VOLKTEK

User Manual

INS-8624P

4x 10/100/1000Base-T PoE+ & 2x Gigabit SFP
Managed Industrial PoE+ Ethernet Switch

Version-1.2 30th Dec 2024

VOLKTEK

COPYRIGHT

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.

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

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

Do not work on the system or connect or disconnect cables during periods of lightning activity.

Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Do not stack the chassis on any other equipment. If the chassis falls, it can cause severe bodily injury and equipment damage.

An exposed wire lead from a DC-input power source can conduct harmful levels of electricity. Be sure that no exposed portion of the DC-input power source wire extends from the terminal block plug.

Warning

Ethernet cables must be shielded when used in a central office environment.

Warı

If a redundant power system (RPS) is not connected to the switch, install an RPS connector cover on the back of the switch.

Warı

Warning

Read the wall-mounting instructions carefully before beginning installation. Failure to use the correct hardware or to follow the correct procedures could result in a hazardous situation to people and damage to the system.

Before performing any of the following procedures, ensure that power is removed from the DC circuit.

Warı

Read the installation instructions before connecting the system to the power source.

Warı

Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.

Warı

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Warı

Warning

When installing or replacing the unit, the ground connection must always be made first and disconnected last.

VOLKTEK

Warning

No user-serviceable parts inside. Do not open.

Warning

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

VOLKTEK

Table of Content

VOLKTEK

Revision History

Date	Version	Writer	Note
2017.01.21		Justin Sheu	Release!
2018.02.23		Justin Sheu	Release for D-Link firmware.

1. About this Manual

1.1. Welcome

The INS-8624P managed industrial switch is a Power Source Equipment (PSE) device engineered with rugged hardware to meet the high reliability requirements of Industrial or Outdoor PoE applications. Built in a well-protected IP-40 aluminum housing, the switch withstands in operating temperatures ranging from -40℃ to 75℃ and operates consistently even in harsh industrial environments. The INS-8624P supports QoS, IGMP snooping, SFP DDMI, PoE and other device management features to fulfill the needs of high performance managed Industrial networks.

PoE function on 4-10/100/1000Base-T copper ports of the INS-8624P complies with IEEE 802.3at standards and allows them to supply up to 30W per port for network attached powered devices such as WLAN Access Points, VoIP phones and IP surveillance cameras. Two gigabit fiber slots of the switch can be configured as dual fiber ring ports to quickly recover network failures and provide an easy way to establish redundant gigabit network. Thus, INS-8624P ensures a reliable and highly available managed industrial network while delivering all the benefits of PoE power.

1.2. Purpose

This manual discusses how to install and configure your Managed PoE Switch.

1.3. Terms/ Usage

In this manual, the term “Switch” (first letter upper case) refers to the INS-8624P Switch, and “switch” (first letter lower case) refers to other switches.

2. About the INS-8624P

2.1. Features

PoE function

Total PoE power budget control

Per port PoE function enable/disable

PoE Port power feeding priority

Per PoE port power limit

PD classification detection

PoE Schedule

PD Alive check

PD (reboot & Alarm)

Configuration

Command Line Interface

Telnet, Web GUI,

SNMP v1/v1c

Management VLAN

System log

Firmware Upgradable

Configuration Upload/Download

Dual Homing

VLAN

802.1Q Tag-based VLA N

MAC-based VLAN

256 Active VLAN

Traffic Control

IGMP snooping v1/v2/v3

802.1p Priority Queues per port

Rate Limitation

Storm Control

Port Isolation

Diagnostic

LED status

SNMP trap

SFP DDMI support

E-mail alarm

Port Mirroring

SNTP

Port Statistic

2.2. Specifications

IEEE Standards

IEEE 802.3	10Base-T
IEEE 802.3u	100Base-TX
EEE 802.3ab	1000Base-T
IEEE 802.3z	1000Base-SX/LX
IEEE 802.3x	Flow Control
IEEE 802.1p	Class of service
IEEE 802.1q	VLAN Tagging

IEEE 802.3af	Power over Ethernet
IEEE 802.3at	Power over Ethernet plus
IEEE 802.1ab	Link Layer Discovery Protocol
IEEE 802.3az	Energy Efficient Ethernet

Performance

Switching fabric	12Gbps
L2 forwarding	8.93Mpps
Packet buffer size	4.1Mbit
MAC table size	8k
Jumbo Frame Size	10k
Throughput	14,880 pps to 10 Mbps ports
	148,800 pps to 100 Mbps ports
	1,488,000 pps to 1000 Mbps ports

Physical ports

2 x Gigabit SFP

4 x 10/100/1000Base-T (PSE)

Maximum Distances

RJ-45	up to 100 m
SFP	up to 120 km

PoE

Power Available at PD	25.50 W
Max Power delivered by PSE	30 W
Voltage Range (at PSE)	50-57V
Voltage Range (at PD)	42.5-57V
Maximum Current	600 mA
Maximum Cable resistance	12.5 Ω (Category 5)

Per port up to 30 W and up to limited power budget

PoE output short circuit protection

PoE Power Budget: 120W

PoE supported mode: Mode A

Power

Input Voltage:

- Primary inputs : 48~57VDC
- Redundant inputs : 48~57VDC

Connection:

- One removable 6-pin terminal block
- One 48V DC power jack

Support Overload current protection

Support Power Reverse Polarity Protection

One relay output with current carrying capacity of 1 A @ 24V DC

ESD protection: 8KV/15KV (Contact/Air)

Surge protection: 6KV (Line to ground)

Power Consumption: 10W

Mechanical

Dimension (WxHxD)	50x150x120 mm (1.97x5.90x4.72 inch)
Housing	IP40 protection (Aluminum Case)
Weight	529g
Installation	DIN-Rail or Wall Mount

Operating Requirement

Wide Operating Temperature	-40 to 75℃
Storage Temperature	-40 to 85℃
Operating Humidity	10 to 95% RH (non-condensing)
Storage Humidity	5 to 95% RH (non-condensing)

3. Hardware Description

3.1. Connectors

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

3.1.1. 10/100/1000Base-T Ports

The 10/100/1000Base-T ports support network speeds of 10Mbps, 100Mbps or 1000Mbps, 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) 10Mbps – Cat 3 or better; (2) 100/1000Mbps – Cat 5e or better.

