 802.1p priority tags or change the existing priority tags based on the criteria you select. The Switch allows you to choose one of the following methods for assigning priority to incoming packets on the Switch:

- **802.1p Tag Priority** - Assign priority to packets based on the packet's 802.1p tagged priority.
- **Port Based QoS** - Assign priority to packets based on the incoming port on

the Switch.

- **DSCP Based QoS** - Assign priority to packets based on their Differentiated Services Code Points (DSCPs).

Note: Advanced QoS methods only affect the internal priority queue mapping for the Switch. The Switch does not modify the IEEE 802.1p value for the egress frames.

You can choose one of these ways to alter the way incoming packets are prioritized or you can choose not to use any QoS enhancement setting on the Switch.

802.1p Priority

When using 802.1p priority mechanism, the packet is examined for the presence of a valid 802.1p priority tag. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues.

Ethernet Packet:

6	6	2	42-1496	4
DA	SA	Type / Length	Data	FCS

6	6	4	2	42-1496	4
DA	SA	802.1Q Tag	Type / Length	Data	FCS

802.1Q Tag:

2 bytes		2 bytes		
Tag Protocol Identifier (TPID)		Tag Control Information (TCI)		
16 bits		3 bits	1 bit	12 bits
TPID (0x8100)		Priority	CFI	VID

- Tag Protocol Identifier (TPID): a 16-bit field set to a value of **0x8100** in order to identify the frame as an IEEE 802.1Q-tagged frame.
- Tag Control Information (TCI)
 - Priority Code Point (PCP): a 3-bit field which refers to the IEEE 802.1p priority. It indicates the frame priority level from **0 (lowest) to 7 (highest)**, which can be used to prioritize different classes of traffic (voice, video, data, etc).
 - Canonical Format Indicator (CFI): a 1-bit field. If the value of this field is 1, the MAC address is in non-canonical format. If the value is 0, the MAC address is in canonical format. It is always set to zero for Ethernet switches. CFI is used for compatibility between Ethernet and Token Ring networks. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be bridged to an untagged port.
 - VLAN Identifier (VID): a 12-bit field specifying the VLAN to which the frame belongs. A value of 0 means that the frame doesn't belong to any VLAN; in this case the 802.1Q tag specifies only a priority and is referred to as a **priority tag**. A value of hex 0xFFF is reserved for implementation use. All other values may be used as VLAN identifiers, allowing up to 4094 VLANs. On bridges, VLAN 1 is often reserved for management.

Priority Levels:

PCP: Priority Code Point.

PCP	Network Priority	Traffic Characteristics
1	0 (lowest)	Background
0	1	Best Effort
2	2	Excellent Effort
3	3	Critical Applications
4	4	Video, <100 ms latency
5	5	Video, < 10 ms latency
6	6	Internet Control
7	7 (highest)	Network Control

DiffServ (DSCP)

Differentiated Services or **DiffServ** is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing Quality of Service (**QoS**) guarantees on modern IP networks. DiffServ can, for example, be used to provide low-latency, guaranteed service (**GS**) to critical network traffic such as voice or video while providing simple best-effort traffic guarantees to non-critical services such as web traffic or file transfers.

Differentiated Services Code Point (DSCP) is a 6-bit field in the header of IP packets for packet classification purposes. DSCP replaces the outdated IP precedence, a 3-bit field in the Type of Service byte of the IP header originally used to classify and prioritize types of traffic.

When using the DiffServ priority mechanism, the packet is classified based on the DSCP field in the IP header. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues.

Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
Time to Live	Protocol	Header Checksum		
Source Address				
Destination Address				
Options			Padding	

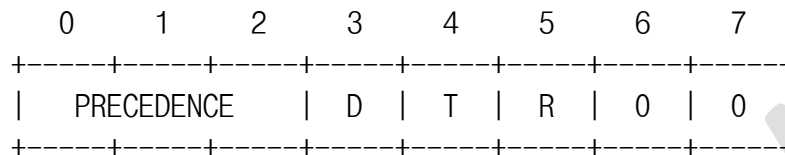
Example Internet Datagram Header

IP Header Type of Service: 8 bits

The Type of Service provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when transmitting a datagram through a particular network. Several networks offer service precedence, which somehow treats high precedence traffic as more important than other traffic (generally by accepting only traffic above certain precedence at time of high load). The major choice is a three way tradeoff between low-delay,

high-reliability, and high-throughput.

- Bits 0-2: Precedence.
- Bit 3: 0 = Normal Delay, 1 = Low Delay.
- Bits 4: 0 = Normal Throughput, 1 = High Throughput.
- Bits 5: 0 = Normal Reliability, 1 = High Reliability.
- Bit 6-7: Reserved for Future Use.



Precedence

- 111 - Network Control
- 110 - Internetwork Control
- 101 - CRITIC/ECP
- 100 - Flash Override
- 011 - Flash
- 010 - Immediate
- 001 - Priority
- 000 - Routine

The use of the Delay, Throughput, and Reliability indications may increase the cost (in some sense) of the service. In many networks better performance for one of these parameters is coupled with worse performance on another. Except for very unusual cases at most two of these three indications should be set.

The type of service is used to specify the treatment of the datagram during its transmission through the internet system. Example mappings of the internet type of service to the actual service provided on networks such as AUTODIN II, ARPANET, SATNET, and PRNET is given in "Service Mappings".

The Network Control precedence designation is intended to be used within a network only. The actual use and control of that designation is up to each network. The Internetwork Control designation is intended for use by gateway control originators only.

If the actual use of these precedence designations is of concern to a particular network, it is the responsibility of that network to control the access to, and use of, those precedence designations.

DSCP	Priority	DSCP	Priority	DSCP	Priority
0	0	1	0	2	0
...					
60	0	61	0	62	0

63 0

Example:

IP Header

DSCP=50 → 45 C8 . . .

Queuing Algorithms

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

- **Strict-Priority (SPQ)**

Strict-Queuing will empty the four hardware priority queues in order, beginning with the highest priority queue, 3, to the lowest priority queue, 0. Each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue will begin transmitting any packets it may have received.

- **Weighted round robin (WRR)**

Round Robin scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin (WRR) scheduling uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

Default Settings

- Qos mode : High First (SPQ)

The mapping of the Priority to Queue are:

```

PRIO 0 ==> COSQ 2
PRIO 1 ==> COSQ 0
PRIO 2 ==> COSQ 1
PRIO 3 ==> COSQ 3
PRIO 4 ==> COSQ 4
PRIO 5 ==> COSQ 5
PRIO 6 ==> COSQ 6
PRIO 7 ==> COSQ 7

```


The DiffServ is disabled on the switch.

DSCP	Priority	DSCP	Priority	DSCP	Priority	DSCP	Priority
----	-----	----	-----	----	-----	----	-----
00	0	01	0	02	0	03	0
04	0	05	0	06	0	07	0
08	0	09	0	10	0	11	0
12	0	13	0	14	0	15	0
16	0	17	0	18	0	19	0
20	0	21	0	22	0	23	0
24	0	25	0	26	0	27	0
28	0	29	0	30	0	31	0
32	0	33	0	34	0	35	0
36	0	37	0	38	0	39	0
40	0	41	0	42	0	43	0
44	0	45	0	46	0	47	0
48	0	49	0	50	0	51	0
52	0	53	0	54	0	55	0
56	0	57	0	58	0	59	0
60	0	61	0	62	0	63	0

5.1.1.1. CLI Configuration

Node	Command	Description
enable	show queue cos-map	This command displays the current 802.1p priority mapping to the service queue.
enable	show qos mode	This command displays the current QoS scheduling mode of IEEE 802.1p.
configure	queue cos-map PRIORITY QUEUE_ID	This command configures the 802.1p priority mapping to the service queue.
configure	no queue cos-map	This command configures the 802.1p priority mapping to the service queue to default.
configure	qos mode high-first	This command configures the QoS scheduling mode to high_first, each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets.
configure	qos mode wrp-queue weights VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE	This command configures the QoS scheduling mode to Weighted Round Robin.
interface	default-priority	This command allows the user to specify a default priority handling of untagged packets received by the Switch. The priority value entered with this

		command will be used to determine which of the hardware priority queues the packet is forwarded to. Default: 0.
interface	no default-priority	This command configures the default priority for the specific port to default (0).

5.1.1.2. Web Configuration

Port Priority

QoS

Port Priority
IP DiffServ (DSCP)
Priority/Queue Mapping
Schedule Mode

Port Priority Settings

All Ports 802.1p priority :

Port	802.1p priority	Port	802.1p priority
1	<input type="text" value="0"/>	2	<input type="text" value="0"/>
3	<input type="text" value="0"/>	4	<input type="text" value="0"/>
5	<input type="text" value="0"/>	6	<input type="text" value="0"/>

Parameter	Description
All Ports 802.1p priority	Use this field to set a priority for all ports. The value indicates packet priority and is added to the priority tag field of incoming packets. The values range from 0 (lowest priority) to 7 (highest priority).
Port	This field displays the number of a port.
802.1p Priority	Select a priority for packets received by the port. Only packets without a 802.1p priority tagged will be applied the priority you set here.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

IP DiffServ (DSCP)

QoS

Port Priority
IP DiffServ (DSCP)
Priority/Queue Mapping
Schedule Mode

DSCP Settings

Mode Tag Over DSCP ▾

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

Apply
Refresh

Parameter	Description
Mode	“Tag Over DSCP” or “DSCP Over Tag”. “Tag Over DSCP” means the 802.1p tag has higher priority than DSCP.
Priority	This field displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority).
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Priority/Queue Mapping

QoS

Port Priority
IP DiffServ (DSCP)
Priority/Queue Mapping
Schedule Mode

Priority/Queue Mapping Settings

Reset to default

Priority	Queue ID
0	1 ▼
1	0 ▼
2	2 ▼
3	3 ▼
4	4 ▼
5	5 ▼
6	6 ▼
7	7 ▼

Apply

Refresh

Parameter	Description
Reset to Default	Click this button to reset the priority to queue mappings to the defaults.
Priority	This field displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority).
Queue ID	Select the number of a queue for packets with the priority level.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

Schedule Mode

QoS

Port Priority
IP DiffServ (DSCP)
Priority/Queue Mapping
Schedule Mode

Schedule Mode Settings

Schedule Mode: ▼

Queue ID	Weight Value (Range:1~255)
0	<input type="text"/>
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>

Parameter	Description
Schedule Mode	<p>Select Strict Priority (SP) or Weighted Round Robin (WRR). Note: Queue weights can only be changed when Weighted Round Robin is selected.</p> <p>Weighted Round Robin scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue Weight field). Queues with larger weights get more service than queues with smaller weights.</p>
Queue ID	<p>This field indicates which Queue (0 to 7) you are configuring. Queue 0 has the lowest priority and Queue 7 the highest priority.</p>
Weight Value	<p>You can only configure the queue weights when Weighted Round Robin is selected. Bandwidth is divided across the different traffic queues according to their weights.</p> <p>Note: If you want to use Strict Priority but want to change the weights for the queues, configure them with Weighted Round Robin selected first and then change the scheduling method to Strict Priority.</p>
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

5.1.2. Rate Limitation

5.1.2.1. Storm Control

A broadcast storm means that your network is overwhelmed with constant broadcast or multicast traffic. Broadcast storms can eventually lead to a complete loss of network connectivity as the packets proliferate.

Storm Control protects the Switch bandwidth from flooding packets, including broadcast packets, multicast packets, and destination lookup failure (DLF). The **Rate** is a threshold that limits the total number of the selected type of packets. For example, if the broadcast and multicast options are selected, the total amount of packets per second for those two types will not exceed the limit value.

Broadcast storm control limits the number of broadcast, multicast and unknown unicast (also referred to as Destination Lookup Failure or DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and unknown unicast packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and unknown unicast packets in your network.

Storm Control unit : 625 pps.

Default Settings

Broadcast Storm Control : 652 pps.
 Multicast Storm Control : None.
 DLF Storm Control : 652 pps.

5.1.2.1.1. CLI Configuration

Node	Command	Description
enable	show storm-control	This command displays the current storm control configurations.
configure	storm-control rate RATE_LIMIT type (bcast mcast DLF bcast+mcast bcast+DLF mcast+DLF bcast+mcast+DLF) ports PORTLISTS	This command enables the bandwidth limit for broadcast or multicast or DLF packets and set the limitation.
configure	no storm-control type (bcast mcast DLF bcast+mcast bcast+DLF mcast+DLF bcast+mcast+DLF) ports PORTLISTS	This command disables the bandwidth limit for broadcast or multicast or DLF packets.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#storm-control rate 1 type broadcast ports 1-6
L2SWITCH(config)#storm-control rate 1 type multicast ports 1-6
L2SWITCH(config)#storm-control rate 1 type DLF ports 1-6
```

5.1.2.1.2. Web Configuration

Rate Limitation

Storm Control
Bandwidth Limitation

Storm Control Settings

Port	Rate	Type
From: <input type="text" value="1"/> <input type="button" value="v"/> To: <input type="text" value="1"/> <input type="button" value="v"/>	<input type="text" value="0"/> (units)	<input type="text" value="Multicast"/> <input type="button" value="v"/>

(Disable:0. One unit is about 652 pps.)

Storm Control Status

Port	Rate(units)	Multicast	Broadcast	DLF	Port	Rate(units)	Multicast	Broadcast	DLF
1	1	Disable	Enable	Enable	2	1	Disable	Enable	Enable
3	1	Disable	Enable	Enable	4	1	Disable	Enable	Enable
5	1	Disable	Enable	Enable	6	1	Disable	Enable	Enable

Parameter	Description
Port	Select the port number for which you want to configure storm control settings.
Rate	Select the number of packets (of the type specified in the Type field) per second the Switch can receive per second.
Type	Select Broadcast - to specify a limit for the amount of broadcast packets received per second. Multicast - to specify a limit for the amount of multicast packets received per second. DLF - to specify a limit for the amount of DLF packets received per second.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

5.1.2.2. Rate Limitation

The rate limitation is used to control the rate of traffic sent or received on a network interface.

Rate Limitation unit: Mbs.

Default Setting: All ports' Ingress and Egress rate limitation are disabled.

5.1.2.2.1. CLI Configuration

Node	Command	Description
enable	show bandwidth-limit	This command displays the current rate control configurations.
configure	bandwidth-limit egress RATE_LIMIT ports PORTLISTS	This command enables the bandwidth limit for outgoing packets and set the limitation.
configure	no bandwidth-limit egress ports PORTLISTS	This command disables the bandwidth limit for outgoing packets.
configure	bandwidth-limit ingress RATE_LIMIT ports PORTLISTS	This command enables the bandwidth limit for incoming packets and set the limitation.
configure	no bandwidth-limit ingress ports PORTLISTS	This command disables the bandwidth limit for incoming packets.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#bandwidth-limit egress 1 ports 1-26
L2SWITCH(config)#bandwidth-limit ingress 1 ports 1-26
```

5.1.2.2.2. Web Configuration

Rate Limitation

Storm Control
Bandwidth Limitation

Bandwidth Limitation Settings

Port	Ingress	Egress
From: <input type="text" value="1"/> To: <input type="text" value="1"/>	<input type="text" value="0"/> (Mbs)	<input type="text" value="0"/> (Mbs)

(Disable:0)

Bandwidth Limitation Status

Port	Ingress (Mbs)	Egress (Mbs)	Port	Ingress (Mbs)	Egress (Mbs)
1	0	0	2	0	0
3	0	0	4	0	0
5	0	0	6	0	0

Parameter	Description
Port	Selects a port that you want to configure.
Ingress	Configures the rate limitation for the ingress packets.
Egress	Configures the rate limitation for the egress packets.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

5.2. VLAN

5.2.1. MAC-based VLAN

The MAC base VLAN allows users to create VLAN with MAC address. The MAC address can be the leading three or more bytes of the MAC address. For example, 00:0b:04 or 00:03:04:05 or 00:01:02:03:04:05.

When the Switch receives packets, it will compare MAC-based VLAN configures. If the SA is matched the MAC-based VLAN configures, the Switch replace the VLAN with user configured and them forward them.

For example: Configurations: 00:0B:04, VLAN=23, Priority=2.

The packets with SA=00:0B:04:xx:xx:xx will be forwarded to VLAN 22 member ports.

Notices: The 802.1Q port base VLAN should be created first.

5.2.1.1. CLI Configuration

Node	Command	Description
enable	show mac-vlan	This command displays the all of the mac-vlan configurations.
configure	mac-vlan STRINGS vlan VLANID priority <0-7>	This command creates a mac-vlan entry with the leading three or more bytes of mac address and the VLAN and the priority.
configure	no mac-vlan entry STRINGS	This command deletes a mac-vlan entry.
configure	no mac-vlan all	This command deletes all of the mac-vlan entries.

Where the STRINGS is the leading three or more bytes of the mac address.

For example:

00:0B:04:11:22:33

Example:

```
L2SWITCH(config)#mac-vlan 00:01:02:03:04   vlan 111 priority 1
L2SWITCH(config)#mac-vlan 00:01:02:22:04   vlan 121 priority 1
L2SWITCH(config)#mac-vlan 00:01:22:22:04:05 vlan 221 priority 1
```

5.2.1.2. Web Configuration

MAC VLAN

MAC VLAN Settings

MAC Address	VLAN	Priority
<input type="text"/>	<input type="text"/> (1~4094)	0 <input type="button" value="v"/>

Ex: 00:0B:04 will only filter 3 bytes of source mac address.
 00:0B:04:11:22 will only filter 5 bytes of source mac address.
 00:0B:04:11:22:33 will filter all bytes of source mac address.

MAC VLAN Table

Index	MAC Address	VLAN	Priority	Action
1	00:01:02	22	3	<input type="button" value="Delete"/>

Parameter	Description
MAC Address	Configures the leading three or more bytes of the MAC address.
VLAN	Configures the VLAN.
Priority	Configures the 802.1Q priority.
Action	Click the “Delete” button to delete the protocol VLAN profile.

5.2.2. Port Isolation

The port isolation is a port-based virtual LAN feature. It partitions the switching ports into virtual private domains designated on a per port basis. Data switching outside of the port’s private domain is not allowed. It will ignore the packets’ tag VLAN information.

This feature is a per port setting to configure the egress port(s) for the specific port to forward its received packets. If the CPU port (port 0) is not an egress port for a specific port, the host connected to the specific port cannot manage the Switch.

If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.

Example: If you want to allow port-1 and port-3 to talk to each other, you must configure as below:

```
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#port-isolation ports 3
L2SWITCH(config-if)#exit
; Allow the port-1 to send its ingress packets to port-3.
```

```
L2SWITCH(config)#interface 1/0/3
L2SWITCH(config-if)#port-isolation ports 1
L2SWITCH(config-if)#exit
; Allow the port-3 to send its ingress packets to port-1
```

Default Settings

(Port-0=CPU) .

Egress Port		Egress Port	
Port	01234567890	Port	01234567890
1	WWWWWWW	2	WWWWWWW
3	WWWWWWW	4	WWWWWWW
5	WWWWWWW	6	WWWWWWW
7	WWWWWWW	8	WWWWWWW
9	WWWWWWW	10	WWWWWWW

5.2.2.1. CLI Configuration

Node	Command	Description
enable	show port-isolation	This command displays the current port isolation configurations. “V” indicates the port’s packets can be sent to that port. “-” indicates the port’s packets cannot be sent to that port.
interface	port-isolation ports PORTLISTS	This command configures a port or a range of ports to egress traffic from the specific port.
interface	no port-isolation	This command configures all ports to egress traffic from the specific port.

Example:

```
L2SWITCH(config)#interface 1/0/2
L2SWITCH(config-if)#port-isolation ports 3-10
```

5.2.2.2. Web Configuration

Port Isolation

Port Isolation Settings

Port From: To:

Egress Port :

Select All Deselect All

1 3 5 7

2 4 6 8 9 10 0 (CPU)

Port Isolation Status

Port	Egress Port										
	0	1	2	3	4	5	6	7	8	9	10
1	v	v	v	v	v	v	v	v	v	v	v
2	v	v	v	v	v	v	v	v	v	v	v
3	v	v	v	v	v	v	v	v	v	v	v
4	v	v	v	v	v	v	v	v	v	v	v
5	v	v	v	v	v	v	v	v	v	v	v
6	v	v	v	v	v	v	v	v	v	v	v

Parameter	Description
Port	Select a port number to configure its port isolation settings. Select All Ports to configure the port isolation settings for all ports on the Switch.
Egress Port	An egress port is an outgoing port, that is, a port through which a data packet leaves. Selecting a port as an outgoing port means it will communicate with the port currently being configured.
Select All/ Deselect All	Click Select All to mark all ports as egress ports and permit traffic. Click Deselect All to unmark all ports and isolate them. Deselecting all ports means the port being configured cannot communicate with any other port.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last saved setting.
Port Isolation Status	“V” indicates the port’s packets can be sent to that port. “-” indicates the port’s packets cannot be sent to that port.

5.2.3. 802.1Q VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

VID- VLAN ID is the identification of the VLAN, which is basically used by the standard 802.1Q. It has 12 bits and allow the identification of 4096 (2^{12}) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 bytes	3 bits	1 bit	12 bits

- Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

- 802.1Q Port base VLAN

With port-based VLAN membership, the port is assigned to a specific VLAN independent of the user or system attached to the port. This means all users attached to the port should be members of the same VLAN. The network administrator typically performs the VLAN assignment. The port configuration is static and cannot be automatically changed to another VLAN without manual reconfiguration.

As with other VLAN approaches, the packets forwarded using this method do not leak into other VLAN domains on the network. After a port has been assigned to a VLAN, the port cannot send to or receive from devices in another VLAN without the intervention of a Layer 3 device.

The device that is attached to the port likely has no understanding that a VLAN exists. The device simply knows that it is a member of a subnet and that the device should be able to talk to all other members of the subnet by simply sending information to the cable segment. The switch is responsible for identifying that the information came from a specific VLAN and for ensuring that the information gets to all other members of the VLAN. The switch is further responsible for ensuring that ports in a different VLAN do not receive the information.

This approach is quite simple, fast, and easy to manage in that there are no complex lookup tables required for VLAN segmentation. If port-to-VLAN association is done with an application-specific integrated circuit (ASIC), the performance is very good. An ASIC allows the port-to-VLAN mapping to be done at the hardware level.

Default Settings

- The default PVID is 1 for all ports.
- The default Acceptable Frame is All for all ports.
- All ports join in the VLAN 1.

Notices

- The maximum VLAN group is 4094.