3.1.2. SFP Slots for SFP modules

The one SFP slots are designed to Gigabit SFP modules that support network speed of 1000Mbps.

3.2. 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.

3.2.1. Hardware Installation

- ✓ **Step 1**: Unpack the device and other contents of the package.
- ✓ **Step 2**: Fasten DIN-Rail or Wall-mount kit on the rear of the INS-8624P
- ✓ **Step 3:** Connect the 48~57V DC power supply to the PWR & RPS terminal block or 4-pin power adapter to DC jack receiver on the top of the Switch (Refer to "**Wiring Redundant Power Inputs**")
- ✓ **Step 4**: Connect the Ethernet (RJ-45) port to the networking device and check the LED status to confirm the connection is established.

3.2.2. DIN rail Installation

The INS-8624P has a DIN rail bracket on the back of the Switch to satisfy the mounting installation.

Location: The INS-8624P can be DIN-Rail-mounted in cabinet or enclosure.

Mounting the switch

Place the INS-8624P on the DIN rail from above using the slot. Push the front of the switch toward the mounting surface until it snaps into place with a click sound.

Dismounting the switch

Pull out the lower edge of the switch and then remove the switch from the DIN rail.

3.2.3. Wall mount Installation

Location: The INS-8624P can be placed on a horizontal surface through wall-mounted kit

Place the switch by using mounting holes on the wall at the appropriate place

3.2.4. Wiring Redundant Power Inputs

You can use either "DC-Jack" or "Terminal Block (PWR)" for primary power and "Terminal Block (RPS)" for secondary power source, to be a Redundant Power Input.
Top views of DC-Jack and Terminal Block are shown as pictures:

Redundant Power Input: Choose either "DC-Jack" or "Terminal Block (PWR)" as primary power. If you choose "Terminal Block (PWR)", please refer to option 1, unless follow option 2.

- ✓ **Option 1:** Insert the terminal block connector which includes "PWR" and "RPS" into the terminal block receptor.
- ✓ **Option 2:** Insert the "DC-Jack" connector into "DC-Jack" receiver and "Terminal Block (RPS)" into terminal block receptor.

Connect power cables to terminal block: *Use your finger to press the orange plug on top of terminal block connector to insert power cables*

3.2.5. Power On the Unit

The Switch accepts the power input voltage from 48~57V DC.

- ✓ Wiring appropriate power source as above guideline before turn on the power.
- ✓ 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.

Notice: Turn off the power before connecting modules or wires.

- *The correct power supply voltage is listed on the product label. Check the voltage of your power source to make sure that you are using the correct voltage. Do NOT use a voltage greater than what is specified on the product label.*
- *Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If current go above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.*

3.2.6. Hardware Reset

There has "Reset" function on the top of Switch, which can help to manually reboot or reload to factory default setting.

- ✓ If press "Reset" button **more** than 2 seconds, the Switch will be rebooted
- ✓ If press "Reset" button **more** than 5 seconds, the Switch will be reloaded to factory default setting

3.3. 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:

PWR (Green)	Illuminated	Power On by terminal block PWR/DC-Jack at 48VDC
	Off	Terminal block PWR/DC-Jack fails or is not available
RPS (Green)	Illuminated	Power On by terminal block RPS at 48VDC
	Off	Terminal block RPS fails or is not available
ALM (Red)	Illuminated	Power lost alarm
	Off	No power lost or DIP function is disabled
10/100/1000Mbps 1~4th (Green)	Illuminated	Copper port speeds at 1000Mbps
	Off	Copper port speeds at 10/100Mbps
LNK/ACT (Green)	Illuminated	Ethernet link-up
	Blinking	Activity (receiving or transmitting data)
	Off	Port disconnected or link failed
SFP slots (1000Mbps) 5~6th (Green)	Illuminated	Ethernet link-up
	Blinking	Activity (receiving or transmitting data)
	Off	Port disconnected or link failed
PoE (Green) 1~4th port	Illuminated	PoE power is delivered to the PD device
	Off	No outgoing PoE power

Notice:

- ✓ ***PWR****: Primary Power*
- ✓ ***RPS****: Redundant Power Supply*
- ✓ ***ALM****: Alarm*

4. System Status

4.1. Console Port (Onboard Pin header connector)

- Connect your computer to the console port on the Switch using the appropriate cable.
- Use terminal emulation software with the following settings:

Default Settings for the Console Port

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

- Press [ENTER] to open the login screen.

Setting	Default Value
Default Username	admin
Default Password	admin

4.2. Telnet

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

Default Management IP Address

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

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

4.3. 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

4.4. 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

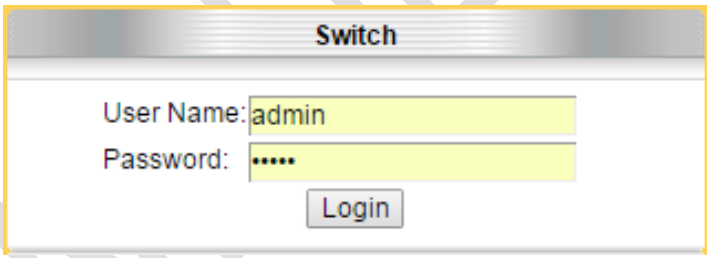
Its command prompt is "***L2SWITCH(config-if)#".***
It means these commands can be executed in this command prompt.
In ***Configure*** code, executing command "***interface gigaethernet1/0/5***" enter the interface port 5 node.
Or
In ***Configure*** code, executing command "***interface fastethernet1/0/5***" enter the interface port 5 node.
Note: depend on your port speed, gigaethernet1/0/5 for gigabit Ethernet ports and fastethernet1/0/5 for fast Ethernet ports.

L2SWITCH(config)#interface gigaethernet1/0/5
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)#

4.5. GUI Login



Parameter	Description
User ID	Enter the user name.
Password	Enter the password.

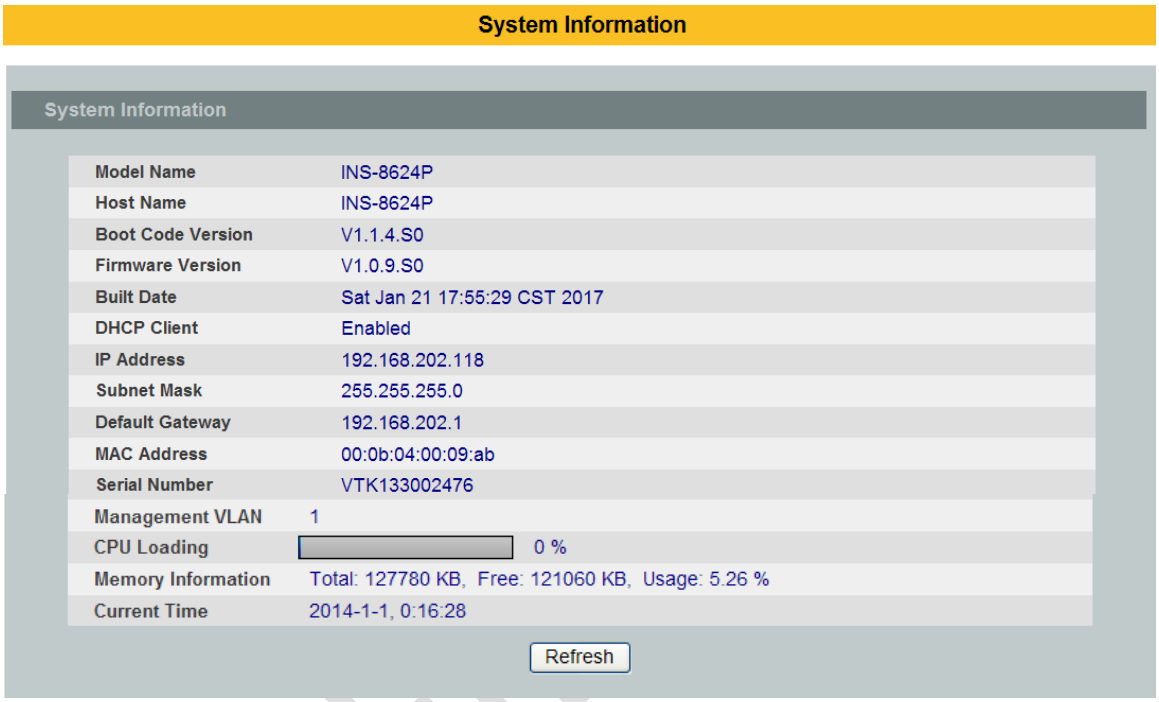
Default:
User name: admin
Password: admin

4.6. 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.

4.7. System Information



Parameter	Description
Model Name	This field displays the model name of the Switch.
Host name	This field displays the name of the Switch.
Boot Code Version	This field displays the boot code version.
Firmware Version	This field displays the firmware version.
Built Date	This field displays the built date of the firmware.
DHCP Client	This field displays whether the DHCP client is enabled on the Switch.
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 assigned by manufacture for identification of the 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.

5. Basic Settings

5.1. General Settings

5.1.1. System

5.1.1.1. Introduction

Management VLAN

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.

5.1.1.2. CLI Configuration

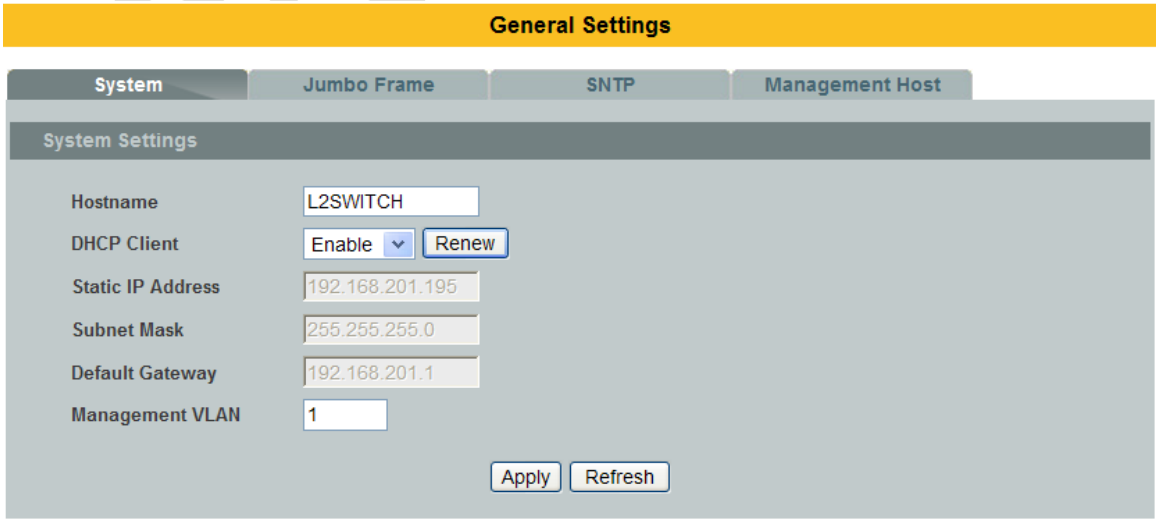
Node	Command	Description
enable	ping IPADDR [–c COUNT]	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4.
enable	ping IPADDR [–s SIZE]	This command sends an echo request to the destination host. The –s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
enable	ping IPADDR [–c COUNT –s SIZE]	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4. The –s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
enable	ping IPADDR [-s SIZE –c COUNT]	This command sends an echo request to the destination host. The –c parameter allow user to specific the packet count. The default count is 4. The –s parameter allow user to specific the packet size. Valid range: 0 ~ 1047 bytes.
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.
configure	configure terminal	This command changes the mode to config

		mode.
configure	interface eth0	This command changes the mode to eth0 mode.
eth0	show	This command displays the eth0 configurations.
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 VLANID	This command configures the management vlan.

The procedures to configure an IP address for the Switch.

- ✓ To enter the configure node.
  L2SWITCH#configure terminal
  L2SWITCH(config)#
- ✓ To enter the ETH0 interface node.
  L2SWITCH(config)#interface eth0
  L2SWITCH(config-if)#
- ✓ To get an IP address from a DHCP server.
  L2SWITCH(config-if)#ip dhcp client enable
- ✓ To configure a static IP address for the Switch.
  L2SWITCH(config-if)#ip address 192.168.202.111/24

5.1.1.3. Web Configuration



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 this button to take effect the settings.
Refresh	Click this button to reset the fields to the last setting.

5.1.2. Jumbo Frame

5.1.2.1. Introduction

Jumbo frames are Ethernet frames with a payload greater than 1500 bytes. Jumbo frames can enhance data transmission efficiency in a network. The bigger the frame size, the better the performance.