5.2.3.1. CLI Configuration

Node	Command	Description
enable	show vlan VLANID	This command displays the VLAN configurations.
configure	vlan <1~4094>	This command enables a VLAN and enters the VLAN node.
configure	no vlan <1~4094>	This command deletes a VLAN.
vlan	show	This command displays the current VLAN configurations.
vlan	fixed PORT_LIST	This command assigns ports for permanent member of the VLAN group.
vlan	forbidden PORT_LIST	This command assigns ports to prohibit the port to join in the VLAN group. The ports should be one/some of the permanent members of the vlan

		group.
vlan	untagged PORT_LIST	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the vlan group.
vlan	name STRING	This command assigns a name for the specific VLAN. The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_). The maximum length of the name is 16 characters.
vlan	no fixed	This command removes all fixed member from the vlan.
vlan	no forbidden	This command removes all forbidden member from the vlan.
vlan	no untagged	This command removes all untagged member from the vlan.
vlan	no name	This command configures the vlan name to default. Note: The default vlan name is "VLAN"+vlan_ID, VLAN1, VLAN2,...
vlan	acceptable frame type (all tagged untagged)	This command configures the acceptable frame type. all – acceptable all frame types.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#vlan 2
L2SWITCH(config-vlan)#fixed 1-6
L2SWITCH(config-vlan)#untagged 1-3
```

5.2.3.2. Web Configuration

VLAN Settings

VLAN

VLAN Settings
Tag Settings
Port Settings

VLAN Settings

VLAN ID	VLAN Name	Member Port
<input type="text"/>	<input type="text"/>	<input style="width: 90%;" type="text"/>

VLAN List

VLAN ID	VLAN Name	VLAN Status	Member Port	Action
1	VLAN1	Static	1-10	

Parameter	Description
-----------	-------------

VLAN ID	Enter the VLAN ID for this entry; the valid range is between 1 and 4094.
VLAN Name	Enter a descriptive name for the VLAN for identification purposes. The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_). The maximum length of the name is 16 characters.
Member Port	Enter the port numbers you want the Switch to assign to the VLAN as members. You can designate multiple port numbers individually by using a comma (,) and by range with a hyphen (-).
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
VLAN List	
VLAN ID	This field displays the index number of the VLAN entry. Click the number to modify the VLAN.
VLAN Name	This field displays the name of the VLAN.
VLAN Status	This field displays the status of the VLAN. Static or Dynamic (802.1Q VLAN).
Member Port	This field displays which ports have been assigned as members of the VLAN. This will display None if no ports have been assigned.
Action	Click Delete to remove the VLAN. The VLAN 1 cannot be deleted.

Tag Settings

VLAN

VLAN Settings
Tag Settings
Port Settings

Tag Settings

VLAN ID

Tag Port :

Select All
 Deselect All

<input type="checkbox"/> 1	<input type="checkbox"/> 3	<input type="checkbox"/> 5	<input type="checkbox"/> 7	<input type="checkbox"/> 9
<input type="checkbox"/> 2	<input type="checkbox"/> 4	<input type="checkbox"/> 6	<input type="checkbox"/> 8	<input type="checkbox"/> 10

Tag Status

VLAN ID	Tag Ports	UnTag Ports
1		1-10

Parameter	Description
VLAN ID	Select a VLAN ID to configure its port tagging settings.
Tag Port	Selecting a port which is a member of the selected VLAN ID will make it a tag port. This means the port will tag all outgoing frames transmitted with the VLAN ID.
Select All	Click Select All to mark all member ports as tag ports.
Deselect All	Click Deselect All to mark all member ports as untag ports.
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
Tag Status	
VLAN ID	This field displays the VLAN ID.
Tag Ports	This field displays the ports that have been assigned as tag ports.
Untag Ports	This field displays the ports that have been assigned as untag ports.

Port Settings

VLAN

VLAN Settings
Tag Settings
Port Settings

Port Settings

Port	PVID	Acceptable Frame
From: <input type="text" value="1"/> <input type="button" value="v"/> To: <input type="text" value="1"/> <input type="button" value="v"/>	<input type="text" value="1"/> <input type="button" value="v"/>	<input type="text" value="All"/> <input type="button" value="v"/>

Port Status

Port	PVID	Acceptable Frame	Port	PVID	Acceptable Frame
1	1	All	2	1	All
3	1	All	4	1	All
5	1	All	6	1	All

Parameter	Description
Port	Select a port number to configure from the drop-down box. Select All to configure all ports at the same time.
PVID	Select a PVID (Port VLAN ID number) from the drop-down

	box.
Acceptable Frame	Specify the type of frames allowed on a port. Choices are All , VLAN Untagged Only or VLAN Tagged Only . Select All from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select VLAN Tagged Only to accept only tagged frames on this port. All untagged frames will be dropped. Select VLAN Untagged Only to accept only untagged frames on this port. All tagged frames will be dropped.
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
Port Status	
Port	This field displays the port number.
PVID	This field displays the Port VLAN ID number.
Acceptable Frame	This field displays the type of frames allowed on the port. This will either display All or VLAN Tagged Only or VLAN Untagged Only .

5.2.4. GARP/GVRP

GARP and GVRP are industry-standard protocols that are described in IEEE 802.1p. GVRP is a GARP application that provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports.

With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches that are connected through **802.1Q trunk ports**.

GVRP makes use of GID and GIP, which provide the common state machine descriptions and the common information propagation mechanisms defined for use in GARP-based applications. GVRP runs only on 802.1Q trunk links. GVRP prunes trunk links so that only active VLANs will be sent across trunk connections. GVRP expects to hear join messages from the switches before it will add a VLAN to the trunk. GVRP updates and hold timers can be altered. GVRP ports run in various modes to control how they will prune VLANs. GVRP can be configured to dynamically add and manage VLANs to the VLAN database for trunking purposes.

In other words, GVRP allows the propagation of VLAN information from device to device. With GVRP, a single switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically.

An endnode can be plugged into any switch and be connected to that endnode's desired VLAN. For endnodes to make use of GVRP, they need GVRP-aware Network Interface Cards (NICs). The GVRP-aware NIC is configured with the desired VLAN or VLANs, then connected to a GVRP-enabled switch. The NIC communicates with the switch, and VLAN connectivity is established between the NIC and switch.

Registration Mode:

- Normal : The **normal** registration mode allows dynamic creation (if dynamic VLAN creation is enabled), registration, and deregistration of VLANs on the trunk port. Normal mode is the default.
- Forbidden: The **forbidden** registration mode deregisters all VLANs (except VLAN 1) and prevents any further VLAN creation or registration on the trunk port.
- Fixed : The **fixed** registration mode allows manual creation and registration of VLANs, prevents VLAN deregistration, and registers all known VLANs on other ports on the trunk port. (Same as the static VLAN)

GVRP Timer:

Join Timer : Specifies the maximum number of milliseconds the interface waits before sending VLAN advertisements.

Leave Timer : Specifies the number of milliseconds an interface waits after receiving a leave message before the interface leaves the VLAN specified in the message.

Leaveall Timer: Specifies the interval in milliseconds at which Leave All messages are sent on interfaces. Leave All messages help to maintain current GVRP VLAN membership information in the network.

The value for **leave** must be greater than three times the **join** value (**leave** >= **join** * 3).
The value for **leaveall** must be greater than the value for **leave** (**leaveall** > **leave**).

Default Settings

The default port Join Time is 20 for all ports.
The default port Leave Time is 60 for all ports.
The default port Leaveall Time is 1000 for all ports.
The default port Hold Time is 10 for all ports.

5.2.4.1. CLI Configuration

Node	Command	Description
enable	show gvrp configuration	This command displays the GVRP configurations.
enable	show gvrp statistics	This command displays the GVRP configurations on a port or all ports.
enable	show garp timer	This command displays the timers for the GARP.
configure	gvrp (disable enable)	This command disables / enables the GVRP on the

		switch.
configure	no gvrp configuration	This command set GVRP configuration to its defaults.
interface	gvrp (disable enable)	This command disables / enables the GVRP on the specific port.
interface	gvrp registration (normal forbidden)	This command configures the registration mode for the GVRP on the specific port.
interface	no gvrp configuration	This command set GVRP configuration to its defaults for the specific port.
interface	garp join-time VALUE leave-time VALUE leaveall-time VALUE	This command configures the join time / leaves time / leave all time for the GARP on the specific port.
interface	no garp time	This command configures the join time / leaves time / leaves all time to default for the GARP on the specific port.

5.2.4.2. Web Configuration

GVRP Settings

GARP VLAN Registration Protocol

GVRP
GARP Timer

GVRP Settings

GVRP State Disable ▾

Port	State	Registration Mode
From: 1 ▾ To: 1 ▾	Disable ▾	Normal ▾

Apply Refresh

GVRP Status

Port	State	Registration Mode	Port	State	Registration Mode
1	Disabled	-	2	Disabled	-
3	Disabled	-	4	Disabled	-
5	Disabled	-	6	Disabled	-

Parameter	Description
GVRP State	Select Enable to activate GVRP function to exchange VLAN configuration information with other GVRP switches. Select Disable to deactivate the feature.
Port	Select the port that you want to configure the GVRP settings.

State	Select Enable to activate the port GVRP function. Select Disable to deactivate the port GVRP function.
Registration Mode	Select Normal to allows dynamic creation (if dynamic VLAN creation is enabled), registration, and deregistration of VLANs on the trunk port. Select Forbidden to deregister all VLANs (except VLAN 1) and prevents any further VLAN creation or registration on the trunk port.

GARP Timer

GARP VLAN Registration Protocol

GVRP
GARP Timer

GARP Timer Settings

Port	Join Time	Leave Time	Leave All Time
From: 1 <input type="button" value="v"/> To: 1 <input type="button" value="v"/>	20 <input type="text"/>	60 <input type="text"/>	1000 <input type="text"/>

2*Join Time < Leave Time < Leave All Time
Time unit:(centi-sec)

GARP Timer Status

Port	Join Time	Hold Time	Leave Time	Leave All Time
1	20	10	60	1000
2	20	10	60	1000
3	20	10	60	1000
4	20	10	60	1000
5	20	10	60	1000
6	20	10	60	1000

Parameter	Description
Join Time	Specifies the maximum number of milliseconds the interface waits before sending VLAN advertisements.
Leave Time	Specifies the number of milliseconds an interface waits after receiving a leave message before the interface leaves the VLAN specified in the message.
Leaveall Time	Specifies the interval in milliseconds at which Leave All messages are sent on interfaces. Leave All messages help to maintain current GVRP VLAN membership information in the network.

5.2.5. Protocol-Based VLAN

The Protocol based VLAN allows users to create VLAN with packet frame type. The packet frame type can be one of the three frame types: EthernetII, NonLLC-SNAP and LLC-SNAP. If configuring the Ethernet II frame type, the configuration will be more detail with the ethernet type.

When the user configures the protocol VLAN as LLC-SNAP, VLAN:22, ports list: 1-3.

If the Switch receives packets with LLC-SNAP frame type from port 1 to 3, the packets' VLAN will be replaced with VLAN 22 and be forwarded to VLAN 22 member ports.

Notices: The 802.1Q port base VLAN should be created first.

5.2.5.1. CLI Configuration

Node	Command	Description
enable	show protocol-vlan	This command displays the all of the protocol-vlan configurations.
configure	protocol-vlan frame-type ethernetII ether-type STRINGS vlan VLANID ports PORTLISTS	This command creates a protocol-vlan entry with ethernetII frame type.
configure	protocol-vlan frame-type nonLLC-SNAP vlan VLANID ports PORTLISTS	This command creates a protocol-vlan entry with nonLLC-SNAP frame type.
configure	protocol-vlan frame-type LLC-SNAP vlan VLANID ports PORTLISTS	This command creates a protocol-vlan entry with LLC-SNAP frame type.
configure	no protocol-vlan frame-type ethernetII ether-type STRINGS vlan VLANID	This command deletes a protocol-vlan entry with ethernetII frame type.
configure	no protocol-vlan frame-type nonLLC-SNAP vlan VLANID	This command deletes a protocol-vlan entry with nonLLC-SNAP frame type and vlan.
configure	no protocol-vlan frame-type LLC-SNAP vlan VLANID	This command deletes a protocol-vlan entry with LLC-SNAP frame type and vlan.
configure	no protocol-vlan all	This command deletes all of the protocol-vlan entries.

Example:

```
L2SWITCH(config)#protocol-vlan frame-type LLC-SNAP vlan 12 ports 22-23
L2SWITCH(config)#protocol-vlan frame-type nonLLC-SNAP vlan 13 ports 22-23
L2SWITCH(config)#protocol-vlan frame-type ethernetII ether-type 0800 vlan 13 ports 22-23
```


5.2.5.2. Web Configuration

Protocol VLAN

Protocol VLAN Settings

Frame Type	Ethernet Type	VLAN	Port List
<div style="border: 1px solid #ccc; padding: 2px;"> ▼ EthernetII EthernetII NonLLC-SNAP LLC-SNAP </div>	<input style="width: 80%;" type="text"/>	<input style="width: 80%;" type="text"/> (1~4094)	<input style="width: 80%;" type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>			

Protocol VLAN Table

Index	Frame Type	Ethernet Type	VLAN	Port List	Action
1	EthernetII	0x8888	22	1-4	<input type="button" value="Delete"/>

Parameter	Description
Frame Type	Select one of three frame types, “EthernetIU” and “NonLLC-SNAP” and “LLC-SNAP”.
Ethernet type	Input the Ethernet type for the EthernetII frame type.
VLAN	Configure the VLAN ID.
Port List	Configure the member ports.
Action	Click the “Delete” button to delete the protocol VLAN profile.

5.2.6. Q-in-Q VLAN (VLAN Stacking)

Q-in-Q tunneling is also known as VLAN stacking. Both of them use 802.1q double tagging technology. Q-in-Q is required by ISPs (Internet Service Provider) that require Transparent LAN services (TLS), and the service provider has their own set of VLAN, independent of customer VLANs. Typically, each service provider VLAN interconnects a group of sites belonging to a customer. However, a service provider VLAN could also be shared by a set of customers sharing the same end points and quality of service requirements of the VLAN. Double tagging is considered to be a relatively simpler way of implementing transparent LAN. This is accomplished by encapsulating Ethernet Frame. A second or outer VLAN tag is inserted in Ethernet frames sent over the ingress PE (Provider Edge). This VLAN tag corresponds to the VLAN of the Service Provider (SP). When the frame reaches the destination PE, the SP VLAN is stripped off. The DA of the encapsulated frame and the VLAN ID are used to take further L2 decisions, similar to an Ethernet frame arriving from a physical Ethernet port. The SP VLAN tag determines the VPLS (Virtual Private LAN Service) membership. Double tagging aggregates multiple VLANs within another VLAN and provides a private, dedicated Ethernet connection between customers to reach their subnet transparently across multiple networks. Thus service providers can create their own VLANs without interfering with customer VLANs by using double tagging. This allows them to connect customers to ISPs and ASPs

(Application Service Provider).

The ports that are connected to the service provider VLANs are called tunnel ports, and the ports that are connected to the customer VLANs are called access (subscriber/customer) ports. When a port is configured as tunnel port, all the outgoing packets on this port will be sent out with SPVLAN (SPVID and 1p priority) tag. The incoming packet can have two tags (SPVLAN + CVLAN), one tag (SPVLAN or CVLAN), or no tag. In all cases, the packet is sent out with a SPVLAN tag. When a port is configured as an access port, the incoming traffic can have only a CVLAN (CVID and 1p priority) tag or no tag. Hence, all the packets that are being sent out of access ports will be untagged or single tagged (CVLAN). When a port is configured as a normal port, it will ignore the frames with double tagging.

Double Tagging Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

TPID	Priority	VID
------	----------	-----

TPID (Tag Protocol Identifier) is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. The value of this field is 0x8100 as defined in IEEE 802.1Q. Other vendors may use a different value, such as 0x9100.

Tunnel TPID is the VLAN stacking tag type the Switch adds to the outgoing frames sent through a Tunnel Port of the service provider's edge devices

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for. "0" is the lowest priority level and "7" is the highest.

VID is the VLAN ID. SP VID is the VID for the second or outer (service provider's) VLAN tag. CVID is the VID for the first or inner (Customer's) VLAN tag.

The frame formats for an untagged Ethernet frame; a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) are shown as following.

untagged frame	DA	SA	Len or Etype	Data	FCS						
single-tagged frame	DA	SA	TPID	P	VID	Len or Etype	Data	FCS			
double-tagged frame	DA	SA	Tunnel TPID	P	VID	TPID	P	VID	Len or Etype	Data	FCS

DA: Destination Address

SA: Source Address

Tunnel TPID: Tag Protocol Identifier added on a tunnel port
 P: 802.1p priority
 VID: VLAN ID
 Len or Etype: Length or Ethernet frame type
 Data: Frame data
 FCS: Frame Check Sequence

VLAN Stacking Port Roles

Each port can have three VLAN stacking “roles”, Normal, Access Port and Tunnel Port.

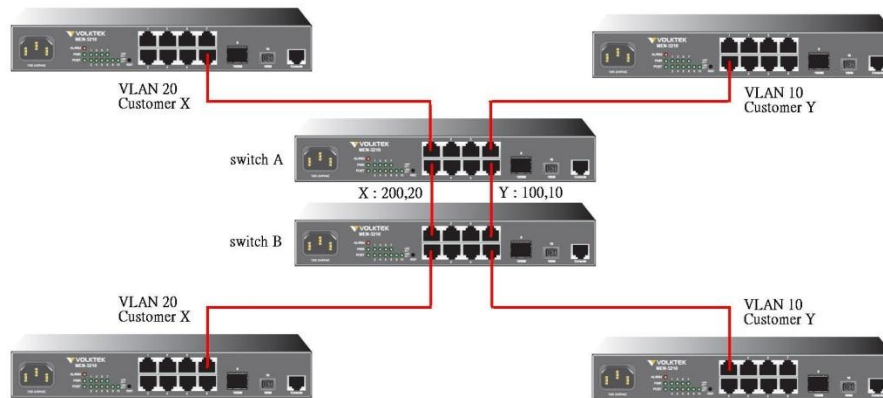
- Select **Normal** for “regular” (non-VLAN stacking) IEEE 802.1Q frame switching.
- Select **Access Port** for ingress ports on the service provider's edge devices. The incoming frame is treated as "untagged", so a second VLAN tag (outer VLAN tag) can be added.
- Select **Tunnel Port** for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by SP VID).

NOTE: In order to have the double tagged frames switching correctly, user has to configure a service provider’s VLAN (SPVLAN) on the Q-in-Q switch. Then, the double tagged frames can be switched according to the SP VID. The SPVLAN should include all the related Tunnel and Access ports. Also, user has to configure the Tunnel posts as tagged ports and the Access ports as untagged ports.

Port-based Q-in-Q

Q-in-Q encapsulation is to convert a single tagged 802.1Q packet into a double tagged Q-in-Q packet. The Q-in-Q encapsulation can be based on port or traffic. Port-based Q-in-Q is to encapsulate all the packets incoming to a port with the same SPVID outer tag. The mode is more inflexible.

In the following example figure, both **X** and **Y** are Service Provider’s Network (**SPN**) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag **100** to distinguish customer **X** and tag **200** to distinguish customer **Y** at edge device A and then stripping those tags at edge device B as the data frames leave the network.

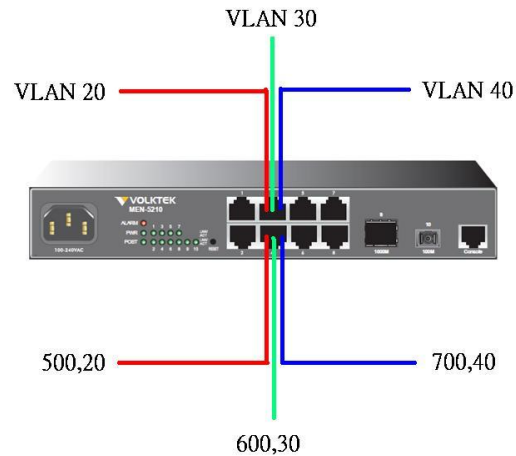


This example shows how to configure switch A with ports 1 on the Switch to tag incoming frames with the service provider's VID of 200 (ports are connected to customer X network) and configure port 7 to service provider's VID of 100 (ports are connected to customer Y network). This example also shows how to set the priority for port 1 to 3 and port 7 to 4.

```
L2SWITCH(config)# vlan-stacking port-based
L2SWITCH(config)# vlan-stacking tpid-table index 2 value 88a8
L2SWITCH(config)# vlan 10
L2SWITCH(config-vlan)# fixed 7,8
L2SWITCH(config-vlan)# tagged 7
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 100
L2SWITCH(config-vlan)# fixed 7,8
L2SWITCH(config-vlan)# tagged 8
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 20
L2SWITCH(config-vlan)# fixed 1,2
L2SWITCH(config-vlan)# tagged 1
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 200
L2SWITCH(config-vlan)# fixed 1,2
L2SWITCH(config-vlan)# tagged 2
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# interface gigaethernet1/0/1
L2SWITCH(config-if)# vlan-stacking port-based role access
L2SWITCH(config-if)# vlan-stacking spvid 200
L2SWITCH(config-if)# vlan-stacking priority 3
L2SWITCH(config)# interface gigaethernet1/0/2
L2SWITCH(config-if)# vlan-stacking port-based role tunnel
L2SWITCH(config-if)# vlan-stacking tunnel-tpid index 2
L2SWITCH(config)# interface gigaethernet1/0/7
L2SWITCH(config-if)# vlan-stacking port-based role access
L2SWITCH(config-if)# vlan-stacking spvid 100
L2SWITCH(config-if)# vlan-stacking priority 4
L2SWITCH(config)# interface gigaethernet1/0/8
L2SWITCH(config-if)# vlan-stacking port-based role tunnel
L2SWITCH(config-if)# vlan-stacking tunnel-tpid index 2
L2SWITCH(config-if)# exite
L2SWITCH(config)# exit
L2SWITCH# show vlan-stacking
L2SWITCH# show vlan-stacking tpid-table
L2SWITCH# show vlan-stacking portbased-qinq
```

Selective Q-in-Q

The traffic based Q-in-Q is also called Selective Q-in-Q. Selective Q-in-Q allows the Switch to add different outer VLAN tags to the incoming frames received on one port according to their inner VLAN tags. In the Selective Q-in-Q mode, switch performs traffic classification for the traffic incoming to a port based on the VLAN ID. When a user uses different VLAN IDs for different services, traffic can be classified according to the VLAN ID. For example, the VLAN ID 100 for surfing on the internet by PC. The VLAN ID 200 of IPTV. The VLAN ID 300 of VIP customers. After receiving user data, the switch labels the traffic of surfing on the Internet by PC with 500 as a SPVID outer tag, IPTV with 600, and VIP customers with 700.



This following example shows how to configure ports 3 on the Switch to tag incoming frames with the different service provider's VID and priority.