Notice:

The jumbo frame settings will apply to all ports.

If the size of a packet exceeds the jumbo frame size, the packet will be dropped.

The available values are 10240, 9216, 1522, 1536, 1552.

Default Setting: The default jumbo frame is 10240 bytes.

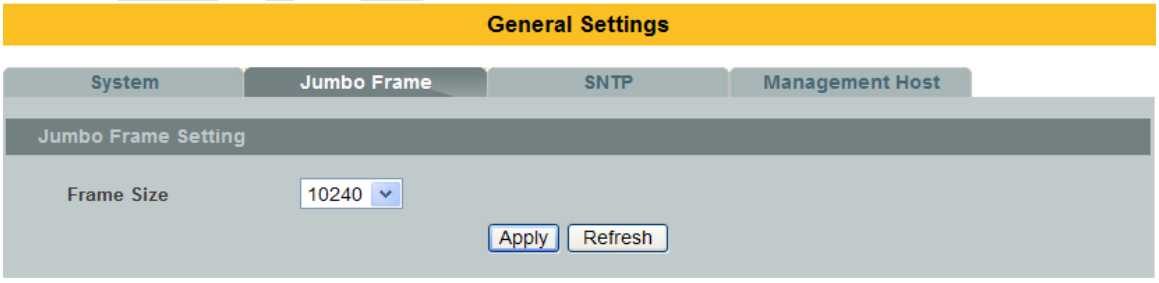
5.1.2.2. CLI Configuration

Node	Command	Description
enable	show jumboframe	This command displays the current jumbo frame settings.
configure	jumboframe (10240|9216|1522|1536|1552)	This command configures the maximum number of bytes of frame size.

The procedures to configure the Jumbo frame size.

- ✓ To enter the configure node.
  L2SWITCH#configure terminal
  L2SWITCH(config)#
- ✓ To configure 9216 as the jumbo frame size for all ports.
  L2SWITCH(config)#jumboframe 9216

5.1.2.3. Web Configuration



Parameter	Description
Frame Size	This field configures the maximum number of bytes of frame size.
Apply	Click this button to take effect the settings.
Refresh	Click this button to reset the fields to the last setting.

5.1.3. SNTP

5.1.3.1. Introduction

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 10 seconds forever.
5. If the Switch has received SNTP reply, the Switch will re-get the time from NTP server every 24 hours.
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.

5.1.3.2. CLI Configuration

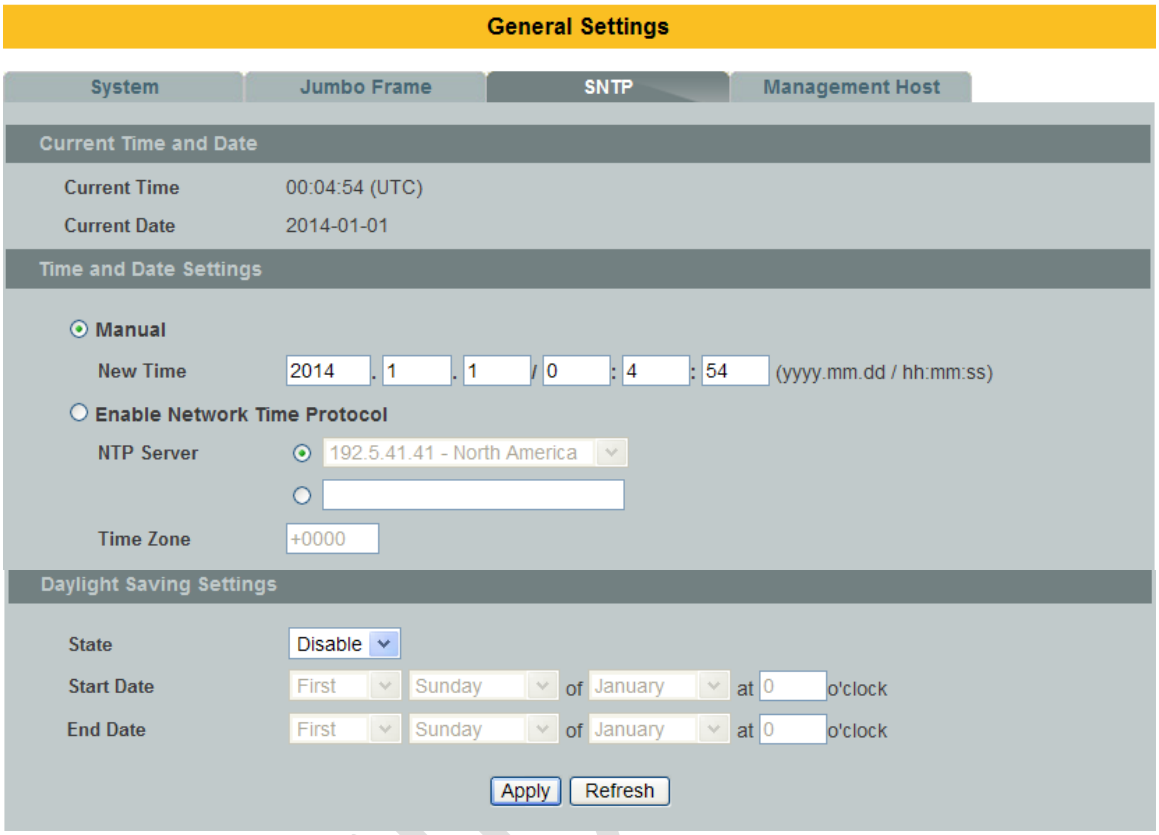
Node	Command	Description

enable	show time	This command displays current time and time configurations.
configure	time HOUR:MINUTE:SECOND	Sets the current time on the Switch. *hour*: 0-23 *min*: 0-59 *sec*: 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. *year*: 1970- *month*: 1-12 *day*: 1-31
configure	time daylight-saving-time	This command enables the daylight saving time.
configure	no time daylight-saving-time	This command disables daylight saving on the Switch.
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	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 +800
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

5.1.3.3. Web Configuration



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	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: 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**. 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).
End Date	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving Time. The time field uses the 24 hour format. Here are a couple of examples: 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**. 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).
Apply	Click this button to take effect the settings.
Refresh	Click this button to reset the fields to the last setting.

5.1.4. 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 10 entries.

Default Settings

This feature allows user to configure management host up to 10 entries.
The default is none, any host can manage the Switch via telnet or web browser.

5.1.4.1. CLI Configuration

Node	Command	Description
enable	show interface eth0	The command displays the all of the interface *eth0* configurations.
eth0	show	The command displays the all of the interface *eth0* configurations.
eth0	management host A.B.C.D	The command adds a management host address.
eth0	management subnet-host A.B.C.D/M	The command adds a management host address with a subnet mask. Which allows user to specify a range of hosts.
eth0	no management host A.B.C.D	The command deletes a management host address.

Example: The procedures to configure management host.

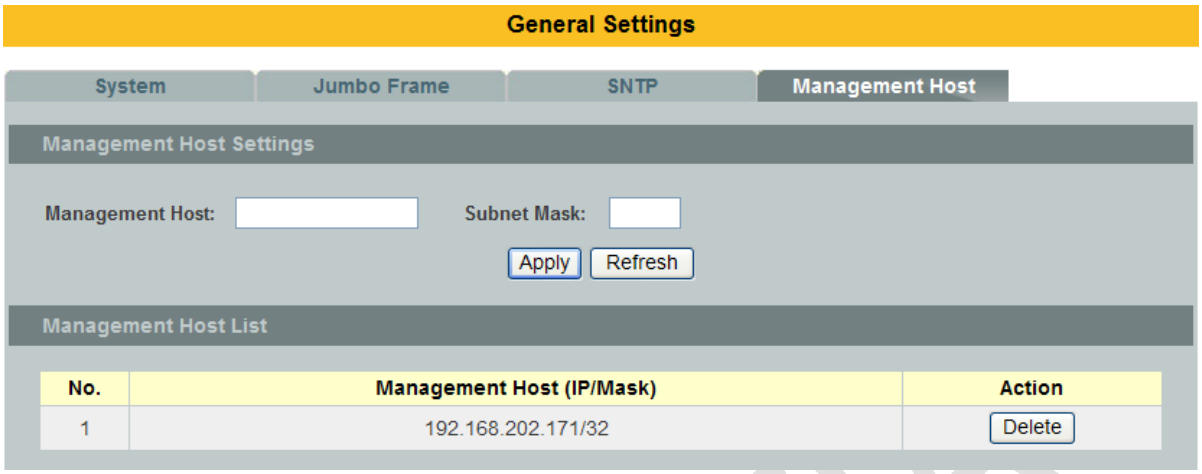
- ✓ To enter the configure node.
  L2SWITCH#configure terminal

- ✓ To enter the interface ETH0 node.
  L2SWITCH#interface eth0

- ✓ To configure a management host.
  L2SWITCH(config-if)#management host 192.168.200.106

- ✓ To remove a management host.
  L2SWITCH(config-if)#no management host 192.168.200.106

5.1.4.2. Web Configuration



Parameter	Description
Management Host	This field configures the management host.
Subnet Mask	This field configures the number of mask bit which allows to configure a range of hosts. If you do not specify value, the system will give 32 for the host automatically.
Apply	Click this button to take effect the settings.
Refresh	Click this button to begin configuring this screen afresh.
Management Host List	
No.	This field displays a sequential number for each management host.
Management Host	This field displays the management host and number of mask bit.
Action	Click the Delete button to remove the specified entry.

5.2. MAC Management

5.2.1. Introduction

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.

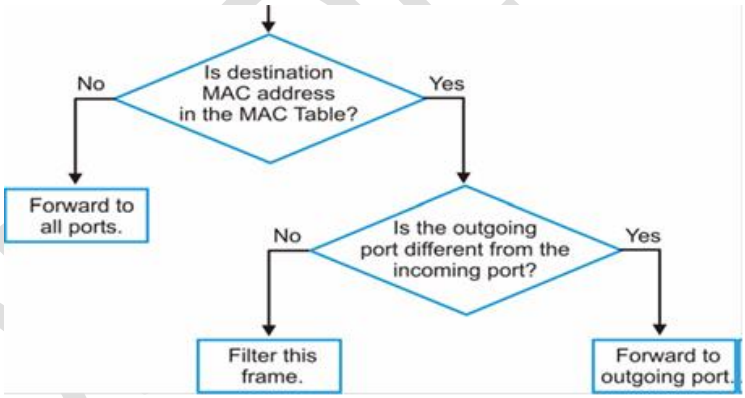


Figure MAC Table Flowchart

Default Settings

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

5.2.2. 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	This command displays information of a

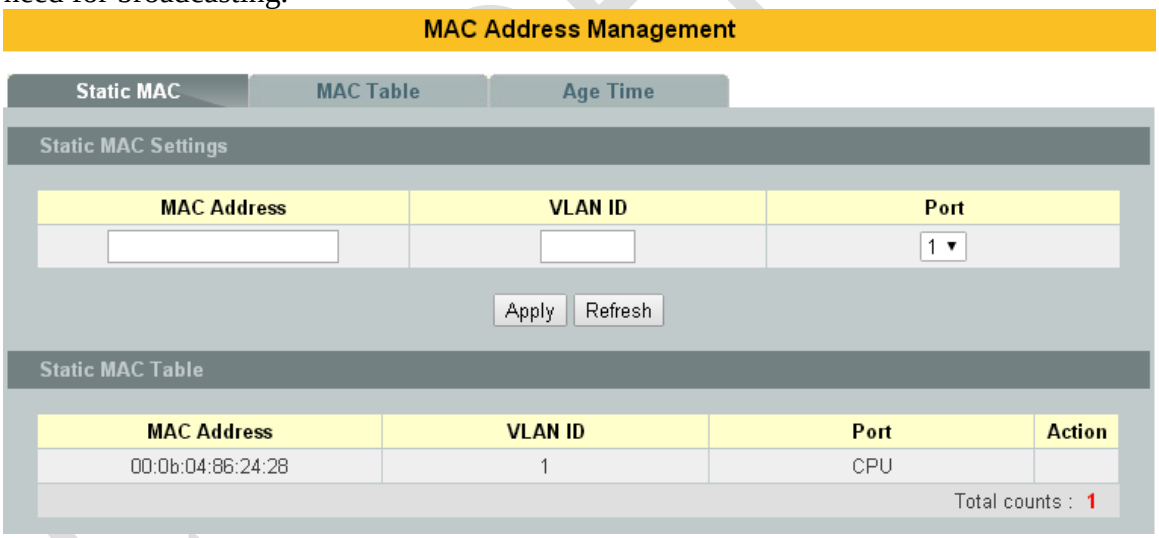
	mac MACADDR	specific MAC.
enable	show mac-address-table port PORT_ID	This command displays the current unicast address entries learnt by the specific port.
configure	mac-address-table static MACADDR vlan <1-4094> port PORT_ID	This command configures a static unicast entry.
configure	no mac-address-table static MACADDR vlan <1-4094>	This command removes a static unicast entry from the address table.
configure	clear mac address-table dynamic	This command clears the dynamic address entries.