```
L2SWITCH(config)# vlan-stacking selective
L2SWITCH(config)# vlan-stacking tpid-table index 6 value 9100
L2SWITCH(config)# vlan 20
L2SWITCH(config-vlan)# fixed 3,4
L2SWITCH(config-vlan)# tagged 3
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 30
L2SWITCH(config-vlan)# fixed 3,4
L2SWITCH(config-vlan)# tagged 3
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 40
L2SWITCH(config-vlan)# fixed 3,4
L2SWITCH(config-vlan)# tagged 3
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 500
L2SWITCH(config-vlan)# fixed 3,4
L2SWITCH(config-vlan)# tagged 4
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 600
L2SWITCH(config-vlan)# fixed 3,4
L2SWITCH(config-vlan)# tagged 4
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 700
L2SWITCH(config-vlan)# fixed 3,4
L2SWITCH(config-vlan)# tagged 4
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan-stacking selective-qinq rule1
L2SWITCH(config-qinq)# cvids 20
L2SWITCH(config-qinq)# priority 2
L2SWITCH(config-qinq)# spvid 500
```



```

L2SWITCH(config-qinq)# access-ports 3
L2SWITCH(config-qinq)# tunnel-ports 4
L2SWITCH(config-qinq)# active
L2SWITCH(config-qinq)# show
L2SWITCH(config-qinq)# exit
L2SWITCH(config)# vlan-stacking selective-qinq rule2
L2SWITCH(config-qinq)# cvids 30
L2SWITCH(config-qinq)# priority 5
L2SWITCH(config-qinq)# spvid 600
L2SWITCH(config-qinq)# access-ports 3
L2SWITCH(config-qinq)# tunnel-ports 4
L2SWITCH(config-qinq)# active
L2SWITCH(config-qinq)# show
L2SWITCH(config-qinq)# exit
L2SWITCH(config)# vlan-stacking selective-qinq rule3
L2SWITCH(config-qinq)# cvids 40
L2SWITCH(config-qinq)# priority 7
L2SWITCH(config-qinq)# spvid 700
L2SWITCH(config-qinq)# access-ports 3
L2SWITCH(config-qinq)# tunnel-ports 4
L2SWITCH(config-qinq)# active
L2SWITCH(config-qinq)# show
L2SWITCH(config-qinq)# exit
L2SWITCH(config)# interface interface 1/0/4
L2SWITCH(config-if)# vlan-stacking tunnel-tpid index 6
L2SWITCH(config-if)# exit
L2SWITCH(config)# exit
L2SWITCH# show vlan-stacking
L2SWITCH# show vlan-stacking tpid-table
L2SWITCH# show vlan-stacking selective-qinq

```

Default Setting: VLAN Stacking is disabled.

5.2.6.1. CLI Configuration

Node	Command	Description
enable	show vlan-stacking	This command displays the current vlan-stacking type.
enable	show vlan-stacking selective-qinq	This command displays the selective Q-in-Q configurations.
enable	show vlan-stacking portbased-qinq	This command displays the port-based q-in-Q configurations.
enable	show vlan-stacking tpid-inform	This command displays the TPID configurations.
config	vlan-stacking (disable port-based selective)	This command disables the vlan stacking or enables the vlan-stacking with port-based or selective on the switch.
config	vlan-stacking selective-qinq STRINGS	This command creates a selective Q-in-Q profile with the name.
config	no vlan-stacking selective-qinq STRINGS	This command removes the selective Q-in-Q profile with the name.
config	vlan-stacking tpid-table index <2-6> value STRINGS	This command configures TPID table.
interface	vlan-stacking port-based	This command sets the priority in port based

	priority <0~7>	Q-in-Q.
interface	vlan-stacking port-based role (tunnel access normal)	This command sets VLAN stacking port role.
interface	vlan-stacking port-based spvid <1~4096>	This command sets the service provider's VID of the specified port.
interface	vlan-stacking tunnel-tpid index <1-6>	This command sets TPID for a Q-in-Q tunnel port.
qinq	active	This command enables the selective Q-in-Q profile.
qinq	inactive	This command disables the selective Q-in-Q profile.
qinq	cvid VLANID	This command specifies the customer's VLAN range on the incoming packets.
qinq	spvid VLANID	This command sets the service provider's VLAN ID for outgoing packets in selective Q-in-Q.
qinq	priority <0-7>	This command sets priority in selective Q-in-Q.
qinq	access-ports PORTLISTS	This command specifies the access ports to apply the rule.
qinq	tunnel-ports PORTLISTS	This command specifies the tunnel ports to apply the rule.
qinq	end	The command exits the CLI Q-in-Q node and enters the CLI enable node.
qinq	exit	The command exits the CLI Q-in-Q node and enter the CLI configure node.
qinq	show	The command shows the current selective Q-in-Q profile configurations.

5.2.6.2. Web Configuration

VLAN Stacking

Q-in-Q

VLAN Stacking
Port-based Q-in-Q
Selective Q-in-Q

VLAN Stacking Setting

Action: Disable

Tunnel TPID Index	TPID
1 (Default)	8100 (0000~ffff)

Port	Tunnel TPID Index
From: 1 To: 1	1 (Default)

Apply Refresh

VLAN Stacking Status

Tunnel TPID Index	TPID
1	8100
2	8100
3	8100
4	8100
5	8100
6	8100

Port	Tunnel TPID Index (TPID)	Port	Tunnel TPID Index (TPID)
1	1 (8100)	2	1 (8100)
3	1 (8100)	4	1 (8100)
5	1 (8100)	6	1 (8100)

Parameter	Description
Action	Select one of the three modes, Disable or Port-Based or Selective for the VLAN stacking.
Configures the TPID Table: The TPID table has 6 entries.	
Tunnel TPID Index	Selects the table index.
TPID	Configures the TPID.
Configures the Port TPID:	
Port	Selects a port or a range of ports which you want to configure.
Tunnel TPID Index	Configures the index of the TPID Table for the specific ports.

Port-Based Q-in-Q

Q-in-Q

VLAN Stacking | Port-based Q-in-Q | Selective Q-in-Q

Port-based Q-in-Q

Port	Role	SPVID	Priority
From: <input type="text" value="1"/> To: <input type="text" value="1"/>	<input type="text" value="Normal"/> <ul style="list-style-type: none"> Normal Access Tunnel 	<input type="text" value="1"/> (1~4094)	<input type="text" value="0"/>

Port-based Q-in-Q Status

Port	Role	SPVID	Priority	Port	Role	SPVID	Priority
1	Normal	1	0	2	Normal	1	0
3	Normal	1	0	4	Normal	1	0
5	Normal	1	0	6	Normal	1	0

Parameter	Description
Port	Selects a port or a range of ports which you want to configure.
Role	Selects one of the three roles, Normal and Access and Tunnel , for the specific ports.
SPVID	Configures the service provider's VLAN.
Priority	Configures the priority for the specific ports.

Selective Q-in-Q

Q-in-Q

VLAN Stacking | Port-based Q-in-Q | Selective Q-in-Q

Selective Q-in-Q Setting

Name	<input type="text"/>
Access Ports	<input type="text"/> (ex. 1,3,5-10)
Tunnel Ports	<input type="text"/> (ex. 1,3,5-10)
CVID	<input type="text"/> (Range: 1~4094)
SPVID	<input type="text"/> (Range: 1~4094)
Priority	<input type="text" value="0"/>
Action	<input type="text" value="Disable"/>

Selective Q-in-Q Status

No.	Name	Access Ports	Tunnel Ports	CVID	SPVID	Priority	Action	Delete

Parameter	Description
Name	Configures the selective Q-in-Q profile name.
Access Ports	Configures a port or a range of ports for the access ports.
Tunnel Ports	Configures a port or a range of ports for the tunnel ports.
CVID	Configures a customer's VLAN.
SPVID	Configures a service provider's VLAN.
Priority	Configures an 802.1Q priority for the profile.
Action	Enables / Disables the profile.

5.3. IGMP Snooping

5.3.1. IGMP Snooping

The IGMP snooping is for multicast traffic. The Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

The Switch can perform IGMP snooping on up to 4094 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first VLANs that send IGMP packets.

This is referred to as auto mode. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

Immediate Leave

When you enable IGMP Immediate-Leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN. (Immediate Leave is only supported on IGMP Version 2 hosts).

The switch uses IGMP snooping Immediate Leave to remove from the forwarding table an interface that sends a leave message without the switch sending group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Immediate Leave ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

Fast Leave

The switch allow user to configure a delay time. When the delay time is expired, the switch removes the interface from the multicast group.

Last Member Query Interval

Last Member Query Interval: The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages.

Without Immediate Leave, when the switch receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP specific query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership.

IGMP Querier

There is normally only one Querier per physical network. All multicast routers start up as a Querier on each attached network. If a multicast router hears a Query message from a router **with a lower IP address**, it MUST become a Non-Querier on that network. If a router has not heard a Query message from another router for [Other Querier Present Interval], it resumes the role of Querier. Routers periodically [Query Interval] send a General Query on each attached network for which this router is the Querier, to solicit membership information. On startup, a router SHOULD send [Startup Query Count] General Queries spaced closely together [Startup Query Interval] in order to quickly and reliably determine membership information. A General Query is addressed to the all-systems multicast group (224.0.0.1), has a Group Address field of 0, and has a Max Response Time of [Query Response Interval].

Port IGMP Querier Mode

- **Auto:**

The Switch uses the port as an IGMP query port if the port receives IGMP query packets.

- **Fixed:**

The Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s).

The Switch always forwards the client's **report/leave** packets to the port. Normally, the port is connected to an IGMP server.

- **Edge:**

The Switch does not use the port as an IGMP query port.

The IGMP query packets received by this port will be dropped.
Normally, the port is connected to an IGMP client.

Note: The Switch will forward the IGMP join and leave packets to the query port.

Configurations:

Users can enable / disable the IGMP Snooping on the Switch. Users also can enable / disable the IGMP Snooping on a specific VLAN. If the IGMP Snooping on the Switch is disabled, the IGMP Snooping is disabled on all VLANs even some of the VLAN IGMP Snooping are enabled.

Default Settings

- If received packets are not received after 400 seconds, all multicast entries will be deleted.
- The default global IGMP snooping state is disabled.
- The default VLAN IGMP snooping state is disabled for all VLANs.
- The unknown multicast packets will be Dropped.
- The default port Immediate Leave state is disabled for all ports.
- The default port Querier Mode state is auto for all ports.
- The IGMP snooping Report Suppression is disabled.

Notices

- There are a global state and per VLAN states.
When the global state is disabled, the IGMP Snooping on the Switch is disabled even per VLAN states are enabled.
When the global state is enabled, user must enable per VLAN states to enable the IGMP Snooping on the specific VLAN.

5.3.1.1. CLI Configuration

Node	Command	Description
enable	show igmp-snooping	This command displays the current IGMP snooping configurations.
enable	show igmp-counters	This command displays the current IGMP snooping counters.
enable	show igmp-counters (port vlan)	This command displays the current IGMP snooping counters per port or per vlan.
configure	igmp-snooping (disable enable)	This command disables / enables the IGMP snooping on the switch.
configure	igmp-snooping vlan VLAN_ID	This command enables the IGMP snooping function on a VLAN or range of VLANs.
configure	no igmp-snooping vlan VLAN_ID	This command disables the IGMP snooping function on a VLAN or range of VLANs.
configure	igmp-snooping querier (disable enable)	This command disables / enables the IGMP snooping querier on the switch.
configure	igmp-snooping	This command enables the IGMP snooping querier

	querier vlan VLAN_ID	function on a VLAN or range of VLANs.
configure	no igmp-snooping querier vlan VLAN_ID	This command disables the IGMP snooping querier function on a VLAN or range of VLANs.
configure	igmp-snooping unknown-multicast (drop flooding)	This command configures the process for unknown multicast packets when the IGMP snooping function is enabled. <i>drop</i> : Drop all of the unknown multicast packets.
configure	igmp-snooping report-suppression (disable enable)	This command disables / enables the IGMP snooping report suppression function on the switch.
configure	clear igmp-counters	This command clears the IGMP snooping counters.
configure	clear igmp-counters (port vlan)	This command clears the IGMP snooping counters for port or vlan.
interface	igmp-querier-mode (auto fixed edge)	This command specifies whether or not and under what conditions the port(s) is (are) IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. (Default:auto)
interface	igmp-immediate-leave	This command enables the IGMP Snooping immediate leave function for the specific interface.
interface	no igmp-immediate-leave	This command disables the IGMP Snooping immediate leave function for the specific interface.
interface	no igmp-group-limit VALUE	This command configures the maximum groups for the specific interface.
interface	no igmp-group-limit	This command removes the limitation of the maximum groups for the specific interface.

Example:

```

L2SWITCH(config)#igmp-snooping enable
L2SWITCH(config)#igmp-snooping vlan 1
L2SWITCH(config)#igmp-snooping querier enable
L2SWITCH(config)#igmp-snooping querier vlan 1
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#igmp-immediate-leave
L2SWITCH(config-if)# igmp-querier-mode fixed
    
```


5.3.1.2. Web Configuration

General Settings

IGMP Snooping

General Settings
Port Settings

IGMP Snooping Settings

IGMP Snooping State Enable

Report Suppression State Disable

IGMP Snooping VLAN State Add 1,100

Unknown Multicast Packets Drop

IGMP Snooping Status

IGMP Snooping State	Enabled
Report Suppression State	Disabled
IGMP Snooping VLAN State	1,100
Unknown Multicast Packets	Drop

Parameter	Description
IGMP Snooping State	Select Enable to activate IGMP Snooping to forward group multicast traffic only to ports that are members of that group. Select Disable to deactivate the feature.
Report Suppression State	Select Enable/Disable to activate/deactivate IGMP Snooping report suppression function.
IGMP Snooping VLAN State	Select Add and enter VLANs upon which the Switch is to perform IGMP snooping. The valid range of VLAN IDs is between 1 and 4094. Use a comma (,) or hyphen (-) to specify more than one VLANs. Select Delete and enter VLANs on which to have the Switch not perform IGMP snooping.
Unknown Multicast Packets	Specify the action to perform when the Switch receives an unknown multicast frame. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last saved setting.
IGMP Snooping State	This field displays whether IGMP snooping is globally enabled or disabled.
Report Suppression State	This field displays whether IGMP snooping report suppression is enabled or disabled.

IGMP Snooping VLAN State	This field displays VLANs on which the Switch is to perform IGMP snooping. None displays if you have not enabled IGMP snooping on any port yet.
Unknown Multicast Packets	This field displays whether the Switch is set to discard or flood unknown multicast packets.

Port Settings

IGMP Snooping

General Settings | Port Settings | Querier Settings

Port Settings

Port	Querier Mode	Immediate Leave	Group Limit
From: <input type="text" value="1"/> To: <input type="text" value="1"/>	<input type="text" value="Auto"/>	<input type="text" value="Disable"/>	<input type="text" value="256"/>

Port Status

Port	Querier Mode	Immediate Leave	Group Counts	Port	Querier Mode	Immediate Leave	Group Counts
1	Auto	Disable	0/256	2	Auto	Disable	0/256
3	Auto	Disable	0/256	4	Auto	Disable	0/256
5	Auto	Disable	0/256	6	Auto	Disable	0/256

Parameter	Description
Querier Mode	Select the desired setting, Auto , Fixed , or Edge . Auto means the Switch uses the port as an IGMP query port if the port receives IGMP query packets. Fixed means the Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). Edge means the Switch does not use the port as an IGMP query port. In this case, the Switch does not keep a record of an IGMP router being connected to this port and the Switch does not forward IGMP join or leave packets to this port.
Immediate Leave	Select individual ports on which to enable immediate leave.
Group Limit	Configures the maximum group for the port or a range of ports.
Apply	Click Apply to apply the settings.
Refresh	Click this to reset the fields.
Port	The port ID.

Querier Mode	The Querier mode setting for the specific port.
Immediate Leave	The Immediate Leave setting for the specific port.
Group Counts	The current joining group count and the maximum group count.

5.3.2. MVR

MVR refers to **Multicast VLAN Registration** that enables a media server to transmit multicast stream in a single multicast VLAN while clients receiving multicast VLAN stream can reside in different VLANs. Clients in different VLANs intend to join or leave the multicast group simply by sending the IGMP Join/leave message to a **receiver** port. The receiver port belonging to one of the multicast groups can receive multicast stream from media server. Without support of MVR, the Multicast stream from media server and subscriber must reside in the same VLAN.

- Source ports : The Stream source ports.
- Receiver ports : The Client ports.
- Tagged ports : Configure the tagged ports for source ports or receiver ports.

MVR Mode

- **Dynamic Mode:**
If we select the dynamic mode in MVR setting, IGMP report message transmitted from the receiver port will be forwarded to a multicast router through its source port. Multicast router knows which multicast groups exist on which interface dynamically.
- **Compatible mode:**
If we select the dynamic mode in MVR setting, IGMP report message transmitted from the receiver port will not be transmitted to a multicast router.

Multicast router must be statically configured.

Operation Mode

- **Join Operation:**
A subscriber sends an IGMP report message to the switch to join the appropriate multicast. The next depends on whether the IGMP report matches the switch configured multicast MAC address. If it matches, the switch CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of MVLAN.
- **Leave Operation:**
Subscriber sends an IGMP leave message to the switch to leave the multicast. The switch CPU sends an IGMP group-specific query through the receiver port VLAN. If there is another subscriber in the VLAN, subscriber must respond within the max response time. If there is no subscriber, the switch would eliminate this receiver

port.

- **Immediate Leave Operation:**

Subscriber sends an IGMP leave message to the switch to leave the multicast. Subscribers do not need to wait for the switch CPU to send an IGMP group-specific query through the receiver port VLAN. The switch will immediately eliminate this receiver port.

Figure-1:

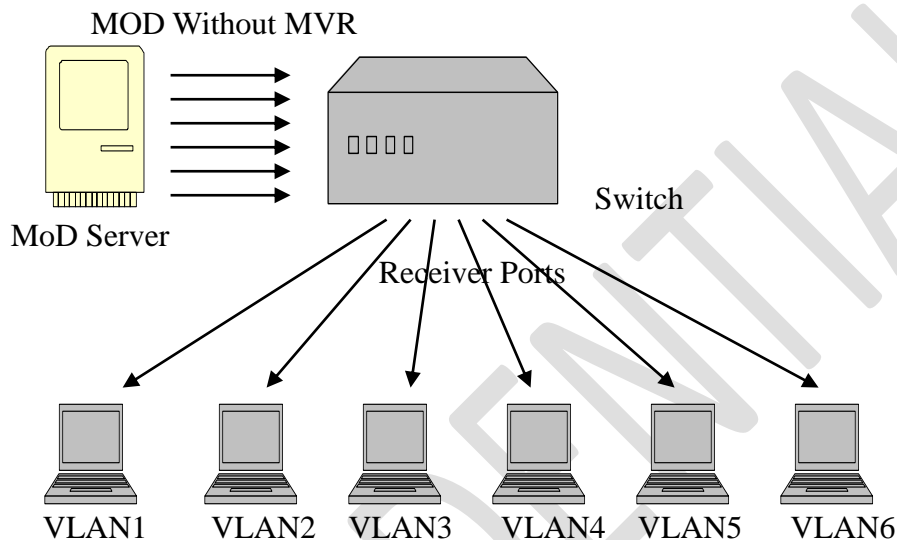
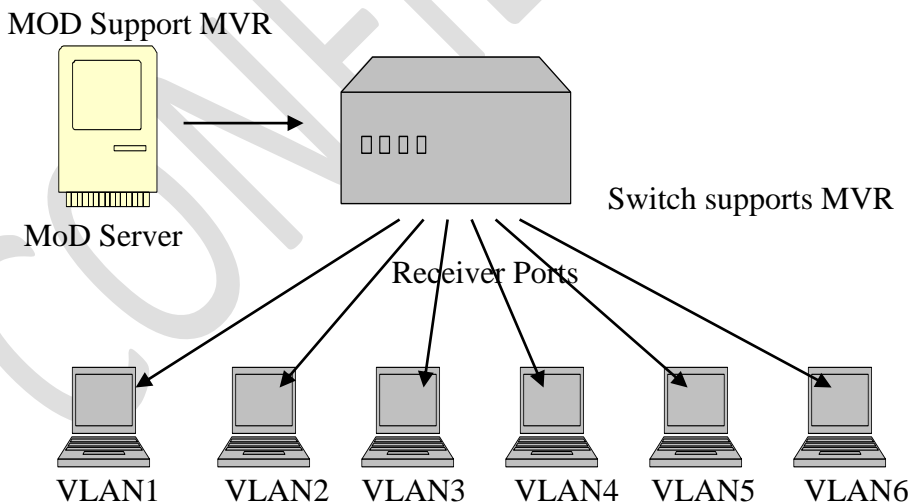


Figure-2:



Default Settings

There is no MVR vlan.

Default configuration for a new MVR:

MVR VLAN Information

VLAN ID : 2

Name : MVR2
 Active : Enabled
 Mode : Dynamic
 Source Port(s) : None
 Receiver Port(s) : None
 Tagged Port(s) : None

The Switch allows user to create up to 250 groups.

The Switch allows user to create up to 16 MVRs.

Notices

- IGMP snooping and MVR can be independently enabled.
- IGMP snooping and MVR use the same IGMP timers.
- MVR can recognize IGMPv3 reports.
- About the IGMPv3 report, switch doesn't treat those group records with the following group record types as membership reports. Those group record types are `MODE_IS_INCLUDE`, `CHANGE_TO_INCLUDE_MODE`, `ALLOW_NEW_SOURCES` and `BLOCK_OLD_SOURCES`.
- Don't use the group address X.0.0.1 for your multicast stream. It is because the system detects and records the 224.0.0.1 for dynamic querier port. The group address X.0.0.1 may conflict with 224.0.0.1.
- Because the lower 23 bits of the 28-bit multicast IP address are mapped into the 23 bits of available Ethernet address space. When you configure group address, the Switch compares the lower 23 bits only.
- CLI command "*group 1 start-address 224.1.1.1 6*", it creates 6 groups. That is, one IP, one group.
- The MVR name should be the combination of the digit or the alphabet.
- The group name should be the combination of the digit or the alphabet.

5.3.2.1. CLI Configuration

Node	Command	Description
enable	show mvr	This command displays the current MVR configurations.
enable	show mvr vlan VLAN_ID	This command displays the current MVR configurations of the specific VLAN.
enable	show igmp-snooping	This command displays the current IGMP snooping configurations.
configure	mvr VLAN_ID	This command configures the MVR configurations for the specific VLAN.
configure	no mvr VLAN_ID	This command disables the MVR configurations for the specific VLAN.
MVR	group NAME	This command configures group configurations for the MVR.
MVR	no group NAME	This command removes the group configurations from the MVR.
MVR	inactive	This command disables the MVR settings.

MVR	no inactive	This command enables the MVR settings.
MVR	mode (dynamic compatible)	This command configures the mode for the MVR. <ul style="list-style-type: none"> ● Dynamic: Sends IGMP report to all MVR source ports in the multicast VLAN. ● Compatible: Sets the Switch not to send IGMP report.
MVR	name STRING	This command configures the name for the MVR.
MVR	no name	This command configures the default name for the MVR.
MVR	receiver-port PORTLIST	This command sets the receiver port(s). Normally the source ports are connected to the streaming client.
MVR	no receiver-port PORTLIST	This command removes a port or range of ports from the receiver port(s).
MVR	source-port PORTLIST	This command sets the source port(s). Normally the source ports are connected to the streaming server.
MVR	no source-port PORTLIST	This command removes a port or range of ports from the source port(s).
MVR	tagged PORTLIST	This command sets the tagged port(s). Same as the VLAN tagged port.
MVR	no tagged PORTLIST	This command removes a port or range of ports from the tagged port(s).

5.3.2.2. Web Configuration

MVR Settings

Multicast VLAN Registration

MVR Settings
Group Settings

[Querier Settings](#)

VLAN ID

State Enable

Source Ports (ex. 1,3,5-10)

Receiver Ports (ex. 1,3,5-10)

Tagged Ports (ex. 1,3,5-10)

Name

Mode Dynamic

MVR Status

VLAN ID	99	Name	99
State	Enabled	Mode	Dynamic
Source Ports	1		
Receiver Ports	3		
Tagged Ports	1		

Parameter	Description
VLAN ID	Configures a VLAN.
NAME	Configures a name for the MVR.
Action	Enables / Disables the MVR.
Mode	Configures the mode for the MVR.
Source Ports	Configures the source port(s) for the MVR. Normally the source ports are connected to the streaming server.
Receive Ports	Configures the receive port(s) for the MVR. Normally the source ports are connected to the streaming client
Tagged Ports	Configures the tagged port(s) for the MVR. Same as the VLAN tagged port.

Group Settings

Multicast VLAN Registration

MVR Settings
Group Settings

Group Settings

MVR VLAN

Group Name

Start Address Quantity:

Group Status

MVR VLAN	2		
Group Name	222	Address Range	224.1.1.1~10 <input type="button" value="Delete"/>

Parameter	Description
MVR VLAN	Select a MVR VLAN.
Group Name	Configures the group name.
Start Address	Configures the multicast start address.
Quantity	Configures the quantity of the multicast address.

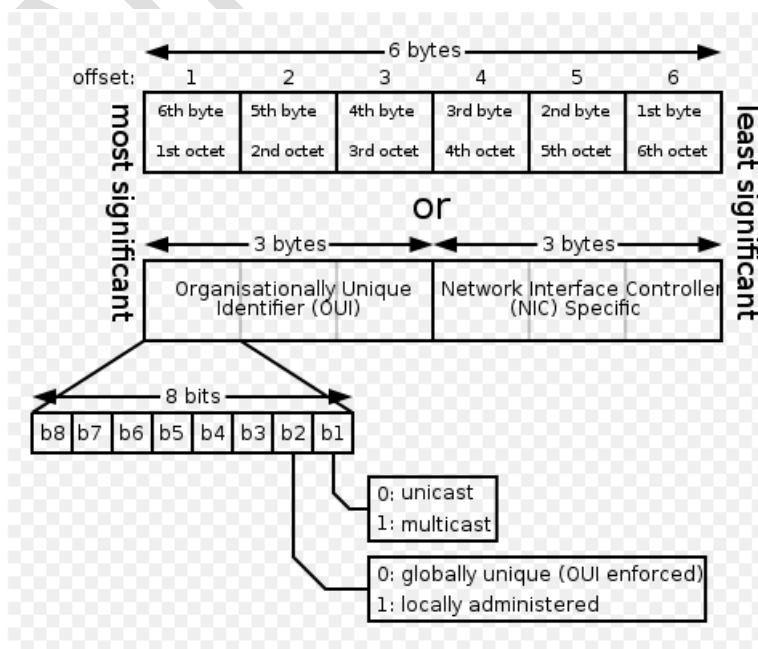
5.3.3. Multicast Address

A multicast address is associated with a group of interested receivers. According to RFC 3171, addresses 224.0.0.0 to 239.255.255.255, the former Class D addresses, are designated as multicast addresses in IPv4.

The IANA owns the OUI MAC address 01:00:5e, therefore multicast packets are delivered by using the Ethernet MAC address range 01:00:5e:00:00:00 - 01:00:5e:7f:ff:ff. This is 23 bits of available address space.

The first octet (01) includes the broadcast/multicast bit. The lower 23 bits of the 28-bit multicast IP address are mapped into the 23 bits of available Ethernet address space. This means that there is ambiguity in delivering packets. If two hosts on the same subnet each subscribe to a different multicast group whose address differs only in the first 5 bits, Ethernet packets for both multicast groups will be delivered to both hosts, requiring the network software in the hosts to discard the unrequired packets.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.



IP multicast address	Description
224.0.0.0	Base address (reserved)
224.0.0.1	The All Hosts multicast group that contains all systems on the same network segment
224.0.0.2	The All Routers multicast group that contains all routers on the same network segment
224.0.0.5	The Open Shortest Path First (OSPF) AllSPFRouters address. Used to send Hello packets to all OSPF routers on a network segment
224.0.0.6	The OSPF AllDRouters address. Used to send OSPF routing information to OSPF designated routers on a network segment
224.0.0.9	The <u>RIP</u> version 2 group address. Used to send routing information using the RIP protocol to all RIP v2-aware routers on a network segment
224.0.0.10	EIGRP group address. Used to send EIGRP routing information to all EIGRP routers on a network segment
224.0.0.13	PIM Version 2 (Protocol Independent Multicast)
224.0.0.18	Virtual Router Redundancy Protocol
224.0.0.19 - 21	IS-IS over IP
224.0.0.22	IGMP Version 3 (Internet Group Management Protocol)
224.0.0.102	Hot Standby Router Protocol Version 2
224.0.0.251	Multicast DNS address
224.0.0.252	Link-local Multicast Name Resolution address
224.0.1.1	Network Time Protocol address
224.0.1.39	Cisco Auto-RP-Announce address
224.0.1.40	Cisco Auto-RP-Discovery address
224.0.1.41	H.323 Gatekeeper discovery address

5.3.3.1. CLI Configuration

Node	Command	Description
enable	show mac-address-table multicast	This command displays the current static/dynamic multicast address entries.
configure	mac-address-table multicast MACADDR vlan VLAN_ID ports PORTLIST	This command configures a static multicast entry.
configure	no mac-address-table multicast MACADDR	This command removes a static multicast entry from the address table.

5.3.3.2. Web Configuration

Multicast Address

Static Multicast Address Settings

VLAN ID	MAC Address	Port
1	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>

Multicast Address Table

VLAN ID	MAC Address	Status	Port	Action
1	01:00:5e:22:33:44	Static	1-6	<input type="button" value="Delete"/>

Total counts : 1

Parameter	Description
VLAN ID	Configures the VLAN that you want to configure.
MAC Address	Configures the multicast MAC which will not be aged out. Valid format is hh:hh:hh:hh:hh:hh.
Port	Configures the member port for the multicast address.
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.

5.4. DHCP Relay

Because the *DHCPDISCOVER* message is a broadcast message, and broadcasts only cross other segments when they are explicitly routed, you might have to configure a DHCP Relay Agent on the router interface so that all DHCPDISCOVER messages can be forwarded to your DHCP server. Alternatively, you can configure the router to forward DHCP messages and BOOTP message. *In a routed network, you would need DHCP Relay Agents if you plan to implement only one DHCP server.*

The DHCP Relay that either a host or an IP router that listens for DHCP client messages being broadcast on a subnet and then forwards those DHCP messages directly to a configured DHCP server. The DHCP server sends DHCP response messages directly back to the DHCP relay agent, which then forwards them to the DHCP client. The DHCP administrator uses DHCP relay agents to centralize DHCP servers, avoiding the need for a DHCP server on each subnet.

Most of the time in small networks DHCP uses broadcasts however there are some circumstances where unicast addresses will be used. When networks have a single DHCP

server that provides IP addresses for multiple subnets. A router for such a subnet receives the DHCP broadcasts, converts them to unicast (with a destination MAC/IP address of the configured DHCP server, source MAC/IP of the router itself). The field identified as the GIADDR in the main DHCP page is populated with the IP address of the interface on the router it received the DHCP request on. The DHCP server uses the **GIADDR** field to identify the subnet the device and select an IP address from the correct pool. The DHCP server then sends the DHCP OFFER back to the router via unicast which then converts it back to a broadcast and out to the correct subnet containing the device requesting an address.

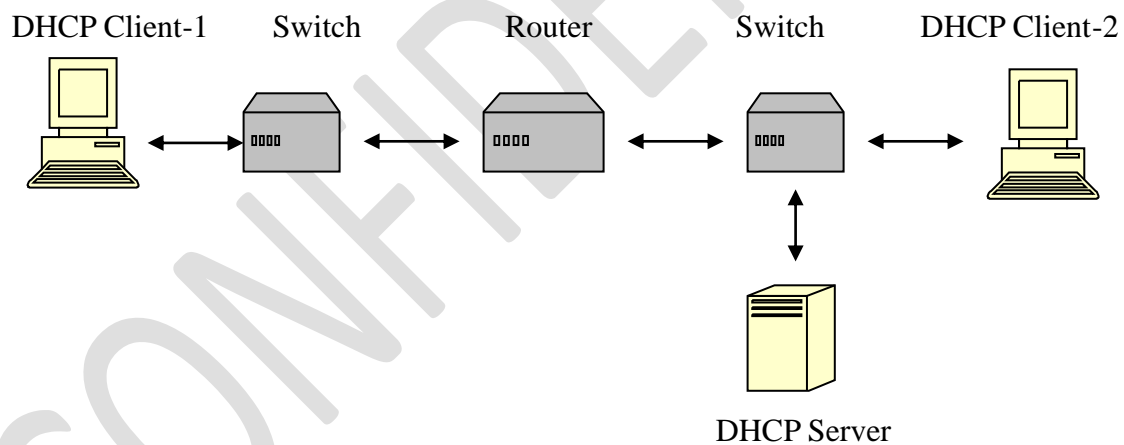
Configurations:

Users can enable / disable the DHCP Relay on the Switch. Users also can enable / disable the DHCP Relay on a specific VLAN. If the DHCP Relay on the Switch is disabled, the DHCP Relay is disabled on all VLANs even some of the VLAN DHCP Relay are enabled.

Applications

- Application-1 (Over a Router)

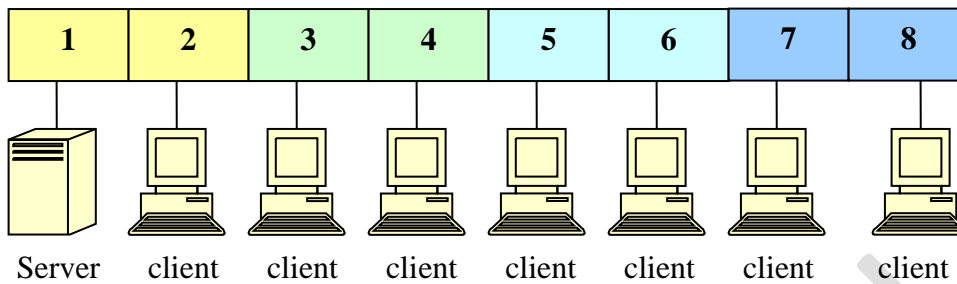
The DHCP client-1 and DHCP client-2 are located in different IP segments. But they allocate IP address from the same DHCP server.



- Application-2 (Local in different VLANs)

The DHCP client-1 and DHCP client-2 are located in different VLAN. But they allocate IP address from the same DHCP server.

Switch DHCP Relay agent



VLAN 1: port 1, 2 (Management VLAN)

VLAN 2: port 3, 4

VLAN 3: port 5, 6

VLAN 4: port 7, 8

DHCP Server → Port 1.

DHCP Client → Port 2, 3, 4, 5, 6, 7, 8.

Result: Hosts connected to port 2,3,4,5,6,7,8 can get IP from DHCP server.

Note: The DHCP Server must connect to the management VLAN member ports.
The DHCP Relay in management VLAN should be enabled.

DHCP Relay Option 82

DHCP Option 82 is the “DHCP Relay Agent Information Option”. Option 82 was designed to allow a DHCP Relay Agent to insert circuit specific information into a request that is being forwarded to a DHCP server. Specifically the option works by setting two sub-options: Circuit ID and Remote ID.

The DHCP option 82 is working on the DHCP snooping **or/and** DHCP relay.

The switch will monitor the DHCP packets and append some information as below to the DHCPDISCOVER and DHCPREQUEST packets. The switch will remove the DHCP Option 82 from the DHCPOFFER and DHCPACK packets. The DHCP server will assign IP domain to the client dependent on these information.

The maximum length of the information is 32 characters.

In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP option-82 feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

When you enable the DHCP snooping information option 82 on the switch, this sequence of events occurs:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote-ID suboption) and the port identifier, vlan-mod-port, from which the packet is received (the circuit-ID suboption).
- If the IP address of the relay agent is configured, the switch adds the IP address in the DHCP packet.
- The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
- The DHCP server receives the packet. If the server is option-82 capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server **echoes** the option-82 field in the DHCP reply.
- The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The switch **removes** the option-82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

Option Frame Format:

Code	Len	Agent Information Field					
82	N	i1	i2	i3	i4	...	iN

The Agent Information field consists of a sequence of SubOpt/Length/Value tuples for each sub-option, encoded in the following manner:

Sub-Option	Len	Sub-Option Value					
1	N	s1	s2	s3	s4	...	sN

DHCP Agent Sub-option Code	Sub-Option Description
----- 1	----- Agent Circuit ID Sub-option
2	Agent Remote ID Sub-option

Circuit ID Suboption Frame Format:

Suboption Type	Length	Circuit ID Type	Length	VLAN	Module	Port
1	6	0	4	2	1	1

Remote ID Suboption Frame Format:

Suboption Type	Length	Circuit ID Type	Length	MAC Address
----------------	--------	-----------------	--------	-------------

2	8	0	6	6
---	---	---	---	---

Format:

Circuit ID Sub-option Format:

Code	Len	Suboption Type	Length	Slot ID	Port ID	Vlan ID	Information
0x52	0x0c	0x01	0x0a	0x01	0x01	0x0002	justin

Default Settings

- The default global DHCP relay state is disabled.
- The default VLAN DHCP relay state is disabled for all VLANs.
- The default DHCP server is 0.0.0.0
- The default global DHCP option 82 state is disabled.
- The default information of the DHCP option 82 is NULL.
- Maximum length of the option information : 32 characters.

5.4.1. CLI Configuration

Node	Command	Description
enable	show dhcp relay	This command displays the current configurations for the DHCP relay.
configure	dhcp relay (disable enable)	This command disables / enables the DHCP relay on the switch.
configure	dhcp relay vlan VLAN_RANGE	This command enables the DHCP relay function on a VLAN or a range of VLANs.
configure	no dhcp relay vlan VLAN_RANGE	This command disables the DHCP relay function on a VLAN or a range of VLANs.
configure	dhcp helper-address IP_ADDRESS	This command configures the DHCP server's IP address.
configure	no dhcp helper-address	This command removes the DHCP server's IP address.
configure	dhcp option82 (disable enable)	This command disables / enables the DHCP relay option 82 on the switch.
configure	dhcp option82 information STRING	This command configures the information for the DHCP relay option 82.
configure	no dhcp option82 information	This command removes the information for the DHCP relay option 82.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)# interface eth0
L2SWITCH(config-if)# ip address 172.20.1.101/24
L2SWITCH(config-if)# ip address default-gateway 172.20.1.1
L2SWITCH(config)#dhcp relay enable
L2SWITCH(config)# dhcp relay vlan 1
L2SWITCH(config)# dhcp helper-address 172.20.1.1
```

```
L2SWITCH(config)#dhcp option82 enable
L2SWITCH(config)#dhcp option82 information Justin
```

5.4.2. Web Configuration

DHCP Relay

DHCP Relay Settings

State	Disable	<input type="button" value="v"/>
VLAN State	Add	<input type="button" value="v"/> <input style="width: 100%;" type="text"/>
DHCP Server IP	0.0.0.0	<input style="width: 100%;" type="text"/>
Option 82 State	Disable	<input type="button" value="v"/>
Option 82 Information	<input style="width: 100%;" type="text"/>	

DHCP Relay Status

DHCP Relay State	Disabled
Enabled on VLAN	None
DHCP Server IP	0.0.0.0
Option 82 State	Disabled
Option 82 Information	None

Parameter		Description
State		Enables / disables the DHCP relay for the Switch.
VLAN State		Enables / disables the DHCP relay on the specific VLAN(s).
DHCP Server IP		Configures the DHCP server's IP address.
Option 82 State		Enables / disables the DHCP Relay Option 82 for the Switch.
Option Information	82	The information for the DHCP Relay Option 82. If the DHCP Option 82 is enabled, the Switch will append the Information into the DHCP discover and request packets.

5.5. Dual Homing

Dual Homing is a network topology in which a device is connected to the network by way of two independent access points (points of attachment). One access point is the primary connection, and the other is a standby connection that is activated in the event of a failure of the primary connection.

How Dual-Homing Works ?

Assume the primary connection and secondary connections are connected to Internet by different way. For example, primary connection is connected to a physical network but secondary connection is connected to a wireless network. When enable dual homing feature, device will default connect to Internet by primary connection and secondary connection will be shutdown. If the port or all ports of primary connection are link-down, then device will replace primary connection by secondary connection to connect to Internet. At this situation, if secondary connection is also link-down, device will do nothing. Secondary connection only works as primary connection disconnecting.

Default Settings

Dual-Homing Configurations:

State : Disable.
 Primary Channel : -
 Secondary Channel : -

Detail Status:

Primary Channel Status : -
 Secondary Channel Status : -

Notices: If the channel is a single port, then the port cannot add into any trunk group.

5.5.1. CLI Configuration

Node	Command	Description
enable	show dual-homing	This command displays the dual-homing information.
configure	dual-homing (disable enable)	This command disables / enables the dual-homing function for the system.
configure	dual-homing primary-channel (port trunk) VALUE	This command sets the dual-homing primary channel for the system. The channel can be a single port or a trunk group.
configure	no dual-homing primary-channel	This command removes the dual-homing primary channel for the system.
configure	dual-homing secondary-channel (port trunk) VALUE	This command sets the dual-homing secondary channel for the system. The channel can be a single port or a trunk group.
configure	no dual-homing secondary-channel	This command removes the dual-homing secondary channel for the system.

Example:

```
L2SWITCH(config)# link-aggregation 1 ports 5-6
L2SWITCH(config)# link-aggregation 1 enable
L2SWITCH(config)# dual-homing primary-channel port 2
L2SWITCH(config)# dual-homing secondary -channel trunk 1
L2SWITCH(config)# dual-homing enable
```

5.5.2. Web Configuration

Dual Homing

General Settings

Dual Homing Settings

State Enable

Primary Channel Port

Secondary Channel Port

Dual Homing Status

State	Enabled
Primary Channel	Port 1 (Forwarding)
Secondary Channel	Port 2 (Blocking)

Parameter	Description
State	Enables / disables the Dual-Homing for the Switch.
Primary channel	Configures the primary channel. The channel can be single port or a trunk group.
Secondary channel	Configures the secondary channel. The channel can be single port or a trunk group.

5.6. EEE (Energy Efficient Ethernet)

The Energy Efficient Ethernet (EEE) is an IEEE 802.3az standard that is designed to reduce power consumption in Ethernet networks during idle periods.

EEE can be enabled on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

Notice: This feature is for Ethernet copper ports only.

Default Settings: All ports' EEE states are disabled.

5.6.1. CLI Configuration


Node	Command	Description
enable	show interface [IFNAME]	This command displays the current port configurations.
interface	power efficient-ethernet auto	The command enables EEE on the specified interface. When EEE is enabled, the device advertises and auto negotiates EEE to its link partner.
interface	no power efficient-ethernet auto	The command disables EEE on the specified interface.

Example :

```
L2SWITCH#configure terminal
L2SWITCH(config-if)#interface gigabitethernet1/0/1
L2SWITCH(config-if)#power efficient-ethernet auto
L2SWITCH(config-if)#no power efficient-ethernet auto
```

5.6.2. Web Configuration

Energy Efficient Ethernet



Parameter	Description
EEE Port State	Click a port to enable IEEE 802.3az Energy Efficient Ethernet on that port.
Select All	Click this to enable IEEE 802.3az Energy Efficient Ethernet across all ports.
Deselect All	Click this to disable IEEE 802.3az Energy Efficient Ethernet across all ports.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last saved setting.

5.7. Link Aggregation

5.7.1. Static Trunk

Link Aggregation (Trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports. The Switch supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your Switch.

Default Settings

- The default group Link Aggregation state is disabled for all groups.
- The default group Link Aggregation load balance is source MAC and destination MAC for all groups.
- Maximum link aggregation group : 8.
- Maximum port in link aggregation group : 6.

5.7.1.1. CLI Configuration

Node	Command	Description
enable	show link-aggregation	The command displays the current trunk configurations.
configure	link-aggregation [GROUP_ID] (disable enable)	The command disables / enables the trunk on the specific trunk group.
configure	link-aggregation [GROUP_ID] interface PORTLISTS	The command adds ports to a specific trunk group.
configure	no link-aggregation [GROUP_ID] interface PORTLISTS	The commands delete ports from a specific trunk group.
configure	link-aggregation [GROUP_ID] load-balance (src-mac dst-mac src-dst-mac src-ip dst-ip src-dst-ip)	The commands configures load-balance algorithm for the specific trunk group. src-mac: source mac. dst-mac: destination mac. src-dst-mac: source and destination mac. src-ip: source IP. dst-ip: destination IP. src-dst-ip: source and destination IP.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#link-aggregation 1 enable
L2SWITCH(config)#link-aggregation 1 load-balance src-mac
L2SWITCH(config)#link-aggregation 1 interface 1-4
```

5.7.1.2. Web Configuration

Link Aggregation

StaticTrunk

LACP

Static Trunk Settings

Group State: Group 1 Disable

Member Ports:

Select All Deselect All

1 3 5 7

2 4 6 8 9 10

Trunk Group Status

Group ID	State	Member Ports
1	Disabled	
2	Disabled	
3	Disabled	
4	Disabled	
5	Disabled	
6	Disabled	

Member Ports: T is Trunk member port but no link, A is Trunk member and link up.

Parameter	Description
Group State	Select the group ID to use for this trunk group, that is, one logical link containing multiple ports. Select Enable to use this static trunk group.
Load Balance	Configures the load balance algorithm for the specific trunk group.
Member Ports	Select the ports to be added to the static trunk group.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last saved setting.
Trunk Group Status	
Group ID	This field displays the group ID to identify a trunk group, that is,

	one logical link containing multiple ports.
State	This field displays if the trunk group is enabled or disabled.
Load Balance	This field displays the load balance policy for the trunk group.
Member Ports	This field displays the assigned ports that comprise the static trunk group.

5.7.2. LACP

The Switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking. The IEEE 802.3ad standard describes the Link Aggregation Control Protocol (LACP) for dynamically creating and managing trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.
- Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

System Priority:

The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.

System ID:

The LACP system ID is the combination of the LACP system priority value and the MAC address of the router.

Administrative Key:

The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by these factors:

- Port physical characteristics, such as data rate, duplex capability, and point-to-point or shared medium.
- Configuration restrictions that you establish.

Port Priority:

The port priority determines which ports should be put in standby mode when there is a

hardware limitation that prevents all compatible ports from aggregating.

Default Settings

The default System Priority is 32768.

The default group LACP state is disabled for all groups.

5.7.2.1. CLI Configuration

Node	Command	Description
enable	show trunk	This command displays the current trunk configurations.
enable	show lacp counters [GROUP_ID]	This command displays the LACP counters for the specific group or all groups.
enable	show lacp internal [GROUP_ID]	This command displays the LACP internal information for the specific group or all groups.
enable	show lacp neighbor [GROUP_ID]	This command displays the LACP neighbor's information for the specific group or all groups.
enable	show lacp port_priority	This command displays the port priority for the LACP.
enable	show lacp sys_id	This command displays the actor's and partner's system ID.
configure	Lacp (disable enable)	This command disables / enables the LACP on the switch.
configure	Lacp GROUP_ID (disable enable)	This command disables / enables the LACP on the specific trunk group.
configure	clear lacp counters [PORT_ID]	This command clears the LACP statistics for the specific port or all ports.
configure	lacp system-priority <1-65535>	This command configures the system priority for the LACP. Note: The default value is 32768.
configure	no lacp system-priority	This command configures the default for the system priority for the LACP.
interface	lacp port_priority <1-65535>	This command configures the priority for the specific port. Note: The default value is 32768.
interface	no lacp port_priority	This command configures the default for the priority for the specific port.

5.7.2.2. Web Configuration

LACP Settings

Link Aggregation

StaticTrunk
LACP Settings
LACP Info.

LACP Settings

State:

System Priority:

Group LACP:

Port Priority: From: ~ :

LACP Group Status

Group ID	LACP State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled

LACP Port Priority Status

Port	Priority	Port	Priority
1	32768	2	32768
3	32768	4	32768
5	32768	6	32768

Parameter	Description
State	Select Enable from the drop down box to enable Link Aggregation Control Protocol (LACP). Select Disable to not use LACP.
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group LACP	Select a trunk group ID and then select whether to Enable or Disable Group Link Aggregation Control Protocol for that trunk group.

Port Priority	Select a port or a range of ports to configure its (their) LACP priority.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last saved setting.
LACP Group Status	
Group ID	The field identifies the LACP group ID.
LACP State	This field displays if the group has LACP enabled.
LACP Port Priority Status	
Port	The field identifies the port ID.
Priority	The field identifies the port's LACP priority.

LACP Info.

Link Aggregation

StaticTrunk
LACP Settings
LACP Info.

LACP Informations

Group ID

Group ID	1						
Neighbors Information							
Port	System Priority	System ID	Port	Age	Port State	Port Priority	Oper Key
5	1	0000.0000.0000	0	0s	0x45	1	0
7	32768	0005.0202.0839	13	87s	0x05	32768	1
Internal Information							
Port	Port Priority	Admin Key	Oper Key	Port State			
5	32768	1	1	0x45			
7	32768	1	1	0x0d			

Parameter	Description
Group ID	Select a LACP group that you want to view.
Neighbors Information	
Port	The LACP member port ID.
System Priority	LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default:

	32768)
System ID	The neighbor Switch's system ID.
Port	The direct connected port Id of the neighbor Switch.
Age	The available time period of the neighbor Switch LACP information.
Port State	The direct connected port's state of the neighbor Switch.
Port Priority	The direct connected port's priority of the neighbor Switch.
Oper Key	The Oper key of the neighbor Switch.
Internal Information	
Port	The LACP member port ID.
Port Priority	The port priority of the LACP member port.
Admin Key	The Admin key of the LACP member port.
Oper Key	The Oper key of the LACP member port.
Port State	The port state of the LACP member port.

5.8. Link Layer Discovery Protocol (LLDP)

The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802® LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities.

The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

Default Settings

The LLDP on the Switch is disabled.

Tx Interval : 30 seconds.

Tx Hold : 4 times.

Time To Live : 120 seconds.

Port	Status	Port	Status
----	-----	----	-----

- | | | | |
|---|--------|---|--------|
| 1 | Enable | 2 | Enable |
| 3 | Enable | 4 | Enable |
| 5 | Enable | 6 | Enable |

5.8.1. CLI Configuration

Node	Command	Description
enable	show lldp	This command displays the LLDP configurations.
enable	show lldp neighbor	This command displays all of the ports' neighbor information.
configure	lldp (disable enable)	This command globally enables / disables the LLDP function on the Switch.
configure	lldp tx-interval	This command configures the interval to transmit the LLDP packets.
configure	lldp tx-hold	This command configures the tx-hold time which determines the TTL of the Switch's message. (TTL=tx-hold * tx-interval)
interface	lldp-agent (disable enable rx-only tx-only)	This command configures the LLDP agent function. disable – Disable the LLDP on the specific port. enable – Transmit and Receive the LLDP packet on the specific port. tx-only – Transmit the LLDP packet on the specific port only. rx-only – Receive the LLDP packet on the specific port.

5.8.2. Web Configuration

LLDP

Settings
Neighbor

LLDP Settings

State Disable ▾

Tx Interval 30 seconds

Tx Hold 4 times

Time To Live 120 seconds

Port

From: 1 ▾ To: 1 ▾

State

Enable ▾

LLDP Status

Port	State	Port	State
1	Enable	2	Enable
3	Enable	4	Enable
5	Enable	6	Enable

Parameter	Description
State	Globally enables / disables the LLDP on the Switch.
Tx Interval	Configures the interval to transmit the LLDP packets.
Tx Hold	Configures the tx-hold time which determines the TTL of the Switch's message. (TTL=tx-hold * tx-interval)
Time To Live	The hold time for the Switch's information.
Port	The port range which you want to configure.
State	Enables / disables the LLDP on these ports.
LLDP Status	
Port	The Port ID.
State	The LLDP state for the specific port.

LLDP

Settings
Neighbor

LLDP Neighbor Information

Port All Apply

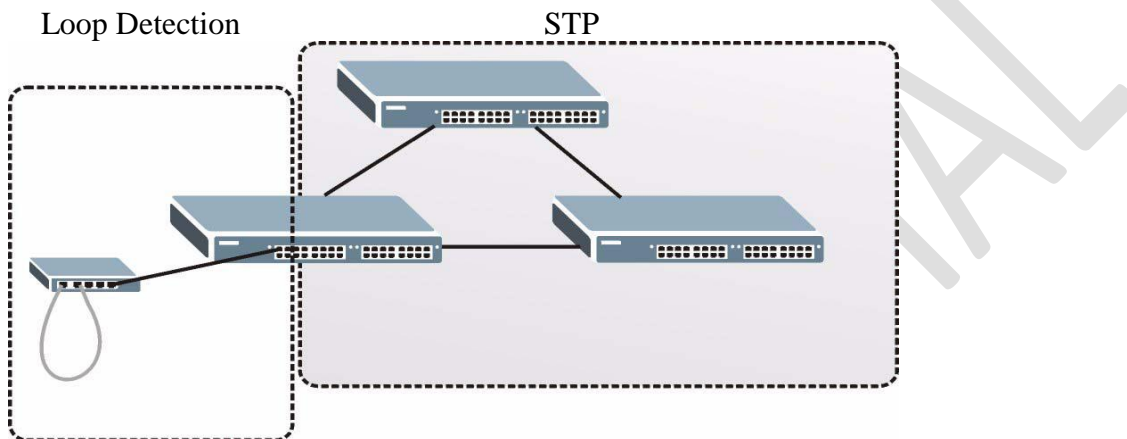
Local Port 2	
Remote Port ID	4
Chassis ID	00-0b-04-52-14-20
System Name	L2SWITCH
System Description	Volktek Corp./MEN5214/5214-000-1.0.7.b1/Oct 16 17:07:21 CST 2013
System Capabilities	Bridge/Switch (enabled)
Management Address	192.168.202.144
Time To Live	120 sec(s)

Parameter	Description
Port	Select the port(s) which you want to display the port's neighbor information.
Local Port	The local port ID.
Remote Port ID	The connected port ID.
Chassis ID	The neighbor's chassis ID.
System Name	The neighbor's system name.
System Description	The neighbor's system description.
System Capabilities	The neighbor's capability.
Management Address	The neighbor's management address.
Time To Live	The hold time for the neighbor's information.

5.9. Loop Detection

Loop detection is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

The difference between the Loop Detection and STP:



The loop detection function sends probe packets periodically to detect if the port connect to a network in loop state. The Switch shuts down a port if the Switch detects that **probe packets loop back to the same port of the Switch**.

Loop Recovery:

When the loop detection is enabled, the Switch will send one probe packets every two seconds and then listen this packet. If it receives the packet at the same port, the Switch will disable this port. After the time period, **recovery time**, the Switch will enable this port and do loop detection again.

The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop detection feature.

For the access Switch, it may not enable the STP function. To guarantee the network topology is loop free, the Loop detection function also need detect below scenario.

Default Settings

The default global Loop-Detection state is disabled.

The default Loop Detection Destination MAC is 00:0b:04:aa:aa:ab

The default Port Loop-Detection state is disabled for all ports.

The default Port Loop-Detection status is unblocked for all ports.

The loop detection on the Switch is disabled.

Loop Detection Destination MAC=00:0b:04:aa:aa:ab

Port	State	Status	Recovery		Port	State	Status	Recovery	
			State	Time				State	Time
1	Disabled	Normal	Enabled	1	2	Disabled	Normal	Enabled	1
3	Disabled	Normal	Enabled	1	4	Disabled	Normal	Enabled	1
5	Disabled	Normal	Enabled	1	6	Disabled	Normal	Enabled	1

5.9.1. CLI Configuration

Node	Command	Description
enable	show loop-detection	This command displays the current loop detection configurations.
configure	loop-detection (disable enable)	This command disables / enables the loop detection on the switch.
configure	loop-detection address MACADDR	This command configures the destination MAC for the loop detection special packets.
configure	no loop-detection address	This command configures the destination MAC to default (00:0b:04:AA:AA:AB).
interface	loop-detection (disable enable)	This command disables / enables the loop detection on the specific port.
interface	no shutdown	This command enables the specific port. It can unblock port blocked by loop detection.
interface	loop-detection recovery (disable enable)	This command enables / disables the recovery function on the port.
interface	loop-detection recovery time VALUE	This command configures the recovery period time.

Example:

```
L2SWITCH(config)#loop-detection enable
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#loop-detection enable
```

5.9.2. Web Configuration

Loop Detection

Loop Detection Settings

State: Disable ▾

MAC Address: 00:0b:04:aa:aa:ab

Port	State	Action	Loop Recovery	Recovery Time (min)
From: 1 ▾ To: 1 ▾	Disable ▾	None ▾	Enable ▾	1 (Range: 1-60)

Apply
Refresh

Loop Detection Status

Port	State	Status	Loop Recovery	Recovery Time (min)
1	Disabled	Normal	Enabled	1
2	Disabled	Normal	Enabled	1
3	Disabled	Normal	Enabled	1
4	Disabled	Normal	Enabled	1
5	Disabled	Normal	Enabled	1
6	Disabled	Normal	Enabled	1

Parameter	Description
State	Select this option to enable loop guard on the Switch.
MAC Address	Enter the destination MAC address the probe packets will be sent to. If the port receives these same packets the port will be shut down.
Port	Select a port on which to configure loop guard protection.
State	Select Enable to use the loop guard feature on the Switch.
Loop Recovery	Select Enable to reactivate the port automatically after the designated recovery time has passed.
Recovery Time	Specify the recovery time in minutes that the Switch will wait before reactivating the port. This can be between 1 to 60 minutes.
Apply	Click Apply to save your changes to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
Loop Guard Status	
Port	This field displays a port number.

State	This field displays if the loop guard feature is enabled.
Status	This field displays if the port is blocked.
Loop Recovery	This field displays if the loop recovery feature is enabled.
Recovery Time (min)	This field displays the recovery time for the loop recovery feature.

5.10. STP

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other (R)STP compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch supports Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge and then the root bridge notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database.

In STP, the port states are Blocking, Listening, Learning, Forwarding.

In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this document, “STP” refers to both STP and RSTP.

STP Terminology

- The root bridge is the base of the spanning tree.
- Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

- On each bridge, the bridge communicates with the root through the root port. The root port is the port on this Switch with the lowest path cost to the root (the root path cost). If there is no root port, then this Switch has been accepted as the root bridge of the spanning tree network.
- For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

Forward Time (Forward Delay):

This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.

Max Age:

This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port whose age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.

Hello Time:

This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

PathCost:

Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.

How STP Works ?

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed. Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

802.1D STP

The Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. It is based on an algorithm invented by Radia Perlman while working for Digital Equipment Corporation. In the OSI model for computer networking, STP falls under the OSI layer-2. 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 manual enabling/disabling of these backup links. Bridge loops must be avoided because they result in flooding the network.

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

STP switch port states:

- Blocking - A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.
- Listening - The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state.
- Learning - While the port does not yet forward frames (packets) it does learn source addresses from frames received and adds them to the filtering database (switching database)
- Forwarding - A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.
- Disabled - Not strictly part of STP, a network administrator can manually disable a port

802.1w RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP), which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP. While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a second.

RSTP bridge port roles:

- Root - A forwarding port that is the best port from Nonroot-bridge to Rootbridge
- Designated - A forwarding port for every LAN segment
- Alternate - An alternate path to the root bridge. This path is different than using the root port.
- Backup - A backup/redundant path to a segment where another bridge port already connects.
- Disabled - Not strictly part of STP, a network administrator can manually

disable a port

Edge Port:

They are attached to a LAN that has no other bridges attached. These edge ports transition directly to the forwarding state. RSTP still continues to monitor the port for BPDUs in case a bridge is connected. RSTP can also be configured to automatically detect edge ports. As soon as the bridge detects a BPDU coming to an edge port, the port becomes a non-edge port.

Forward Delay:

The range is from 4 to 30 seconds. This is the maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).

Transmission Limit:

This is used to configure the minimum interval between the transmission of consecutive RSTP BPDUs. This function can only be enabled in RSTP mode. The range is from 1 to 10 seconds.

Hello Time:

Set the time at which the root switch transmits a configuration message. The range is from 1 to 10 seconds.

Bridge priority:

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will become the root device.

Port Priority:

Set the port priority in the switch. Low numeric value indicates a high priority. A port with lower priority is more likely to be blocked by STP if a network loop is detected. The valid value is from 0 to 240.

Path Cost:

The valid value is from 1 to 200000000. Higher cost paths are more likely to be blocked by STP if a network loop is detected.

BPDU Guard

This is a per port setting. If the port is enabled in BPDU guard and receive any BPDU, the port will be set to disable to avoid the error environments. User must enable the port by manual.

BPDU Filter

It is a feature to filter sending or receiving BPDUs on a switch port. If the port receives any BPDUs, the BPDUs will be dropped.

Notice:

If both of the BPDU filter and BPDU guard are enabled, the BPDU filter has the

high priority.

Root Guard

The Root Guard feature forces an interface to become a designated port to prevent surrounding switches from becoming a root switch. In other words, Root Guard provides a way to enforce the root bridge placement in the network. The Root Guard feature prevents a Designated Port from becoming a Root Port. If a port on which the Root Guard feature receives a superior BPDU, it moves the port into a root-inconsistent state (effectively equal to a listening state), thus maintaining the current Root Bridge status. The port can be moved to forwarding state if no superior BPDU received by this port for three hello time.

Default Settings

- STP/RSTP : disabled.
- STP/RSTP mode : RSTP.
- Forward Time : 15 seconds.
- Hello Time : 2 seconds.
- Maximum Age : 20 seconds.
- System Priority : 32768.
- Transmission Limit : 3 seconds.
- Per port STP state : enabled.
- Per port Priority : 128.
- Per port Edge port : disabled.
- Per port BPDU filter : disabled.
- Per port BPDU guard : disabled.
- Per port BPDU Root guard: disabled.
- Per port Path Cost : depend on port link speed.

Example: Bandwidth -> STP Port Cost Value

10 Mbps -> 100

100 Mbps-> 19

1 Gbps -> 4

10 Gbps -> 2

5.10.1. CLI Configuration

Node	Command	Description
enable	show spanning-tree active	This command displays the spanning tree information for only active port(s)
enable	show spanning-tree blockedports	This command displays the spanning tree information for only blocked port(s)
enable	show spanning-tree port detail PORT_ID	This command displays the spanning tree information for the interface port.
enable	show spanning-tree statistics PORT_ID	This command displays the spanning tree information for the interface port.
enable	show spanning-tree summary	This command displays the summary of port states and configurations
enable	clear spanning-tree	This command clears spanning-tree statistics for all

	counters	ports.
enable	clear spanning-tree counters PORT_ID	This command clears spanning-tree statistics for a specific port.
configure	spanning-tree (disable enable)	This command disables / enables the spanning tree function for the system.
configure	spanning-tree algorithm-timer forward-time TIME max-age TIME hello-time TIME	This command configures the bridge times (forward-delay,max-age,hello-time).
configure	no spanning-tree algorithm-timer	This command configures the default values for forward-time & max-age & hello-time.
configure	spanning-tree forward-time <4-30>	This command configures the bridge forward delay time (sec).
configure	no spanning-tree forward-time	This command configures the default values for forward-time.
configure	spanning-tree hello-time <1-10>	This command configures the bridge hello time (sec).
configure	no spanning-tree hello-time	This command configures the default values for hello-time.
configure	spanning-tree max-age <6-40>	This command configures the bridge message max-age time(sec).
configure	no spanning-tree max-age	This command configures the default values for max-age time.
configure	spanning-tree mode (rstp stp)	This command configures the spanning mode.
configure	spanning-tree pathcost method (short long)	This command configures the pathcost method.
configure	spanning-tree priority <0-61440>	This command configures the priority for the system.
configure	no spanning-tree priority	This command configures the default values for the system priority.
interface	spanning-tree (disable enable)	This command configures enables/disables the STP functions for the specific port.
interface	spanning-tree bpdudfilter (disable enable)	This command configures enables/disables the bpdudfilter function for the specific port.
interface	spanning-tree bpduguard (disable enable)	This command configures enables/disables the bpduguard function for the specific port.
interface	spanning-tree rootguard (disable enable)	This command enables/disables the BPDU Root guard port setting for the specific port.
interface	spanning-tree edge-port	This command enables/disables the edge port setting for the specific port.

	(disable enable)	
interface	spanning-tree cost VALUE	This command configures the cost for the specific port. Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-200000000.
interface	no spanning-tree cost	This command configures the path cost to default for the specific port.
interface	spanning-tree port-priority <0-240>	This command configures the port priority for the specific port. Default: 128.
interface	no spanning-tree port-priority	This command configures the port priority to default for the specific port.

5.10.2. Web Configuration

General Settings

Spanning Tree Protocol

General Settings
Port Parameters
STP Status

Spanning Tree Protocol Settings

State Disable ▾

Mode RSTP ▾

Bridge Parameters

Forward Time	<input type="text" value="15"/>	Max Age	<input type="text" value="20"/>	Hello Time	<input type="text" value="2"/>
Priority	<input type="text" value="32768"/>				
Path Cost	Short ▾				

Parameter	Description
State	Select Enabled to use Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).
Mode	Select to use either Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).
Forward Time	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.

Max Age	<p>This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals.</p> <p>Any port those ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.</p>
Hello Time	<p>This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.</p>
Priority	<p>Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch.</p> <p>Enter a value from 0~61440.</p> <p>The lower the numeric value you assign, the higher the priority for this bridge.</p> <p>Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.</p>
Pathcost	<p>Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.</p>

Port Parameters

Spanning Tree Protocol

General Settings
Port Parameters
STP Status

Port Parameters Settings

Port	Active	Path Cost	Priority	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
From: 1 <input type="button" value="v"/> To: 1 <input type="button" value="v"/>	Enable <input type="button" value="v"/>	250	128	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>

Port Status

Port	Active	Role	Status	Path Cost	Priority	Edge Port	BPDU Filter	BPDU Guard	ROOT Guard
1	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
2	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
3	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
4	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
5	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled
6	Enabled	None	Discarding	250	128	Disabled	Disabled	Disabled	Disabled

Parameter	Description
Port	Selects a port that you want to configure.
Active	Enables/Disables the spanning tree function for the specific port.
Path Cost	Configures the path cost for the specific port.
Priority	Configures the priority for the specific port.
Edge Port	Configures the port type for the specific port. Edge or Non-Edge.
BPDU Filter	Enables/Disables the BPDU filter function for the specific port.
BPDU Guard	Enables/Disables the BPDU guard function for the specific port.
ROOT Guard	Enables/Disables the BPDU root guard function for the specific port.
Port Status	
Active	The state of the STP function.
Role	The port role. Should be one of the Alternated / Designated / Root / Backup / None.
Status	The port's status. Should be one of the Discarding / Blocking / Listening / Learning / Forwarding / Disabled.
Path Cost	The port's path cost.
Priority	The port's priority.
Edge Port	The state of the edge function.
BPDU Filter	The state of the BPDU filter function.
BPDU Guard	The state of the BPDU guard function.
ROOT Guard	The state of the BPDU Root guard function.

STP Status

Spanning Tree Protocol						
General Settings		Port Parameters		STP Status		
Current Root Status						
MAC Address	Priority	Max Age	Hello Time	Forward Delay		
00:03:09:02:08:18	32768	20	2	15		
Current Bridge Status						
MAC Address	Priority	Max Age	Hello Time	Forward Delay	Path Cost	Root Port
00:03:09:02:08:18	32768	20	2	15	0	0
<input type="button" value="Refresh"/>						

Parameter	Description
Current Root Status	
MAC address	This is the MAC address of the root bridge.
Priority	Root refers to the base of the spanning tree (the root bridge). This field displays the root bridge's priority. This Switch may also be the root bridge.
MAX Age	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Hello Time	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Forward Delay	This is the time (in seconds) the root switch will wait before changing states.
Current Bridge Status	
MAC address	This is the MAC address of the current bridge.
Priority	Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.
MAX Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch.
Forward Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a

	blocking state; otherwise, temporary data loops might result.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.
Root Cost	This is the number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.

5.11. Xpress Ring

The Xpress Ring is a fast-acting, self-healing ring recovery technology that enables networks to recover from link failure within 50ms.

Fast Link Recovery and Ring Redundancy are important features for increasing the reliability of non-stop systems.

If the network is planned correctly with an arbiter Switch and ring ports, the network will recover from any segment failure within a very short time.

There are two roles (Forwarder and Arbiter) of the Switch in the Xpress Ring. There is one and only one Switch is the Arbiter Switch and the others are the forwarder Switch.

One of the ring ports of the Arbiter Switch will be set to blocking state. When one of the ring connections is broken, the blocked port will be set to forwarding state.

Default Settings

Xpress Ring Configurations:

```

State      : Disabled.
Ring role  : Forwarder.
Ring port1 : 1.
Ring port2 : 2.
    
```

Current Status:

```

Ring port1 : No connection.
Ring port2 : No connection.
    
```

Notices

If there are old devices (for example: INS-803A) to join the Xpress Ring, they can join as the forwarder only.

5.11.1. CLI Configuration

Node	Command	Description
enable	show xpress-ring	This command displays the current Xpress ring status.
config	xpress-ring (disable enable)	This command enables/disables the Xpress ring function on the Switch.
config	xpress-ring role (forwarder arbiter)	This command configures the role (forwarder/arbiter) for the Switch.
config	xpress-ring ring-port1	This command configures one port of the ring.
config	xpress-ring ring-port2	This command configures the other port of the ring.

5.11.2. Web Configuration

Xpress Ring

Xpress Ring Settings

State:

Role:

Ring Port1:

Ring Port2:

Xpress Ring Status

State	Disabled
Role	Forwarder
Ring Port1	1 (Forwarding)
Ring Port2	2 (No connection)

Parameter	Description
Current Root Status	
State	Enables/Disable the Xpress ring function.
Role	Configures the role of the Switch. (Forwarder / Arbiter)
Ring Port1	Configures one port of the ring.
Ring Port2	Configure the other port of the ring.
Xpress Ring Status	
State	The current Xpress ring state.
Role	The current role of the Switch.
Ring Port1	The current one port of the ring.
Ring Port2	The current other port of the ring.

6. Security

6.1. IP Source Guard

IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. Any IP traffic coming into the interface with a source IP address other than that assigned (via DHCP or static configuration) will be filtered out on the u-trusted Layer 2 ports.

The IP Source Guard feature is enabled in combination with the DHCP snooping feature on untrusted Layer 2 interfaces. It builds and maintains an IP source binding table that is learned by DHCP snooping or manually configured (static IP source bindings). An entry in the IP source binding table contains the IP address and the associated MAC and VLAN numbers. The IP Source Guard is supported on Layer 2 ports only, including access and trunk ports.

The IP Source Guard features include below functions:

1. DHCP Snooping.
2. DHCP Binding table.
3. ARP Inspection.
4. Blacklist Filter. (arp-inspection mac-filter table)

6.1.1. DHCP Snooping

DHCP snooping is a DHCP security feature that provides network security by filtering un-trusted DHCP messages and by building and maintaining a DHCP snooping binding database, which is also referred to as a DHCP snooping binding table.

DHCP snooping acts like a firewall between un-trusted hosts and DHCP servers. You can use DHCP snooping to differentiate between un-trusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

The DHCP snooping binding database contains the MAC address, the IP address, the lease time, the binding type, the VLAN number, and the interface information that corresponds to the local un-trusted interfaces of a switch.

When a switch receives a packet on an un-trusted interface and the interface belongs to a VLAN in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The switch drops a DHCP packet when one of these situations occurs:

A packet from a DHCP server, such as a DHCP OFFER, DHCP ACK, DHCP NAK, or DHCP REQUEST packet, is received from the un-trusted port.

A packet is received on an un-trusted interface, and the source MAC address and the

DHCP client hardware address do not match any of the current bindings.

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.
- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

DHCP Snooping Database

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again.

Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the Switch.

1. Enable DHCP snooping on the Switch.
2. Enable DHCP snooping on each VLAN.
3. Configure trusted and untrusted ports.
4. Configure static bindings.

Note:

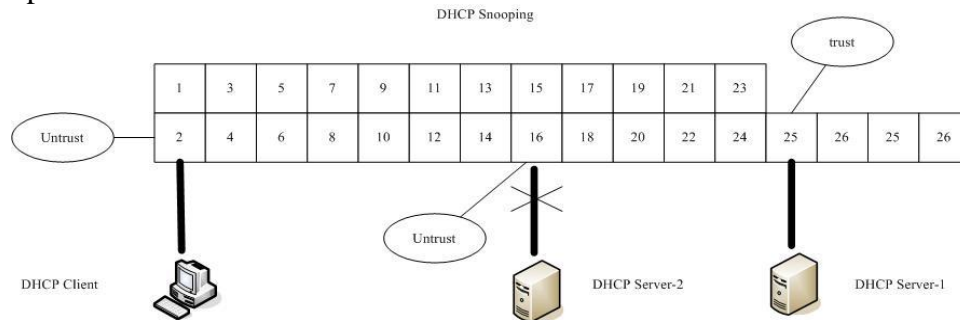
The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

If the port link down, the entries learned by this port in the DHCP snooping binding table will be deleted.

You must enable the global DHCP snooping and DHCP Snooping for vlan first.

The main purposes of the DHCP Snooping are:

1. Create and maintain a binding table for ARP Inspection functions.
2. Filter the DHCP server's packets that the DHCP server connects to a un-trust port.



The DHCP server connected to an un-trusted port will be filtered.

Default Settings

The DHCP snooping on the Switch is disabled.
 The DHCP snooping is enabled in VLAN(s): None.
 The DHCP option 82 on the Switch is disabled.
 The information of the DHCP option 82 is NULL.

Port	Trusted	Maximum Host Count	Port	Trusted	Maximum Host Count
1	no	32	2	no	32
3	no	32	4	no	32
5	no	32	6	no	32

Notices

- The Option 82 configurations are shared with DHCP Relay function.
 - There are a global state and per VLAN states.
- When the global state is disabled, the DHCP Snooping on the Switch is disabled even per VLAN states are enabled.
- When the global state is enabled, user must enable per VLAN states to enable the DHCP Snooping on the specific VLAN.

VLAN 1 : port 1-10.
 DHCP Client-1 : connect to port 3.
 DHCP Server : connect to port 1.

Procedures:

1. Default environments:
 - A. DHCP Client-1: ipconfig /release
 - B. DHCP Client-1: ipconfig /renew
 → DHCP Client-1 can get an IP address.

2. Enable the global DHCP Snooping.
 - A. L2SWITCH(config)#dhcp-snooping
 - B. DHCP Client-1: ipconfig /release
 - C. DHCP Client-1: ipconfig /renew
→ DHCP Client-1 can get an IP address.

3. Enable the global DHCP Snooping and VLAN 1 DHCP Snooping.
 - A. L2SWITCH(config)#dhcp-snooping
 - B. L2SWITCH(config)#dhcp-snooping vlan 1
 - C. DHCP Client-1: ipconfig /release
 - D. DHCP Client-1: ipconfig /renew
→ DHCP Client-1 cannot get an IP address.
; Because the DHCP server connects to a un-trust port.

4. Enable the global DHCP Snooping and VLAN 1 DHCP Snooping.
 - A. L2SWITCH(config)#dhcp-snooping
 - B. L2SWITCH(config)#dhcp-snooping vlan 1
 - C. L2SWITCH(config)#interface gi1/0/1
 - D. L2SWITCH(config-if)#dhcp-snooping trust
 - E. DHCP Client-1: ipconfig /release
 - F. DHCP Client-1: ipconfig /renew
→ DHCP Client-1 can get an IP address.

5. If you configure a static host entry in the DHCP snooping binding table, and then you want to change the host to DHCP client. The host will not get a new IP from DHCP server. You must delete the static host entry first.

6.1.1.1. CLI Configuration

Node	Command	Description
enable	show dhcp-snooping	This command displays the current DHCP snooping configurations.
configure	dhcp-snooping (disable enable)	This command disables/enables the DHCP snooping on the switch.
configure	dhcp-snooping vlan VLAN_ID	This command enables the DHCP snooping function on a VLAN or range of VLANs.
configure	no dhcp-snooping vlan VLANID	This command disables the DHCP snooping function on a VLAN or range of VLANs.
configure	dhcp option82 (disable enable)	This command disables / enables the DHCP relay option 82.
configure	dhcp option82 information STRING	This command configures the information for the DHCP relay option 82.
configure	no dhcp option82 information	This command removes the information for the DHCP relay option 82.
interface	dhcp-snooping host	This command configures the maximum host count for the specific port.

interface	no dhcp-snooping host	This command configures the maximum host count to default for the specific port.
interface	dhcp-snooping trust	This command configures the trust port for the specific port.
interface	no dhcp-snooping trust	This command configures the un-trust port for the specific port.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#dhcp-snooping enable
L2SWITCH(config)#dhcp-snooping vlan 1
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#dhcp-snooping trust
L2SWITCH(config)#dhcp option82 enable
L2SWITCH(config)#dhcp option82 information Test
```

6.1.1.2. Web Configuration

DHCP Snooping

The screenshot displays the DHCP Snooping configuration page. It has two tabs: 'DHCP Snooping' and 'Port Settings'. Under 'DHCP Snooping Settings', there are four rows of configuration options: 'State' set to 'Disable', 'VLAN State' set to 'Add' with an empty input field, 'Option 82 State' set to 'Disable', and 'Option 82 Information' with an empty input field. 'Apply' and 'Refresh' buttons are located below these settings. The 'DHCP Snooping Status' section contains a table with the following data:

DHCP Snooping State	Disabled
Enabled on VLAN	None
Option82 State	Disabled
Option82 Information	None

Parameter	Description
State	Select Enable to use DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLANs and specify trusted ports. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports. Select Disable to not use DHCP snooping..