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

5.2.3. Web Configuration

Static MAC

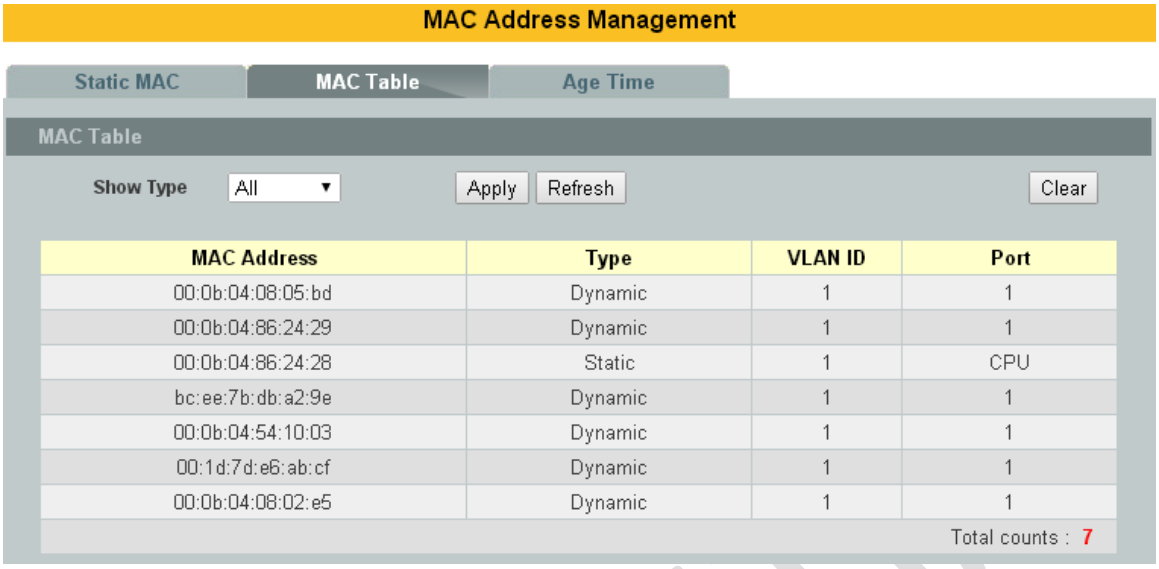
A static Media Access Control (MAC) address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.



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.

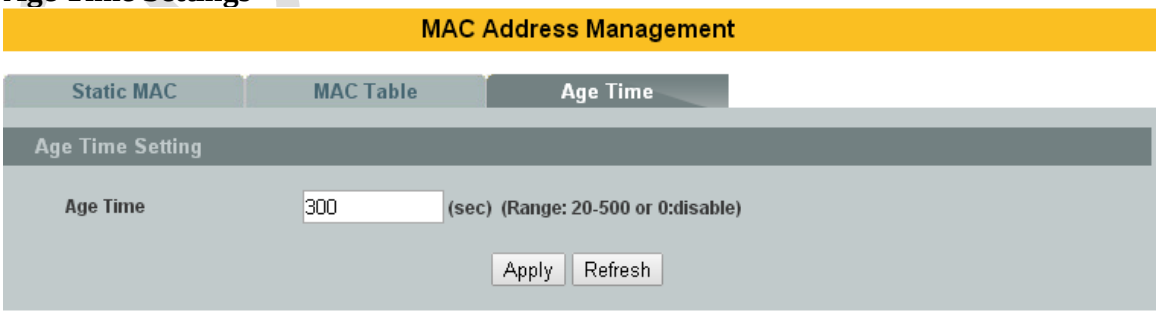
Refresh	Click Refresh to begin configuring this screen afresh.
Static MAC Table	
MAC Address	This field displays the MAC address of a manually entered MAC address entry.
VLAN ID	This field displays the VID of a manually entered MAC address entry.
Port	This field displays the port number of a manually 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



Parameter	Description
Show Type Apply	Select **All, Static**, **Dynamic, Port or MAC** 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



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.

5.3. Port Mirror

5.3.1. Introduction

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

5.3.2. CLI Configuration

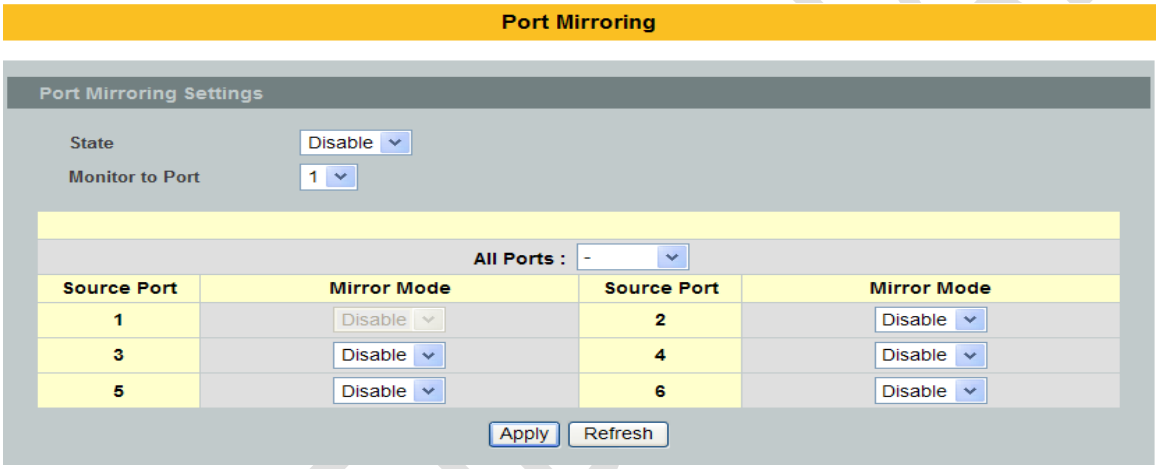
Node	Command	Description
enable	show mirror	This command displays the current port mirroring configurations.
configure	mirror (disable|enable)	This command disables / enables the port mirroring on the switch.
configure	mirror destination port PORT_ID	This command specifies the **monitor port** for the 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 mode both