VLAN State	Select Add and enter the VLAN IDs you want the Switch to enable DHCP snooping on. You can designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-). Select Delete and enter the VLAN IDs you no longer want the Switch to use DHCP snooping on.
Option 82 State	Enables or disables the DHCP Option 82 for the Switch.
Option 82 Information	The information for the DHCP Option 82. If the DHCP Option 82 is enabled, the Switch will append the Information into the DHCP discover and request packets. The maximum length of the information is 32 characters.
DHCP Snooping Status	
DHCP Snooping State	This field displays the current status of the DHCP snooping feature, Enabled or Disabled .
Enabled VLAN	This field displays the VLAN IDs that have DHCP snooping enabled on them. This will display None if no VLANs have been set.

Port Settings

DHCP Snooping

DHCP Snooping
Port Settings
Server Screening

Port Settings

Port: From: To:

Trust:

Maximum Host Count: (Range: 1-32)

Port Status

Port	Trusted	Maximum Host Count	Port	Trusted	Maximum Host Count
1	NO	32	2	NO	32
3	NO	32	4	NO	32
5	NO	32	6	NO	32

Parameter	Description
Port	Select a port number to modify its maximum host count.
Trust	Configures the specific port if it is a trust port.
Maximum Host Count	Enter the maximum number of hosts (1-32) that are permitted to simultaneously connect to a port.

6.1.2. ARP Inspection

Dynamic ARP inspection is a security feature which validates ARP packet in a network. Dynamic ARP inspections validates the packet by performing IP to MAC address binding inspection stored in a trusted database (the DHCP snooping database) before forwarding the packet. Dynamic ARP intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercepts all ARP requests and responses on un-trusted ports.
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before it updates the local ARP cache or before it forwards the packet to the appropriate destination.

Trusted and un-trusted port

- This setting is independent of the trusted and un-trusted setting of the DHCP Snooping.
- The Switch does not discard ARP packets on trusted ports for any reasons.
- The Switch discards ARP packets on un-trusted ports if the sender's information in the ARP packets does not match any of the current bindings.
- Normally, the trusted ports are the uplink port and the un-trusted ports are connected to subscribers.

Configurations:

Users can enable / disable the ARP Inspection on the Switch. Users also can enable / disable the ARP Inspection on a specific VLAN. If the ARP Inspection on the Switch is disabled, the ARP Inspection is disabled on all VLANs even some of the VLAN ARP Inspection are enabled.

Default Settings

The ARP Inspection on the Switch is disabled.

The age time for the MAC filter is 5 minutes.

ARP Inspection is enabled in VLAN(s): None.

Port	Trusted	Port	Trusted
1	no	2	no
3	no	4	no
5	no	6	no

Notices: There are a global state and per VLAN states.

- ✓ When the global state is disabled, the ARP Inspection on the Switch is disabled even per VLAN states are enabled.
- ✓ When the global state is enabled, user must enable per VLAN states to enable

the ARP Inspection on the specific VLAN.

6.1.2.1. CLI Configuration

Node	Command	Description
enable	show arp-inspection	This command displays the current ARP Inspection configurations.
configure	arp-inspection (disable enable)	This command disables/enables the ARP Inspection function on the switch.
configure	arp-inspection vlan VLAN_ID	This command enables the ARP Inspection function on a VLAN or range of VLANs.
configure	no arp-inspection vlan VLAN_ID	This command disables the ARP Inspection function on a VLAN or range of VLANs.
interface	arp-inspection trust	This command configures the trust port for the specific port.
interface	no arp-inspection trust	This command configures the un-trust port for the specific port.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#arp-inspection enable
L2SWITCH(config)#arp-inspection vlan 1
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#arp-inspection trust
```

6.1.2.2. Web Configuration

ARP Inspection

ARP Inspection
Filter Table

ARP Inspection Settings

State: Disable ▾

VLAN State: Add ▾

Trusted Ports

Select All Deselect All

1 3 5 7 9

2 4 6 8 10

Apply
Refresh

ARP Inspection Status

ARP Inspection State	Disabled
Enabled on VLAN	None
Trusted Ports	None

Parameter	Description
State	Use this to Enable or Disable ARP inspection on the Switch.
VLAN State	Enter the VLAN IDs you want the Switch to enable ARP Inspection for. You can designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-).
Trusted Ports	Select the ports which are trusted and deselect the ports which are untrusted. The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports in the following situations: <ul style="list-style-type: none"> • The sender's information in the ARP packet does not match any of the current bindings. • The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Select All	Click this to set all ports to trusted.
Deselect All	Click this to set all ports to untrusted.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
ARP Inspection Status	
ARP Inspection State	This field displays the current status of the ARP Inspection feature, Enabled or Disabled .
Enabled on VLAN	This field displays the VLAN IDs that have ARP Inspection enabled on them. This will display None if no VLANs have been set.
Trusted Ports	This field displays the ports which are trusted. This will display None if no ports are trusted.

6.1.3. Filter Table

Dynamic ARP inspections validates the packet by performing IP to MAC address binding inspection stored in a trusted database (the DHCP snooping database) before forwarding the packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. The switch also periodically deletes entries if the age-time for the entry is expired.

- If the ARP Inspection is enabled and the system detects invalid hosts, the system will create a filtered entry in the MAC address table.
- When Port link down and ARP Inspection was disabled, Switch will remove the

- MAC-filter entries learned by this port.
- When Port link down and ARP Inspection was enabled, Switch will remove the MAC-filter entries learned by this port.
- The maximum entry of the MAC address filter table is 256.
- When MAC address filter table of ARP Inspection is full, the Switch receives unauthorized ARP packet, and it automatically creates a SYSLOG and drop this ARP packet. The SYSLOG event happens on the first time.

Default Settings

- The mac-filter age time : 5 minutes. (0 – No age)
- The maximum mac-filter entries : 256.

6.1.3.1. CLI Configuration

Node	Command	Description
enable	show arp-inspection mac-filter	This command displays the current ARP Inspection filtered MAC.
configure	arp-inspection mac-filter age VALUE	This command configures the age time for the ARP inspection MAC filter entry.
configure	no arp-inspection mac-filter mac MACADDR	This command removes an entry from the ARP inspection MAC filter table.

6.1.3.2. Web Configuration

ARP Inspection

ARP Inspection
Filter Table

Filter Age Time Settings

Filter Age Time minutes (Range: 1-10080)

Filter Table

No.	MAC Address	VLAN	Port	Expiry(min)	Action
Total : 0 record(s)					

Parameter	Description
Filter Age Time	This setting has no effect on existing MAC address filters. Enter how long (1-10080 minutes) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards.
Apply	Click Apply to add/modify the settings.

Refresh	Click Refresh to begin configuring this screen afresh.
Filter Table	
No.	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VLAN	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (min)	This field displays how long (in minutes) the MAC address filter remains in the Switch.
Action	Click Delete to remove the record manually.
Total	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.

6.1.4. Binding Table

The DHCP Snooping binding table records the host information learned by DHCP snooping function (dynamic) or set by user (static). The ARP inspection will use this table to forward or drop the ARP packets. If the ARP packets sent by invalid host, they will be dropped. If the Lease time is expired, the entry will be removed from the table.

Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one.

6.1.4.1. CLI Configuration

Node	Command	Description
enable	show dhcp-snooping binding	This command displays the current DHCP snooping binding table.
configure	dhcp-snooping binding mac MAC_ADDR ip IP_ADDR vlan VLAN_ID port PORT_NO	This command configures a static host into the DHCP snooping binding table.
configure	no dhcp-snooping binding mac MACADDR	This command removes a static host from the DHCP snooping binding table.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#dhcp-snooping binding mac 00:11:22:33:44:55 ip 1.1.1.1 vlan 1
port 2
L2SWITCH(config)#no dhcp-snooping binding mac 00:11:22:33:44:55
L2SWITCH#show dhcp-snooping binding
```

6.1.4.2. Web Configuration

Static Entry Settings

DHCP Snooping Binding Table

Static Entry Settings
Binding Table

Static Entry Settings

MAC Address

IP Address

VLAN ID

Port

Static Binding Table

No.	MAC Address	IP Address	Lease(hour)	VLAN	Port	Type	Action

Parameter	Description
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN ID	Enter the source VLAN ID in the binding.
Port	Specify the port in the binding.
Static Binding Table	
No.	This field displays a sequential number for each binding. Click it to update an existing entry.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease (Hour)	This field displays how long the binding is valid.
VLAN	This field displays the source VLAN ID in the binding.

Port	This field displays the port number in the binding.
Type	This field displays how the Switch learned the binding. Static: This binding was learned from information provided manually by an administrator. Dynamic: This binding was learned by snooping DHCP packets.
Action	Click Delete to remove the specified entry.

Binding Table

Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The Switch learns the dynamic bindings by snooping DHCP packets and from information provided manually in the **Static Entry Settings** screen.

DHCP Snooping Binding Table						
Static Entry Settings		Binding Table				
DHCP Snooping Binding Table						
No.	MAC Address	IP Address	Lease(hour)	VLAN	Port	Type
Refresh						

Parameter	Description
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how long the binding is valid.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Type	This field displays how the Switch learned the binding. Static: This binding was learned from information provided manually by an administrator. Dynamic: This binding was learned by snooping DHCP packets.

6.1.5. DHCP Server Screening

The Switch supports DHCP Server Screening, a feature that denies access to rogue DHCP servers. That is, when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients, the valid DHCP server's packets will be passed to the client.

If you want to enable this feature, you must enable the DHCP Snooping function first. The Switch allows users to configure up to three valid DHCP servers.

If no DHCP servers are configured, it means all DHCP server are valid.

6.1.5.1. CLI Configuration

Node	Command	Description
enable	show dhcp-snooping server	This command displays the valid DHCP server IP.
configure	dhcp-snooping server IPADDR	This command configures a valid DHCP server's IP.
configure	no dhcp-snooping server IPADDR	This command removes a valid DHCP server's IP.

6.1.5.2. Web Configuration

DHCP Snooping

DHCP Snooping
Port Settings
Server Screening

Server Screening Setting

IP Address

Server Screening List

No.	IP Address	Action
<u>1</u>	192.168.201.1	<input type="button" value="Delete"/>
<u>2</u>	192.168.201.5	<input type="button" value="Delete"/>
<u>3</u>	192.168.201.3	<input type="button" value="Delete"/>

Parameter	Description
IP Address	This field configures the valid DHCP server's IP address.
Apply	Click Apply to configure the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Server Screening List	

No.	This field displays the index number of the DHCP server entry. Click the number to modify the entry.
IP Address	This field displays the IP address of the DHCP server.
Action	Click Delete to remove a configured DHCP server.

6.2. ACL

L2 Access control list (ACL) is a list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

L2 ACL function allows user to configure a few rules to reject packets from the specific ingress ports or all ports. These rules will check the packets' source MAC address and destination MAC address. If packets match these rules, the system will do the actions "deny". "deny" means rejecting these packets.

The Action Resolution engine collects the information (action and metering results) from the hit entries: if more than one rule matches, the actions and meter/counters are taken from the policy associated with the matched rule with highest priority.

L2 ACL Support:

1. Filter a specific source MAC address.
Command: *source mac host MACADDR*
2. Filter a specific destination MAC address.
Command: *destination mac host MACADDR*
3. Filter a range of source MAC address.
Command: *source mac MACADDR MACADDR*
The second MACADDR is a mask, for example: ffff.ffff.0000
4. Filter a range of destination MAC address.
Command: *destination mac MACADDR MACADDR*
The second MACADDR is a mask, for example: ffff.ffff.0000

L3 ACL Support:

1. Filter a specific source IP address.
Command: *source ip host IPADDR*
2. Filter a specific destination IP address.
Command: *destination ip host IPADDR*
3. Filter a range of source IP address.
Command: *source ip IPADDR IPADDR*
The second IPADDR is a mask, for example: 255.255.0.0
4. Filter a range of destination IP address.
Command: *destination ip IPADDR IPADDR*

L4 ACL Support:

1. Filter a UDP/TCP source port.
2. Filter a UDP/TCP destination port.

Default Settings

- Maximum profile : 64.
- Maximum profile name length : 16.

Notices

The ACL name should be the combination of the digit or the alphabet.

6.2.1. CLI Configuration

Node	Command	Description
enable	show access-list	This command displays all of the access control profiles.
configure	access-list STRING	This command creates a new access control profile. Where the STRING is the profile name.
configure	no access-list STRING	This command deletes an access control profile.
acl	show	This command displays the current access control profile.
acl	action (disable drop permit)	This command activates this profile. disable – disable the profile. drop – If packets match the profile, the packets will be dropped. permit – If packets match the profile, the packets will be forwarded.
acl	destination mac host MACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR	This command configures the destination MAC and mask for the profile.
acl	destination mac MACADDR MACADDR MACADDR	This command configures the destination MAC and mask for the profile. The second MACADDR parameter is the mask for the profile.
acl	no destination mac	This command removes the destination MAC from the profile.
acl	ethertype STRING	This command configures the ether type for the profile. Where the STRING is a hex-decimal value. e.g.: 08AA.
acl	no ethertype	This command removes the limitation of the ether type from the profile.
acl	source mac host MACADDR	This command configures the source MAC and mask for the profile.
acl	source mac MACADDR	This command configures the source AMC and mask for the profile.

	MACADDR	
acl	no source mac	This command removes the source MAC and mask from the profile.
acl	source ip host IPADDR	This command configures the source IP address for the profile.
acl	source ip IPADDR IPMASK	This command configures the source IP address and mask for the profile.
acl	no source ip	This command removes the source IP address from the profile.
acl	destination ip host IPADDR	This command configures a specific destination IP address for the profile.
acl	destination ip IPADDR IPMASK	This command configures the destination IP address and mask for the profile.
acl	no destination ip	This command removes the destination IP address from the profile.
acl	l4-source-port IPADDR	This command configures UDP/TCP source port for the profile.
acl	no l4-source-port IPADDR	This command removes the UDP/TCP source port from the profile.
acl	L4-destination-port PORT	This command configures the UDP/TCP destination port for the profile.
acl	no l4-destination-port	This command removes the UDP/TCP destination port from the profile.
acl	vlan VLANID	This command configures the VLAN for the profile.
acl	no vlan	This command removes the limitation of the VLAN from the profile.
acl	source interface PORT_ID	This command configures the source interface for the profile.
acl	no source interface PORT_ID	This command removes the source interface from the profile.

Where the MAC mask allows users to filter a range of MAC in the packets' source MAC or destination MAC.

For example:

```
source mac 00:01:02:03:04:05 ff:ff:ff:ff:00
```

➔ The command will filter source MAC range from 00:01:02:03:00:00 to 00:01:02:03:ff:ff

Where the IPMASK mask allows users to filter a range of IP in the packets' source IP or destination IP.