5.3.3. Web Configuration



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

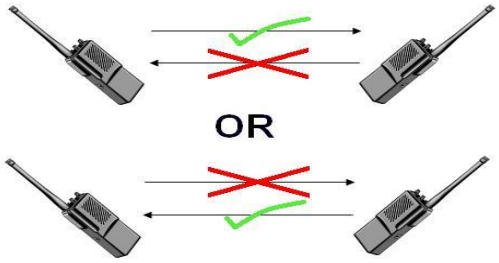
5.4. Port Settings

5.4.1. Introduction

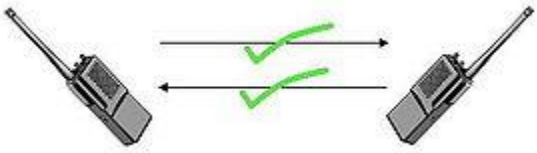
- Duplex mode

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 in 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 and 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.
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.

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.

- Cable Test.

This feature determines the quality of the cables, shorts, and cable impedance mismatch, bad connectors, termination mismatch, and bad magnetics. The feature can work on the copper Ethernet cable only.

Default Settings

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

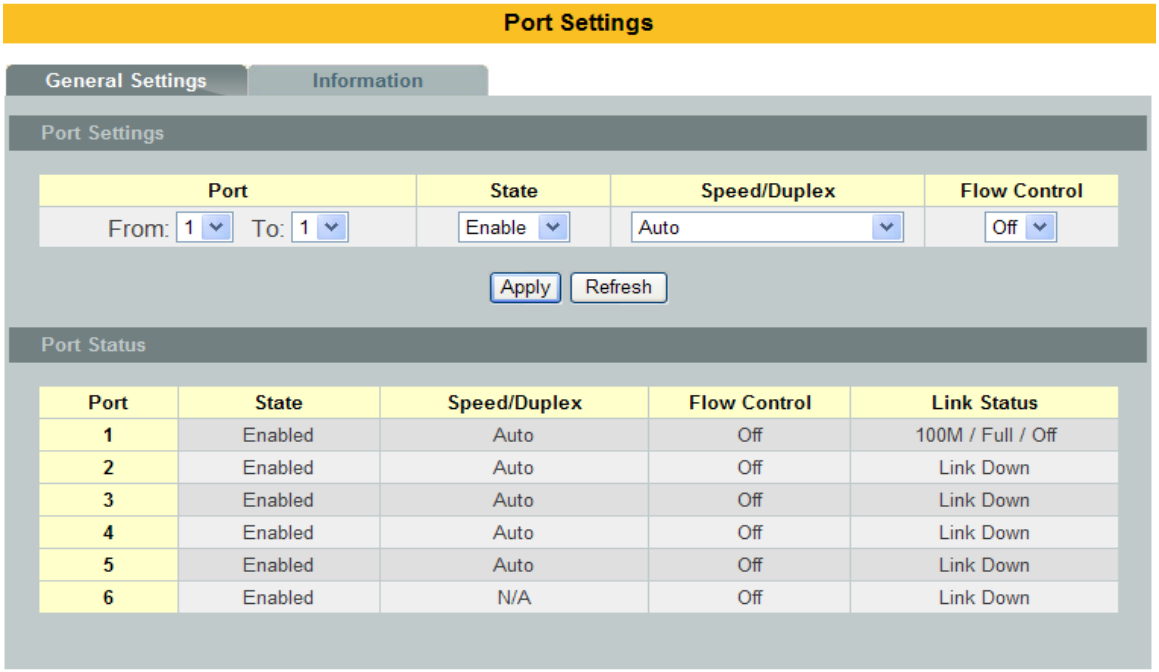
Note: 1000 Base-T doesn't support force mode.

5.4.2. CLI Configuration

Node	Command	Description
enable	show interface IFNAME	This command displays the current port configurations.
configure	interface IFNAME	This command enters the interface configure node.
interface	show	This command displays the current port configurations.
interface	loopback (none | mac)	This command tests 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-full-n | 10-half | 100-full | 100-full–n | 100-half | 1000-full | 1000-full-n)	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	description STRING	This command configures a description for the specific port.
interface	no description	This command configures the default port description.
interface	cable-test start	This command starts to diagnostics the Ethernet cable.
interface	show cable-test result	This command displays the test result of the Ethernet cable test.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	description STRINGs	This command configures a description for the specific ports.
if-range	no description	This command configures the default port description for the specific ports.
if-range	shutdown	This command disables the specific ports.
if-range	no shutdown	This command enables the specific ports.
if-range	speed (auto | 10-full | 10-full-n | 10-half | 100-full | 100-full–n | 100-half | 1000-full | 1000-full-n)	This command configures the speed and duplex for the port.