For example:

```
source ip 172.20.1.1 255.255.0.0
```

➔ The command will filter source IP range from 172.20.0.0 to 172.20.255.255

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#access-list 111
L2SWITCH(config-acl)#vlan 2
L2SWITCH(config-acl)#source interface 1
L2SWITCH(config-acl)#show
Profile Name: 111
Activate: disabled
VLAN: 2
Source Interface: 1
Destination MAC Address: any
Source MAC Address: any
Ethernet Type: any
Source IP Address: any
Destination IP Address: any
Source Application: any
Destination Application: any
```

6.2.2. Web Configuration

Access Control List

Access Control List Settings

Profile Name	<input type="text"/>	Action	Disable <input type="button" value="v"/>
Ethernet Type	Any <input type="button" value="v"/> <input type="text"/>	VLAN	Any <input type="button" value="v"/> <input type="text"/>
Source MAC	Any <input type="button" value="v"/> <input type="text"/>	Mask of Source MAC	<input type="text"/>
Destination MAC	Any <input type="button" value="v"/> <input type="text"/>	Mask of Destination MAC	<input type="text"/>
Source IP	Any <input type="button" value="v"/> <input type="text"/>	Mask of Source IP	<input type="text"/>
Destination IP	Any <input type="button" value="v"/> <input type="text"/>	Mask of Destination IP	<input type="text"/>
Source Application	Any <input type="button" value="v"/> <input type="text"/>		
Destination Application	Any <input type="button" value="v"/> <input type="text"/>		
Source Interface	Any <input type="button" value="v"/> <input type="text"/>		

Access Control List Status

Profile Name	111	State	Disabled
Ethernet Type	Any	VLAN	Any
Source MAC	Any	Mask of Source MAC	None
Destination MAC	Any	Mask of Destination MAC	None
Source IP	Any	Mask of Source IP	None
Destination IP	Any	Mask of Destination IP	None
Source Application	Any	Destination Application	Any
Source Interface(s)	Any		

Parameter	Description
Profile Name	The access control profile name.
State	Disables / Drop / Permits the access control on the Switch.
Ethernet Type	Configures the Ethernet type of the packets that you want to filter.
VLAN	Configures the VLAN of the packets that you want to filter.
Source MAC	Configures the source MAC of the packets that you want to filter.
Mask of Source MAC	Configures the bitmap mask of the source MAC of the packets that you want to filter. If the Source MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured in Source MAC field.
Destination MAC	Configures the destination MAC of the packets that you want to filter.
Mask of Destination MAC	Configures the bitmap mask of the destination MAC of the packets that you want to filter. If the Destination MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured in Destination MAC field.
Source IP	Configures the source IP of the packets that you want to filter.
Mask of Source IP	Configures the bitmap mask of the source IP of the packets that you want to filter. If the Source IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Source IP field.
Destination IP	Configures the destination IP of the packets that you want to filter.
Mask of Destination IP	Configures the bitmap mask of the destination IP of the packets that you want to filter. If the Destination IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Destination IP field.
Source Application	Configures the source UDP/TCP ports of the packets that you want to filter.
Destination Application	Configures the destination UDP/TCP ports of the packets that you want to filter.
Source Interface(s)	Configures one or a range of the source interfaces of the packets that you want to filter.

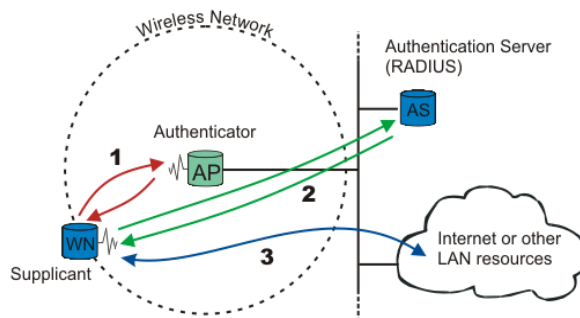
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

6.3. 802.1x

IEEE 802.1X is an IEEE Standard for port-based Network Access Control ("port" meaning a single point of attachment to the LAN infrastructure). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN, either establishing a point-to-point connection or preventing it if authentication fails. It is used for most wireless 802.11 access points and is based on the Extensible Authentication Protocol (EAP).

802.1X provides port-based authentication, which involves communications between a supplicant, authenticator, and authentication server. The supplicant is often software on a client device, such as a laptop, the authenticator is a wired Ethernet switch or wireless access point, and an authentication server is generally a RADIUS database. The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity is authorized. An analogy to this is providing a valid passport at an airport before being allowed to pass through security to the terminal. With 802.1X port-based authentication, the supplicant provides credentials, such as user name / password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the credentials are valid (in the authentication server database), the supplicant (client device) is allowed to access resources located on the protected side of the network.

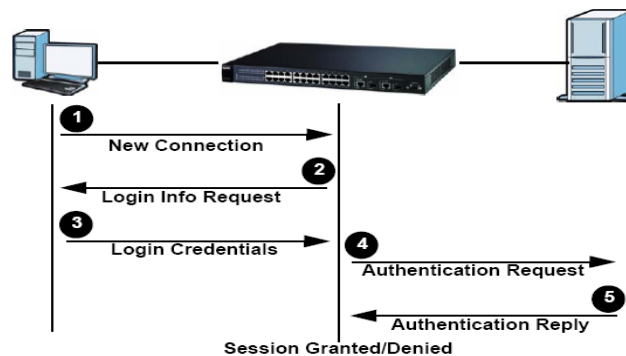
Upon detection of the new client (supplicant), the port on the switch (authenticator) is enabled and set to the "**unauthorized**" state. In this state, only 802.1X traffic is allowed; other traffic, such as DHCP and HTTP, is blocked at the network layer (Layer 3). The authenticator sends out the EAP-Request identity to the supplicant, the supplicant responds with the EAP-response packet that the authenticator forwards to the authenticating server. If the authenticating server accepts the request, the authenticator sets the port to the "authorized" mode and normal traffic is allowed. When the supplicant logs off, it sends an EAP-logoff message to the authenticator. The authenticator then sets the port to the "unauthorized" state, once again blocking all non-EAP traffic.



The following figure illustrates how a client connecting to a IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password.

When the client provides the login credentials, the Switch sends an authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

Figure 62 IEEE 802.1x Authentication Process



Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate users without interacting with a network authentication server. However, there is a limit on the number of users you may authenticate in this way.

Guest VLAN:

The Guest VLAN in IEEE 802.1x port authentication on the switch to provide limited services to clients, such as downloading the IEEE 802.1x client. These clients might be upgrading their system for IEEE 802.1x authentication.

When you enable a guest VLAN on an IEEE 802.1x port, the switch assigns clients to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.

Port Parameters:

- **Admin Control Direction:**
 - both - drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication.
 - in - drop only incoming packets on the port when a user has not passed 802.1x port authentication.
- **Re-authentication:**

Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
- **Reauth-period:**

Specify how often a client has to re-enter his or her username and password to stay connected to the port. The acceptable range for this field is 0 to 65535 seconds.

- **Port Control Mode:**
 auto : Users can access network after authenticating.
 force-authorized : Users can access network without authentication.
 force-unauthorized : Users cannot access network.

- **Quiet Period:**
 Specify a period of the time the client has to wait before the next re-authentication attempt. This will prevent the Switch from becoming overloaded with continuous re-authentication attempts from the client. The acceptable range for this field is 0 to 65535 seconds.

- **Server Timeout:**
 The server-timeout value is used for timing out the Authentication Server.

- **Supp-Timeout:**
 The supp-timeout value is the initialization value used for timing out a Supplicant.

- **Max-req Time:**
 Specify the amount of times the Switch will try to connect to the authentication server before determining the server is down. The acceptable range for this field is 1 to 10 times.

Default Settings

- The default global 802.1x state is disabled.
- The default 802.1x Authentication Method is local.
- The default port 802.1x state is disabled for all ports.
- The default port Admin Control Direction is both for all ports.
- The default port Re-authentication is disabled for all ports.
- The default port Control Mode is auto for all ports.
- The default port Guest VLAN is 0 for all ports. (Guest VLAN is disabled).
- The default port Max-req Time is 2 times for all ports.
- The default port Reauth period is 3600 seconds for all ports.
- The default port Quiet period is 60 seconds for all ports.
- The default port Supp timeout is 30 seconds for all ports.
- The default port Server timeout is 30 seconds for all ports.

6.3.1. CLI Configuration

Node	Command	Description
enable	show dot1x	This command displays the current 802.1x configurations.
enable	show dot1x username	This command displays the current user accounts for the local authentication.
enable	show dot1x	This command displays the local accounting

	accounting-record	records.
configure	dot1x authentication (disable enable)	This command enables/disables the 802.1x authentication on the switch.
configure	dot1x authentic-method (local radius)	This command configures the authentic method of 802.1x.
configure	no dot1x authentic-method	This command configures the authentic method of 802.1x to default.
configure	dot1x radius primary-server-ip <IP> port PORTID	This command configures the primary radius server.
configure	dot1x radius primary-server-ip <IP> port PORTID key KEY	This command configures the primary radius server.
configure	dot1x radius secondary-server-ip <IP> port PORTID	This command configures the secondary radius server.
configure	dot1x radius secondary-server-ip <IP> port PORTID key KEY	This command configures the secondary radius server.
configure	no dot1x radius secondary-server-ip	This command removes the secondary radius server.
configure	dot1x username <STRING> passwd <STRING>	This command configures the user account for local authentication.
configure	no dot1x username <STRING>	This command deletes the user account for local authentication.
configure	dot1x accounting (disable enable)	This command enables/disables the dot1x local accounting records.
configure	dot1x guest-vlan VLAN_ID	This command configures the guest vlan.
configure	no dot1x guest-vlan	This command removes the guest vlan.
interface	dot1x admin-control-direction (both in)	This command configures the control direction for blocking packets.
interface	dot1x default	This command sets the port configuration to default settings.
interface	dot1x max-req <1-10>	This command sets the max-req times of a port. (1~10).
interface	dot1x port-control (auto force-authorized force-unauthorized)	This command configures the port control mode on the port.
interface	dot1x authentication (disable enable)	This command enables/disables the 802.1x on the port.
interface	dot1x reauthentication (disable enable)	This command enables/disables re-authentication on the port.

interface	dot1x timeout quiet-period	This command configures the quiet-period value on the port.
interface	dot1x timeout server-timeout	This command configures the server-timeout value on the port.
interface	dot1x timeout reauth-period	This command configures the reauth-period value on the port.
interface	dot1x timeout supp-timeout	This command configures the supp-timeout value on the port.
interface	dot1x guest-vlan (disable enable)	This command configures the 802.1x state on the port.

6.3.2. Web Configuration

Global Settings

802.1x

Global Settings
Port Settings

Global Settings

State	<input type="text" value="Disable"/>		
Authentication Method	<input type="text" value="Local"/>		
Guest VLAN	<input type="text" value="3"/>		
Primary Radius Server	IP : <input type="text"/>	UDP Port : <input type="text"/>	Shared Key : <input type="text"/>
Secondary Radius Server	IP : <input type="text"/>	UDP Port : <input type="text"/>	Shared Key : <input type="text"/>
Local Authentic User	<input type="text" value="None"/> User Name : <input type="text"/> Password : <input type="text"/>		

Global Status

State	Disabled		
Authentication Method	Local		
Guset VLAN	3		
Primary Radius Server	IP : -	UDP Port : -	Shared Key : -
Secondary Radius Server	IP : -	UDP Port : -	Shared Key : -
Local Authentication User	admin,		

Parameter	Description
State	Select Enable to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
Authentication	Select whether to use Local or RADIUS as the authentication

Method		<p>method.</p> <p>The Local method of authentication uses the “guest” and “user” user groups of the user account database on the Switch itself to authenticate.</p> <p>However, only a certain number of accounts can exist at one time.</p> <p>RADIUS is a security protocol used to authenticate users by means of an external server instead of an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS allows you to validate an unlimited number of users from a central location.</p>
Guest VLAN		Configure the guest vlan.
Primary Server	Radius	When RADIUS is selected as the 802.1x authentication method, the Primary Radius Server will be used for all authentication attempts.
IP Address		Enter the IP address of an external RADIUS server in dotted decimal notation.
UDP Port		The default port of a RADIUS server for authentication is 1812 .
Share Key		Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.
Second Radius Server		This is the backup server used only when the Primary Radius Server is down.
Global Status		
State		This field displays if 802.1x authentication is Enabled or Disabled .
Authentication Method		This field displays if the authentication method is Local or RADIUS .
Guest VLAN		The field displays the guest vlan.
Primary Server	Radius	This field displays the IP address, UDP port and shared key for the Primary Radius Server . This will be blank if nothing has been set.
Secondary Server	Radius	This is the backup server used only when the Primary Radius Server is down.
Apply		Click Apply to add/modify the settings.
Refresh		Click Refresh to begin configuring this screen afresh.

Port Settings

802.1x

Global Settings
Port Settings

Port Settings

Port: From: To:

802.1x State:

Admin Control Direction	Reauthentication	Port Control Mode	Guest VLAN	Max-req Times
<input type="text" value="Both"/>	<input type="text" value="Disable"/>	<input type="text" value="Auto"/>	<input type="text" value="Disable"/>	<input type="text" value="2"/>
Reauth-period	Quiet-period	Supp-timeout	Server-timeout	Reset to Default
<input type="text" value="3600"/>	<input type="text" value="60"/>	<input type="text" value="30"/>	<input type="text" value="30"/>	<input type="checkbox"/>

Note : Please don't set "enable" on all ports at the same time.

Port Status

Port	802.1x State	Admin Control Direction	Reauthentication	Port Control Mode	Guest VLAN	Max-req Times	Reauth-period	Quiet-period	Supp-timeout	Server-timeout
1	Disabled	Both	Disabled	Auto	Disabled	2	3600	60	30	30
2	Disabled	Both	Disabled	Auto	Disabled	2	3600	60	30	30
3	Disabled	Both	Disabled	Auto	Disabled	2	3600	60	30	30

Parameter	Description
Port	Select a port number to configure.
802.1x State	Select Enable to permit 802.1x authentication on the port. You must first enable 802.1x authentication on the Switch before configuring it on each port.
Admin Control Direction	Select Both to drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication. Select In to drop only incoming packets on the port when a user has not passed 802.1x port authentication.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Port Control Mode	Select Auto to require authentication on the port. Select Force Authorized to always force this port to be authorized. Select Force Unauthorized to always force this port to be unauthorized. No packets can pass through this port.
Guest VLAN	Select Disable to disable Guest VLAN on the port.

	Select Enable to enable Guest VLAN on the port.
Max-req Time	Specify the amount of times the Switch will try to connect to the authentication server before determining the server is down. The acceptable range for this field is 1 to 10 times.
Reauth period	Specify how often a client has to re-enter his or her username and password to stay connected to the port. The acceptable range for this field is 0 to 65535 seconds.
Quiet period	Specify a period of the time the client has to wait before the next re-authentication attempt. This will prevent the Switch from becoming overloaded with continuous re-authentication attempts from the client. The acceptable range for this field is 0 to 65535 seconds.
Supp timeout	Specify how long the Switch will wait before communicating with the server. The acceptable range for this field is 0 to 65535 seconds.
Server timeout	Specify how long the Switch to time out the Authentication Server. The acceptable range for this field is 0 to 65535 seconds.
Reset to Default	Select this and click Apply to reset the custom 802.1x port authentication settings back to default.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Port Status	
Port	This field displays the port number.
802.1x State	This field displays if 802.1x authentication is Enabled or Disabled on the port.
Admin Control Direction	This field displays the Admin Control Direction. Both will drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication. In will drop only incoming packets on the port when a user has not passed 802.1x port authentication.
Reauthentication	This field displays if the subscriber must periodically re-enter his or her username and password to stay connected to the port.
Port Control Mode	This field displays the port control mode. Auto requires authentication on the port. Force Authorized forces the port to be authorized. Force Unauthorized forces the port to be unauthorized. No

	packets can Pass through the port.
Guest VLAN	This field displays the Guest VLAN setting for hosts that have not passed authentication.
Max-req Time	This field displays the amount of times the Switch will try to connect to the authentication server before determining the server is down.
Reauth period	This field displays how often a client has to re-enter his or her username and password to stay connected to the port.
Quiet period	This field displays the period of the time the client has to wait before the next re-authentication attempt.
Supp timeout	This field displays how long the Switch will wait before communicating with the server.
Server timeout	This field displays how long the Switch will wait before communicating with the client.

6.4. Port Security

The Switch will learn the MAC address of the device directly connected to a particular port and allow traffic through. We will ask the question: “How do we control who and how many can connect to a switch port?” This is where port security can assist us. The Switch allow us to control which devices can connect to a switch port or how many of them can connect to it (such as when a hub or another switch is connected to the port).

Let’s say we have only one switch port left free and we need to connect five hosts to it. What can we do? Connect a hub or switch to the free port! Connecting a switch or a hub to a port has implications. It means that the network will have more traffic. If a switch or a hub is connected by a user instead of an administrator, then there are chances that loops will be created. So, it is best that number of hosts allowed to connect is restricted at the switch level. This can be done using the “port-security limit” command. This command configures the maximum number of MAC addresses that can source traffic through a port.

Port security can sets maximum number of MAC addresses allowed per interface. When the limit is exceeded, incoming packets with new MAC addresses are dropped. It can be use MAC table to check it. The static MAC addresses are included for the limit.

Note: If you configure a port of the Switch from disabled to enabled, all of the MAC learned by this port will be clear.

Default Settings

- The port security on the Switch is disabled.
- The Maximum MAC per port is 5.
- The port state of the port security is disabled.

6.4.1. CLI Configuration

Node	Command	Description
enable	show port-security	This command displays the current port security configurations.
config	port-security (disable enable)	This command enables / disables the global port security function.
interface	port-security (disable enable)	This command enables / disables the port security function on the specific port.
interface	port-security limit VALUE	This command configures the maximum MAC entries on the specific port.

6.4.2. Web Configuration

Port Security

Port Security Settings

Port Security Disable ▾

Port	State	Maximum MAC
From: 1 ▾ To: 1 ▾	Disable ▾	5 (1~30)

Port Security Status

Port	State	Maximum MAC	Port	State	Maximum MAC
1	Disable	5	2	Disable	5
3	Disable	5	4	Disable	5
5	Disable	5	6	Disable	5

Parameter	Description
Port Security Settings	
Port Security	Select Enable/Disable to permit Port Security on the Switch.
Port	Select a port number to configure.
State	Select Enable/Disable to permit Port Security on the port.
Maximum MAC	The maximum number of MAC addresses allowed per interface. The acceptable range is 1 to 30.
Port Security Status	
Port	This field displays a port number.
State	This field displays if Port Security is Enabled or Disabled
Maximum MAC	This field displays the maximum number of MAC addresses

6.5. Switch Lock

Roles:

- ✓ **Default:** This is an invalid role, for initial configurations only.
If the Switch's role is Default, normal user can configure their Switch to one of below roles. If the Switch's role is one of below roles, user cannot change the Switch's role.
- ✓ **Master:** Can access slave's authentications.
All ports are configured as users want.
- ✓ **Slave:** Uplink ports are enabled. Downlink ports are disabled.
The Switch need authenticate with the master Switch to enable all of the downlink ports.
- ✓ **Master_Slave:** Uplink ports are enabled. Downlink ports are enabled, but blocked with port isolation.
The Switch can access slave's authentication from downlink ports. The Switch need authenticate with a Master which connect to the uplink ports to normalize all of the downlink ports.

When the Switch is authenticating, the POST LED will be On/Off every seconds.

Notice: If the Slave has default vendor key and the Master don't have, the Master will inform the Slave to change its vendor key when the Slave starts to authenticate.

Default Configurations:

- Role = Default. (Invalid), must be changed.
- Uplink Ports = None.
- Vendor Key = 123456789012345678901234567890
- State = disable.

6.5.1. CLI Configurations

Node	Command	Description
enable	show switch-lock	This command displays the current Switch Lock configurations.
configure	switch-lock state (disable enable)	This command enables/disables the global state of the Switch Lock function.
configure	switch-lock clear counter	This command clears all of the ports' authentication counters.
configure	switch-lock role (master slave master-slave)	This command configures the role for the Switch Lock function.
configure	switch-lock uplink-port PORTLIST	This command configures the uplink port list for the Switch Lock.
configure	switch-lock vendor-key STRING	This command configures the vendor key for the Switch Lock.(Up to 30 characters)

switch-lock role (master|slave|master-slave)

- ✓ If the current Role is Default, the Switch can be changed to one of the three roles: master, slave, master-slave.
- ✓ If the role has been changed, it cannot be changed to another role.

switch-lock (disable|enable)

- ✓ If the current state is disabled, the Switch can be enabled.
- ✓ If the state has been enabled, it cannot be disabled again.

switch-lock vendor-key STRING

- ✓ If the current Vendor Key is the default value, 123456789012345678901234567890, the Switch can be configured to any values.
- ✓ If the Vendor Key has been changed, it cannot be changed again.

switch-lock uplink-port PORTLIST

- ✓ User can configure any ports as uplink-port.
- ✓ If the Switch's role is slave, the uplink port count cannot be 0.

6.5.2. Web Configurations

Switch Lock											
Switch Lock											
<table border="1"> <thead> <tr> <th colspan="2">Switch Lock</th> </tr> </thead> <tbody> <tr> <td>State</td> <td>Disabled</td> </tr> <tr> <td>Role</td> <td>Default</td> </tr> <tr> <td>Uplink Port(s)</td> <td>N/A</td> </tr> <tr> <td>Authentication Status</td> <td>N/A</td> </tr> </tbody> </table>		Switch Lock		State	Disabled	Role	Default	Uplink Port(s)	N/A	Authentication Status	N/A
Switch Lock											
State	Disabled										
Role	Default										
Uplink Port(s)	N/A										
Authentication Status	N/A										
Parameter	Description										
State	The current global state for the Switch Lock.										
Role	The current role of the Switch for the Switch Lock.										
Uplink Port	The uplink port list for the Switch Lock.										
Authentication Status	The authentication status for the slave function. (Discovery, Authenticating or Authenticated).										

7. Monitor

7.1. Hardware Information

The feature displays some hardware information to monitor the system to guarantee the network correctly.

- A. Displays the board's and CPU's and MAC chip's temperature.
- B. Displays the 1.0V and 2.5V and 3.3V input status.

7.1.1. CLI Configuration

Node	Command	Description
enable	show hardware-monitor (C/F)	This command displays hardware working information.

```
MEN-5410#show hardware-monitor C
```

Hardware Working Information:

Temperature(C)	Current	MAX	MIN	Threshold	Status
BOARD	0.0	0.0	0.0	80.0	Normal
MAC	0.0	0.0	0.0	80.0	Normal
CPU	0.0	0.0	0.0	80.0	Normal

Voltage(V)	Current	MAX	MIN	Threshold	Status
1.0V IN	0.000	0.000	0.000	+/-5%	Error
2.5V IN	0.000	0.000	0.000	+/-5%	Error
3.3V IN	0.000	0.000	0.000	+/-5%	Error

Battery Information:

Voltage(V)	Current
12VIN_BAT	0.000

7.1.2. Web Configuration

Hardware Information

Hardware Information

Temperature unit: Fahrenheit(F) ▾ Change

Hardware Working Information:

Temperature(F)	Current	MAX	MIN	Threshold	Status
BOARD	88.7	88.7	88.7	176.0	Normal
CPU	95.9	95.9	95.9	176.0	Normal
PHY	110.8	112.6	110.8	176.0	Normal
Voltage(V)	Current	MAX	MIN	Threshold	Status
1.0V IN	0.983	0.983	0.983	+/-5%	Normal
1.8V IN	1.768	1.768	1.768	+/-5%	Normal
3.3V IN	3.272	3.272	3.272	+/-5%	Normal

Battery Information:

Voltage(V)	Current
12VIN_BAT	---

Power Source: AC

Refresh

7.2. Port Utilization

This feature helps users to monitor the ports' traffic utilization, to display the link up ports' traffic utilization only.

7.2.1. CLI Configuration

Node	Command	Description
enable	show port-utilization	This command displays the link up ports' traffic utilization.

7.2.2. Web Configuration

Port Utilization

Port Traffic Utilization Status

Port	Speed	Traffic Utilization (%)
1	1000	0.001

Refresh

Parameter	Description
-----------	-------------

Port	Select a port or a range of ports to display their RMON statistics.
Speed	The current port speed.
Utilization	The port traffic utilization.
Refresh	Click this button to refresh the screen quickly.

7.3. RMON Statistics

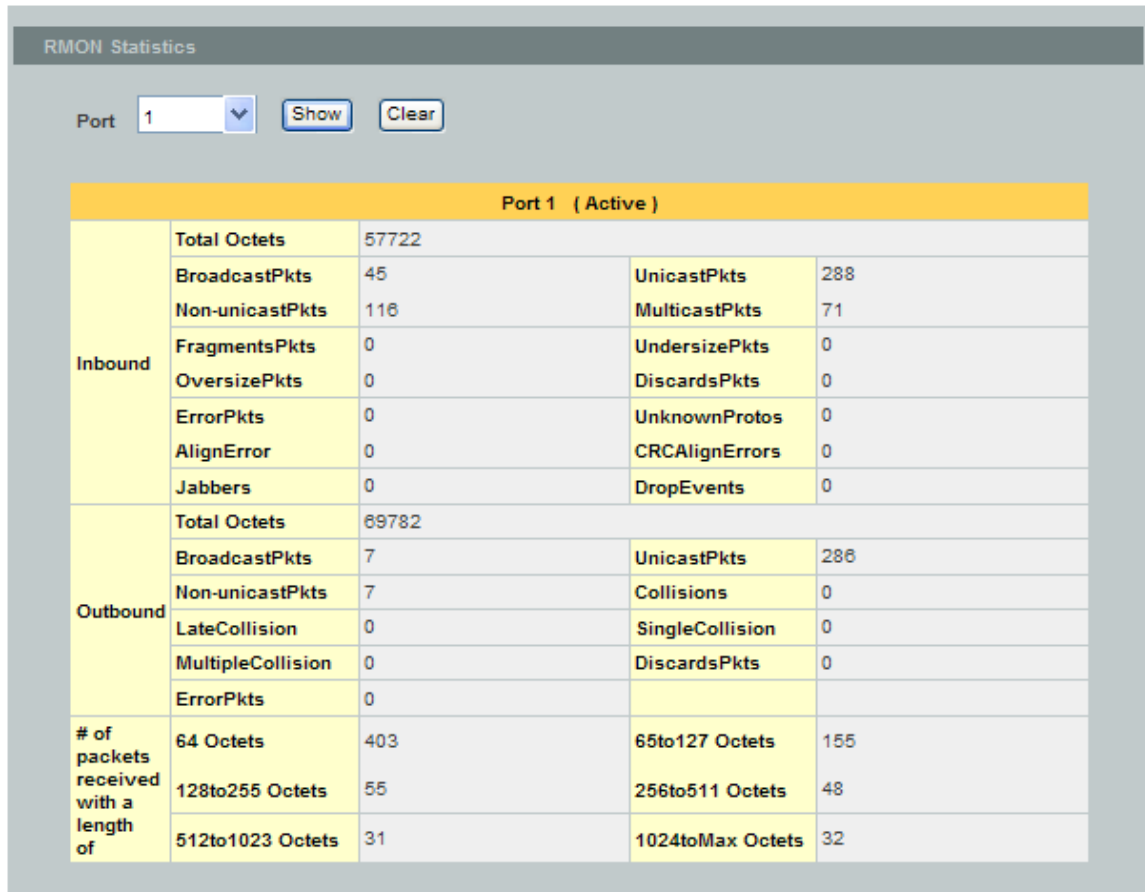
This feature helps users to monitor or clear the port's RMON statistics.

7.3.1. CLI Configuration

Node	Command	Description
enable	show rmon statistics	This command displays the RMON statistics.
configure	clear rmon statistics [IFNAME]	This command clears one port's or all ports' RMON statistics.

7.3.2. Web Configuration

RMON Statistics



The screenshot shows the 'RMON Statistics' web interface. At the top, there is a 'Port' dropdown menu set to '1', and 'Show' and 'Clear' buttons. Below this, a table displays statistics for 'Port 1 (Active)'. The table is organized into three main sections: Inbound, Outbound, and # of packets received with a length of.

Port 1 (Active)			
Inbound	Total Octets	57722	
	BroadcastPkts	45	UnicastPkts 288
	Non-unicastPkts	116	MulticastPkts 71
	FragmentsPkts	0	UndersizePkts 0
	OversizePkts	0	DiscardsPkts 0
	ErrorPkts	0	UnknownProtos 0
	AlignError	0	CRCAlignErrors 0
	Jabbers	0	DropEvents 0
Outbound	Total Octets	69782	
	BroadcastPkts	7	UnicastPkts 288
	Non-unicastPkts	7	Collisions 0
	LateCollision	0	SingleCollision 0
	MultipleCollision	0	DiscardsPkts 0
	ErrorPkts	0	
# of packets received with a length of	64 Octets	403	65to127 Octets 155
	128to255 Octets	55	256to511 Octets 48
	512to1023 Octets	31	1024toMax Octets 32

Parameter	Description
Port	Select a port or a range of ports to display their RMON statistics.
Show	Show them.
Clear	Clear the RMON statistics for the port or a range of ports.

7.4. SFP Information

The SFP information allows user to know the SFP module's information, such as vendor name, connector type, revision, serial number, manufacture date. And to know the DDMI information if the SFP modules have supported the DDMI functions.

7.4.1. CLI Configuration

Node	Command	Description
enable	show sfp info port PORT_ID	This command displays the SFP information.
enable	show sfp ddmI port PORT_ID	This command displays the SFP DDMI status.

7.4.2. Web Configuration

SFP Information

SFP Information

Port

SFP Information	
Fiber Cable	Link Down
Connector	0x7
Vendor Name	ATOP
Vendor PN	AP-B53011-3CDL10
Vendor rev	
Vendor SN	SF53123700002
Date code	120917 7→□□

DDMI Information					
	Current	High-Alarm	Low-Alarm	High-Warnm	Low-Warn
Temperature(C)	31.41	100.00	-45.00	90.00	-40.00
Voltage(V)	3.21	3.60	3.00	3.50	3.10
Tx Bias(mA)	5.70	60.00	2.03	50.00	2.53
Tx Power(dBm)	-10.44	-6.00	-17.01	-7.00	-16.00
Rx Power(dBm)	0.00	0.00	0.00	0.00	0.00

Parameter	Description
Port	Select a port number to configure.
Apply	Click Apply to display the SFP information.
Fiber Cable	To indicate if the fiber cable is connected.
Connector	Code of optical connector type.
Vendor Name	SFP vendor name.
Vendor PN	Part Number.
Vendor rev	Revision level for part number.
Vendor SN	Serial number (ASCII).
Date Code	Manufacturing date code.

7.5. Traffic Monitor

The function can be enabled / disabled on a specific port or globally be enabled disabled on the Switch.

The function will monitor the broadcast / multicast / broadcast and multicast packets rate. If the packet rate is over the user's specification, the port will be blocked. And if the recovery function is enabled, the port will be enabled after recovery time.

Default Settings

Port	State	Status	Packet Type	Packet Rate(pps)	Recovery State	Recovery Time(min)
1	Disabled	Normal	Bcast	1000	Enabled	1
2	Disabled	Normal	Bcast	1000	Enabled	1
3	Disabled	Normal	Bcast	1000	Enabled	1
4	Disabled	Normal	Bcast	1000	Enabled	1
5	Disabled	Normal	Bcast	1000	Enabled	1
6	Disabled	Normal	Bcast	1000	Enabled	1

7.5.1. CLI Configuration

Node	Command	Description
enable	show traffic-monitor	This command displays the traffic monitor configurations and current status.
configure	traffic-monitor (disable enable)	This command enables / disables the traffic monitor on the Switch.

interface	traffic-monitor rate RATE_LIMIT type (bcast mcast bcast+mcast)	This command configures the packet rate and packet type for the traffic monitor on the specific port. bcast – Broadcast packet. mcast – Multicast packet. The rate should be greater than 50 pps.
interface	traffic-monitor (disable enable)	This command enables / disables the traffic monitor on the specific port.
interface	traffic-monitor recovery (disable enable)	This command enables / disables the recovery function for the traffic monitor on the specific port.
interface	traffic-monitor recovery time VALUE	This command configures the recovery time for the traffic monitor on the specific port.

7.5.2. Web Configuration

Traffic Monitor

Traffic Monitor Settings

State: Disable ▾

Port	State	Action	Packet Type	Packet Rate(pps)	Recovery State	Recovery Time (min)
From: 1 ▾ To: 1 ▾	Disable ▾	None ▾	Broadcast ▾	1000	Enable ▾	1

Apply
Refresh

Traffic Monitor Status

Port	State	Status	Packet Type	Packet Rate(pps)	Recovery State	Recovery Time (min)
1	Disabled	Normal	Broadcast	1000	Enabled	1
2	Disabled	Normal	Broadcast	1000	Enabled	1
3	Disabled	Normal	Broadcast	1000	Enabled	1
4	Disabled	Normal	Broadcast	1000	Enabled	1
5	Disabled	Normal	Broadcast	1000	Enabled	1
6	Disabled	Normal	Broadcast	1000	Enabled	1

Parameter	Description
State	Globally enables / disables the traffic monitor function.
Port	The port range which you want to configure.
State	Enables / disables the traffic monitor function on these ports.
Action	Unblock these ports.

Packet Type	Specify the packet type which you want to monitor.
Packet Rate	Specify the packet rate which you want to monitor.
Recover State	Enables / disables the recovery function for the traffic monitor function on these ports.
Recovery Time	Configures the recovery time for the traffic monitor function on these ports.(Range: 1 – 60 minutes)

CONFIDENTIAL

8. Management

8.1. Auto Provision

Auto provision is a service that service provider can quickly, easily and automatically configure remote device or doing firmware upgrade at remote side.

1. When the Auto Provision is enabled, the Switch will download the auto provision information file from the auto provision server first.

The file name is followed below naming rule:

Model_Name_Autoprovision.txt

For Example: *MEN-5410_Autoprovision.txt*

The contents of the file are listed below:

```
AUTO_PROVISION_VER=1
Firmware_Upgrade_State=1
Firmware_Version=5410-000-1.0.0.b1
Firmware_Image_File=5410-000-1.0.0.b1.fw
Firmware_Reboot=1
Global_Configuration_State=0
Global_Configuration_File=5410-000-1.0.0.b1.save
Global_Configuration_Reboot=0
Specific_Configuration_State=0
Specific_Configuration_Reboot=0
```

2. If AUTO_PROVISION_VER is biggest than current auto provision version, do step 3; otherwise, wait 24 hours and go back to step 1.
3. If the Firmware_Upgrade_State =1, do step 4; otherwise, do step 6.
4. If the Firmware_Version is difference than current firmware version, download the Firmware_Image_File and upgrade firmware.
5. If upgrade firmware succeeded and Firmware_Reboot=1, let reboot_flag=1.
6. If the Global_Configuration_State =1, download the Global_Configuration_File and upgrade configuration; otherwise, do step 8.
7. If upgrade configutation succeeded and Global_Configuration_Reboot =1, let reboot_flag=1.
8. If the Specific_Configuration_State =1, download the specific configuration file and upgrade configuration; otherwise do step 10. The naming is “Model_Name _” with 12-bit MAC digits ,example for following is “MEN-5410_00e04c8196b9.txt”
9. If upgrade configutation succeeded and Specific_Configuration_Reboot =1, let

reboot_flag=1.

10. If reboot_flag=1, save running configuration and reboot the switch; otherwise, wait 24 hours and go back to step 1.

Default Settings

Auto provision configuration profile:

Active : Disable
 Version : 0
 Protocol : FTP
 FTP user/pwd : /
 Folder :
 Server address :

8.1.1. CLI Configuration

Node	Command	Description
auto-provision	show	This command displays the current auto provision configurations.
auto-provision	active (enable disable)	This command enables/disables the auto provision function.
auto-provision	server-address IPADDR	This command configures the auto provision server's IP.
auto-provision	protocol (tftp/http/ftp)	The command configurations the upgrade protocol.
auto-provision	FTP-user username STRING password STRING	The command configurations the username and password for the FTP server.
auto-provision	folder STRING	The command configurations the folder for the auto provision server.
auto-provision	version <0-65535>	The command configurations the version for auto provision on the switch.
auto-provision	no folder	The command configurations the folder to default.
auto-provision	no FTP-user	The command configurations the username and password to default.

8.1.2. Web Configuration

Auto Provision

Auto Provision Settings

State	<input type="text" value="Disable"/>
Status	Disable
Version	0
Protocol	<input type="text" value="FTP"/>
Server IP	<input type="text" value="0.0.0.0"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Folder Path	<input type="text"/>

8.2. Mail Alarm

The feature sends an e-mail trap to a predefined administrator when some events occur. The events are listed below:

- ◆ System Reboot : The system warm start or cold start.
- ◆ Port Link Change : A port link up or down.
- ◆ Configuration Change : The system configurations in the NV-RAM have been updated.
- ◆ Firmware Upgrade : The system firmware image has been updated.
- ◆ User Login : A user login the system.
- ◆ Port Blocked : A port is blocked by looping detection or BPDU Guard.

Default Settings

Mail-Alarm Configuration:

State : Disabled.
 Server IP : 0.0.0.0
 Server Port : 25
 Mail From :
 Mail To :

Trap Event Status:

System Reboot : Disabled.
 Port Link Change : Disabled.
 Configuration Change : Disabled.
 Firmware Upgrade : Disabled.

User Login : Disabled.
 Port Blocked : Disabled.
 Alarm : Disabled.

8.2.1. Reference

Default Ports	Server	Authentication	Port
SMTP Server (Outgoing Messages)	Non-Encrypted	AUTH	25 (or 587)
	Secure (TLS)	StartTLS	587
	Secure (SSL)	SSL	465
POP3 Server (Incoming Messages)	Non-Encrypted	AUTH	110
	Secure (SSL)	SSL	995
Googlemail - Gmail			
SMTP Server (Outgoing Messages)	smtp.gmail.com	SSL	465
	smtp.gmail.com	StartTLS	587
POP3 Server (Incoming Messages)	pop.gmail.com	SSL	995
Outlook.com			
SMTP Server (Outgoing Messages)	smtp.live.com	StartTLS	587
POP3 Server (Incoming Messages)	pop3.live.com	SSL	995
Yahoo Mail			
SMTP Server (Outgoing Messages)	smtp.mail.yahoo.com	SSL	465
POP3 Server (Incoming Messages)	pop.mail.yahoo.com	SSL	995
Yahoo Mail Plus			
SMTP Server (Outgoing Messages)	plus.smtp.mail.yahoo.com	SSL	465
POP3 Server (Incoming Messages)	plus.pop.mail.yahoo.com	SSL	995

8.2.2. CLI Configuration

Node	Command	Description
enable	show mail-alarm	This command displays the Mail Alarm configurations.
configure	mail-alarm (disable enable)	This command disables / enables the Mail Alarm function.
configure	mail-alarm auth-account	This command configures the Mail server authentication account.
configure	mail-alarm mail-from	This command configures the mail sender.
configure	mail-alarm mail-to	This command configures the mail receiver.
configure	mail-alarm server-ip	This command configures the mail server IP

	IPADDR server-port VALUE	address and the TCP port.
configure	mail-alarm server-ip IPADDR server-port Default	This command configures the mail server IP address and configures 25 as the server's TCP port.
configure	mail-alarm trap-event (reboot link-change config. firmware login port-blocked alarm) (disable enable)	This command disables / enables mail trap events.

8.2.3. Web Configuration

Mail Alarm

Mail Alarm Settings

State: ▾

Server IP: Server Port: (Default:25)

Account Name: Account Password:

Mail From:

Mail To:

Trap State :

Select All Deselect All

System Reboot Port Link Change Configuration Change Firmware Upgrade User Login

Port Blocked Alarm

Parameter	Description
State	Enable / disable the Mail Alarm function.
Server IP	Specifies the mail server's IP address.
Server Port	Specifies the TCP port for the SMTP.
Account Name	Specifies the mail account name.
Account Password	Specifies the mail account password.
Mail From	Specifies the mail sender.
Mail To	Specifies the mail receiver.
Trap State	Enables / disables the mail trap event states.

8.3. Maintenance

8.3.1. Configuration

8.3.1.1. CLI Configuration

Node	Command	Description
configure	reboot	This command reboots the system.
configure	reload default-config	This command copies a default-config file to replace the current one. Note: The system will reboot automatically to take effect the configurations.
configure	write memory	This command writes current operating configurations to the configuration file.
configure	archive download-config <URL PATH>	This command downloads a new copy of configuration file from TFTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file
configure	archive upload-config <URL PATH>	This command uploads the current configurations file to a TFTP server.
configure	archive download-fw <URL PATH>	This command downloads a new copy of firmware file from TFTP / FTP / HTTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#interface eth0
L2SWITCH(config-if)#ip address 172.20.1.101/24
L2SWITCH(config-if)#ip address default-gateway 172.20.1.1
L2SWITCH(config-if)#management vlan 1
```

Enable the DHCP client function for the switch.

- L2SWITCH#configure terminal
- L2SWITCH(config)#interface eth0
- L2SWITCH(config-if)#ip dhcp client enable

8.3.1.2. Web Configuration

Maintenance

Configuration
Firmware
Reboot

Save Configurations

Save the parameter settings of the Switch :

Upload and Download Configurations

Upload configuration file to your Switch.

File path No file chosen

Press "Download" to save configuration file to your PC.

Reset Configurations

Reset the factory default settings of the Switch :

- IP address will be 192.168.0.254

Save Configurations

Save Configurations

Save the parameter settings of the Switch :

Press the Save button to save the current settings to the NV-RAM (flash).

Upload / Download Configurations to /from a your server

Upload and Download Configurations

Upload configuration file to your Switch.

File path No file chosen

Press "Download" to save configuration file to your PC.

Follow the steps below to save the configuration file to your PC.

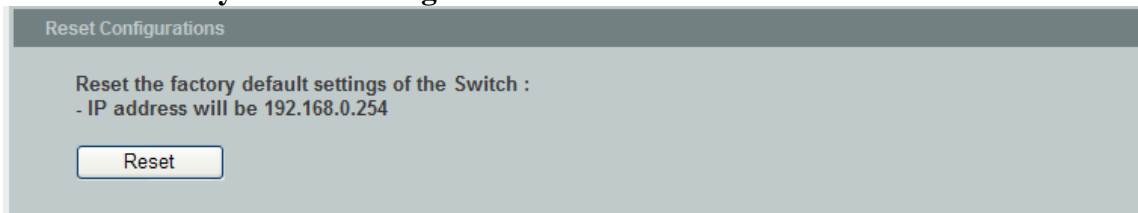
- Select the “Press “Download” to save configurations file to your PC”.
- Click the “Download” button to start the process.

Follow the steps below to load the configuration file from your PC to the Switch.

- Select the “Upload configurations file to your Switch”.

- Select the full path to your configuration file.
- Click the Upload button to start the process.

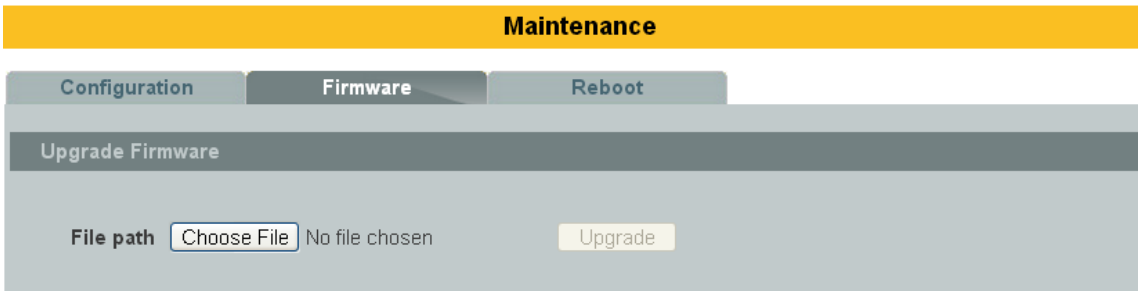
Reset the factory default settings of the Switch



Press the Reset button to set the settings to factory default configurations.

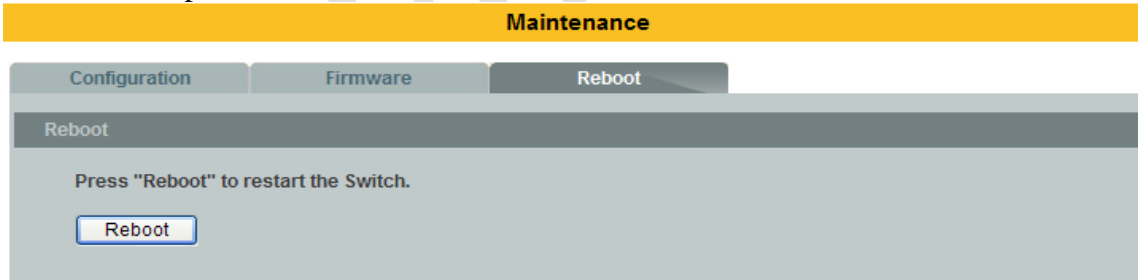
8.3.2. Firmware

Type the path and file name of the firmware file you wish to upload to the Switch in the **File path** text box or click **Browse** to locate it. Click **Upgrade** to load the new firmware.

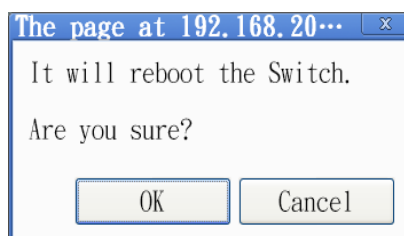


8.3.3. Reboot

Reboot allows you to restart the Switch without physically turning the power off. Follow the steps below to reboot the Switch.



- In the **Reboot** screen, click the **Reboot** button. The following screen displays.



- Click **OK** again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

8.4. SNMP

Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

Support below MIBs:

- RFC 1157 A Simple Network Management Protocol
- RFC 1213 MIB-II
- RFC 1493 Bridge MIB
- RFC 1643 Ethernet Interface MIB
- RFC 1757 RMON Group 1,2,3,9

SNMP community act like passwords and are used to define the security parameters of SNMP clients in an SNMP v1 and SNMP v2c environments. The default SNMP community is “public” for both SNMP v1 and SNMP v2c before SNMP v3 is enabled. Once SNMP v3 is enabled, the communities of SNMP v1 and v2c have to be unique and cannot be shared.

Network ID of Trusted Host:

The IP address is a combination of the Network ID and the Host ID.

Network ID = (Host IP & Mask).

User need only input the network ID and leave the host ID to 0. If user has input the host ID, such as 192.168.1.102, the system will reset the host ID, such as 192.168.1.0

Note: Allow user to configure the community string and rights only.

User configures the Community String and the Rights and the Network ID of Trusted Host=0.0.0.0, Subnet Mask=0.0.0.0. It means that all hosts with the community string can access the Switch.

Default Settings

- SNMP : disabled.
- System Location : L2SWITCH. (Maximum length 64 characters)
- System Contact : None. (Maximum length 64 characters)
- System Name : None. (Maximum length 64characters)
- Trap Receiver : None.
- Community Name : None.
- The maximum entry for community : 3.
- The maximum entry for trap receiver : 5.

8.4.1. CLI Configuration

Node	Command	Description
enable	show snmp	This command displays the SNMP configurations.
configure	snmp community STRING (ro rw) trusted-host IPADDR	This command configures the SNMP community name.
configure	snmp (disable enable)	This command disables/enables the SNMP on the switch.
configure	snmp system-contact STRING	This command configures contact information for the system.
configure	snmp system-location STRING	This command configures the location information for the system.
configure	snmp system-name STRING	This command configures a name for the system. (The System Name is same as the host name)
configure	snmp trap-receiver IPADDR VERSION COMMUNITY	This command configures the trap receiver's configurations, including the IP address, version (v1 or v2c) and community.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#snmp enable
L2SWITCH(config)#snmp community public rw trusted-host 192.168.200.106/24
L2SWITCH(config)#snmp trap-receiver 192.168.200.106 v2c public
L2SWITCH(config)#snmp system-contact IT engineer
L2SWITCH(config)#snmp system-location Volkte
```

8.4.2. Web Configuration

SNMP Setting



Parameter	Description
SNMP State	Select Enable to activate SNMP on the Switch.

	Select Disable to not use SNMP on the Switch.
System Name	Type a System Name for the Switch. (The System Name is same as the host name)
System Location	Type a System Location for the Switch.
System Contact	Type a System Contact for the Switch.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last saved setting.

Community Name

SNMP

SNMP Settings
Community Name
Trap Receiver

Community Name Settings

Community String	Rights	Network ID of Trusted Host	Mask
<input type="text"/>	Read-Only v	<input type="text"/>	<input type="text"/>

Community Name List

No.	Community String	Rights	Network ID of Trusted Host	Mask	Action
1	public	Read/Write	192.168.200.0	255.255.255.0	<input type="button" value="Delete"/>

Parameter	Description
Community String	Enter a Community string; this will act as a password for requests from the management station. An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
Rights	Select Read-Only to allow the SNMP manager using this string to collect information from the Switch. Select Read-Write to allow the SNMP manager using this string to create or edit MIBs (configure settings on the Switch).
Network ID of Trusted Host	Type the IP address of the remote SNMP management station in dotted decimal notation, for example 192.168.1.0.
Mask	Type the subnet mask for the IP address of the remote SNMP management station in dotted decimal notation, for example

	255.255.255.0.
Apply	Click Apply to configure the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Community Name List	
No.	This field indicates the community number. It is used for identification only. Click on the individual community number to edit the community settings.
Community String	This field displays the SNMP community string. An SNMP community string is a text string that acts as a password.
Right	This field displays the community string's rights. This will be Read Only or Read Write .
Network ID of Trusted Host	This field displays the IP address of the remote SNMP management station after it has been modified by the subnet mask.
Subnet Mask	This field displays the subnet mask for the IP address of the remote SNMP management station.
Action	Click Delete to remove a specific Community String.

Trap Receiver

SNMP

SNMP Settings
Community Name
Trap Receiver

Trap Receiver Settings

IP Address	Version	Community String
<input type="text"/>	v1 ▼	<input type="text"/>

Trap Receiver List

No.	IP Address	Version	Community String	Action
1	192.168.200.59	v2c	public	<input type="button" value="Delete"/>

Parameter	Description
IP Address	Enter the IP address of the remote trap station in dotted decimal notation.
Version	Select the version of the Simple Network Management Protocol to use v1 or v2c .
Community String	Specify the community string used with this remote trap station.
Apply	Click Apply to configure the settings.

Refresh	Click Refresh to begin configuring this screen afresh.
Trap Receiver List	
No.	This field displays the index number of the trap receiver entry. Click the number to modify the entry.
IP Address	This field displays the IP address of the remote trap station.
Version	This field displays the version of Simple Network Management Protocol in use. v1 or v2c .
Community String	This field displays the community string used with this remote trap station.
Action	Click Delete to remove a configured trap receiver station.

8.5. System log

The syslog function records some of system information for debugging purpose. Each log message recorded with one of these levels, **Alert / Critical / Error / Warning / Notice / Information**. The syslog function can be enabled or disabled. The default setting is disabled. The log message is recorded in the Switch file system. If the syslog server's IP address has been configured, the Switch will send a copy to the syslog server.

The log message file is limited in 4KB size. If the file is full, the oldest one will be replaced.

8.5.1. CLI Configuration

Node	Command	Description
enable	show syslog	The command displays the entire log message recorded in the Switch.
enable	show syslog level LEVEL	The command displays the log message with the LEVEL recorded in the Switch.
enable	show syslog server	The command displays the syslog server configurations.
configure	syslog (disable enable)	The command disables / enables the syslog function.
configure	syslog ip IPADDR	The command configures the syslog server's IP address.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#syslog-server ip 192.168.200.106
L2SWITCH(config)#syslog-server enable
```

8.5.2. Web Configuration

System Log

Syslog Server Setting

Server IP

System Log

Log Level

No data.

Parameter	Description
Server IP	Enter the Syslog server IP address in dotted decimal notation. For example, 192.168.1.1. Select Enable to activate switch sent log message to Syslog server when any new log message occurred.
Log Level	Select Alert/Critical/Error/Warning/Notice/Information to choose which log message to want see.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

8.6. User Account

The Switch allows users to create up to 6 user account. The user name and the password should be the combination of the digit or the alphabet. The last admin user account cannot be deleted. Users should input a valid user account to login the CLI or web management.

User Authority:

The Switch supports two types of the user account, admin and normal. The **default** users account is **username(admin) / password(admin)**.

- admin - read / write.
- normal - read only.
; Cannot enter the privileged mode in CLI.
; Cannot apply any configurations in web.

The Switch also supports backdoor user account. In case of that user forgot their user name or password, the Switch can generate a backdoor account with the system's MAC. Users can use the new user account to enter the Switch and then create a new user account.

Default Settings

- Maximum user account : 6.
- Maximum user name length : 32.
- Maximum password length : 32.
- Default user account for privileged mode : admin / admin.

Notices

- The Switch allows users to create up to 6 user account.
- The user name and the password should be the combination of the digit or the alphabet.
- The last admin user account cannot be deleted.
- The maximum length of the username and password is 32 characters.

8.6.1. CLI Configuration

Node	Command	Description
enable	show user account	This command displays the current user accounts.
configure	add user USER_ACCOUNT PASSWORD (normal admin)	This command adds a new user account.
configure	delete user USER_ACCOUNT	This command deletes a present user account.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#add user q q admin
L2SWITCH(config)#add user 1 1 normal
```

8.6.2. Web Configuration

User Account

User Account Settings

User Name

User Password

User Authority Normal ▼

User Account List

No.	Name	Authority	Action
1	admin	Admin	
2	q	Admin	<input type="button" value="Delete"/>

Parameter	Description
User Name	Type a new username or modify an existing one.
User Password	Type a new password or modify an existing one. Enter up to 32 alphanumeric or digit characters.
User Authority	Select with which group the user associates. admin (read and write) or normal (read only) for this user account.
Apply	Click Apply to add/modify the user account.
Refresh	Click Refresh to begin configuring this screen afresh.
User Account List	
No.	This field displays the index number of an entry.
User Name	This field displays the name of a user account.
User Password	This field displays the password.
User Authority	This field displays the associated group.
Action	Click the Delete button to remove the user account. Note: You cannot delete the last admin accounts.

Customer support

For all questions related to the MEN-5410 or any other Volktek product, please feel free to contact Volktek customer support:

Address	Volktek Customer Support 4F, 192 Liancheng Road, Zhonghe District, New Taipei City 23553, Taiwan
Phone	+886-2-8242-1000
Fax	+886-2-8242-3333
E-mail	<i>support@volktek.com.tw</i>
Website	www.volktek.com

ISO 9001 Certified

CONFIDENTIAL