5.4.3. Web Configuration

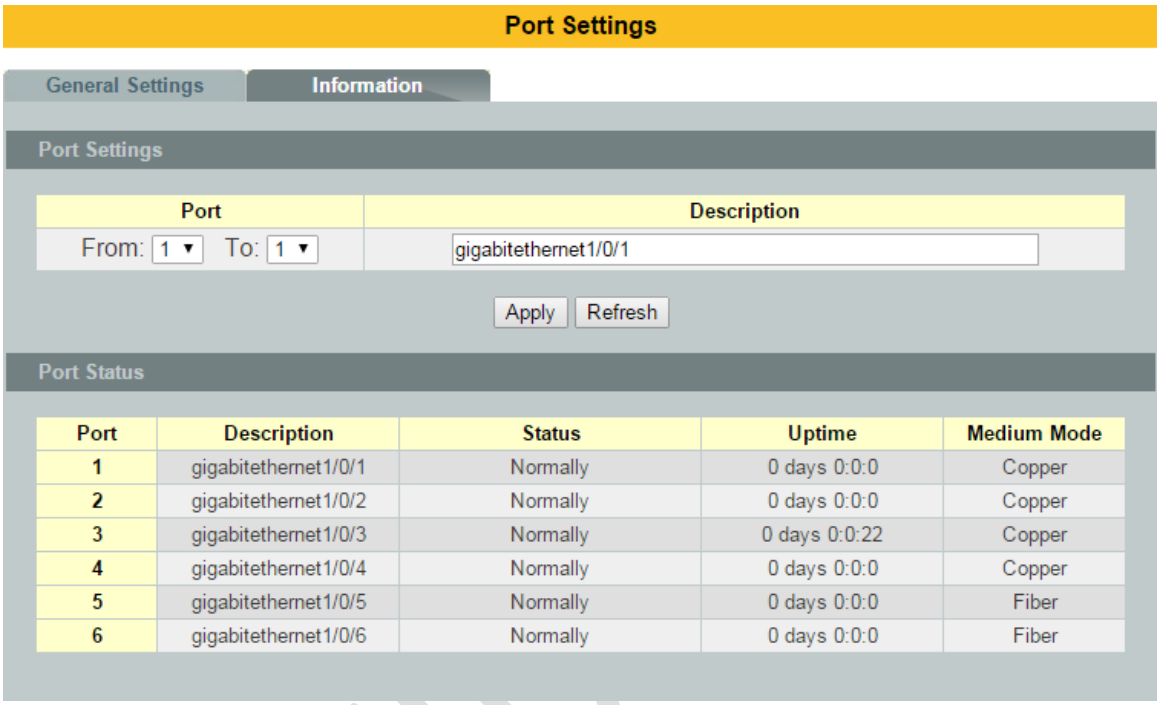
General Settings:



Parameter	Description
Port	Select a port or a range ports 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: • Auto • 10 Mbps / Full • • 10 Mbps / Half • 100 Mbps / Full • • 100 Mbps / Half • 1000 Mbps / Full
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.

Information:



Parameter	**Description**
Port	Select a port or a range ports you want to configure on this screen.
Description	Configures a meaningful name for the port(s).
Port Status	
Port	This field displays the port number.
Description	The meaningful name for the port.
Status	The field displays the detail port status if the port is blocked by some protocol.
Uptime	The sustained time from last link up.
Medium Mode	The current working medium mode, copper or fiber, for the port.

6. Advanced Settings

6.1. Bandwidth Control

6.1.1. QoS

6.1.1.1. Introduction

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, <100ms latency
5	5	Video, < 10ms latency
6	6	Internetwork 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.

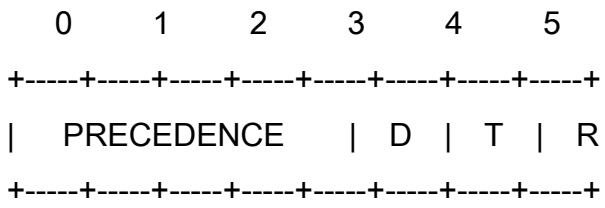
<table>
<tr><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td>Time to Live</td><td colspan="2">Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="4">Options</td><td>Padding</td></tr>
</table>

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 Fair Queuing** (**WFQ**)
  WFQ is a data packet scheduling technique allowing different scheduling priorities to statistically multiplexed data flows. It provides traffic priority management that automatically sorts among individual traffic streams without requiring an access list. WFQ decides which queue is selected in one slot time to guarantee the minimal packet rate of one queue. Thus, WFQ allows Internet operators to define traffic classes and then assign different bandwidth proportions.

- **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 mappings of the Priority to Queue are:

PRIO 0 ==> COSQ 1
PRIO 1 ==> COSQ 0
PRIO 2 ==> COSQ 2

PRIO 3 ==> COSQ 3
PRIO 4 ==> COSQ 4
PRIO 5 ==> COSQ 5
PRIO 6 ==> COSQ 6
PRIO 7 ==> COSQ 7

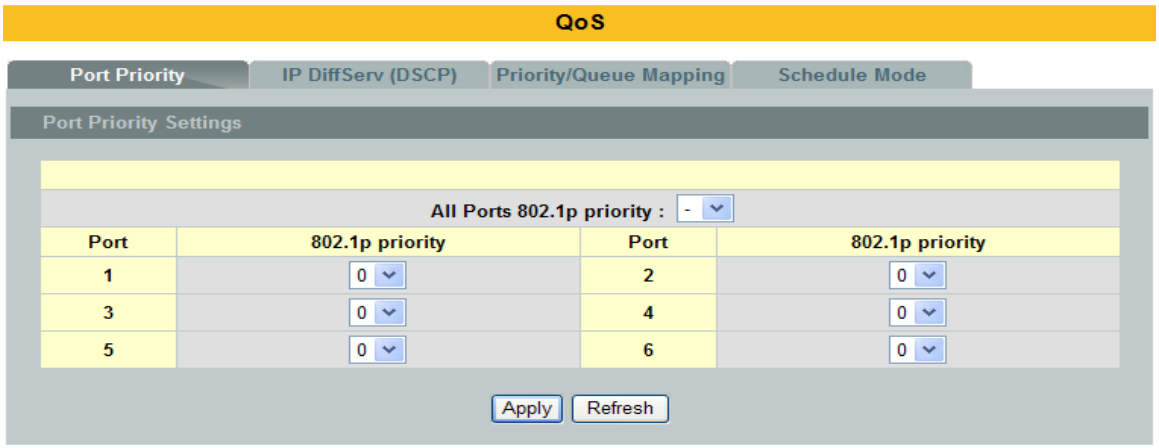
The DiffServ is disabled on the switch.

6.1.1.2. 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 <0-7> 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 wrr-queue weights <1-127> <1-127> <1-127> <1-127> <1-127> <1-127> <1-127> <1-127>	This command configures the QoS scheduling mode to Weighted Round Robin.
configure	qos mode wfr-queue weights <1-127> <1-127> <1-127> <1-127> <1-127> <1-127> <1-127> <1-127>	This command configures the QoS scheduling mode to Weighted fair scheduling.
interface	default-priority <0-7>	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).
enable	show diffserv	This command displays DiffServ configurations.
configure	diffserv (disable|enable)	This command disables / enables the DiffServ function.
configure	diffserv dscp <0-63> priority <0-7>	This command sets the DSCP-to-IEEE 802.1q mappings.

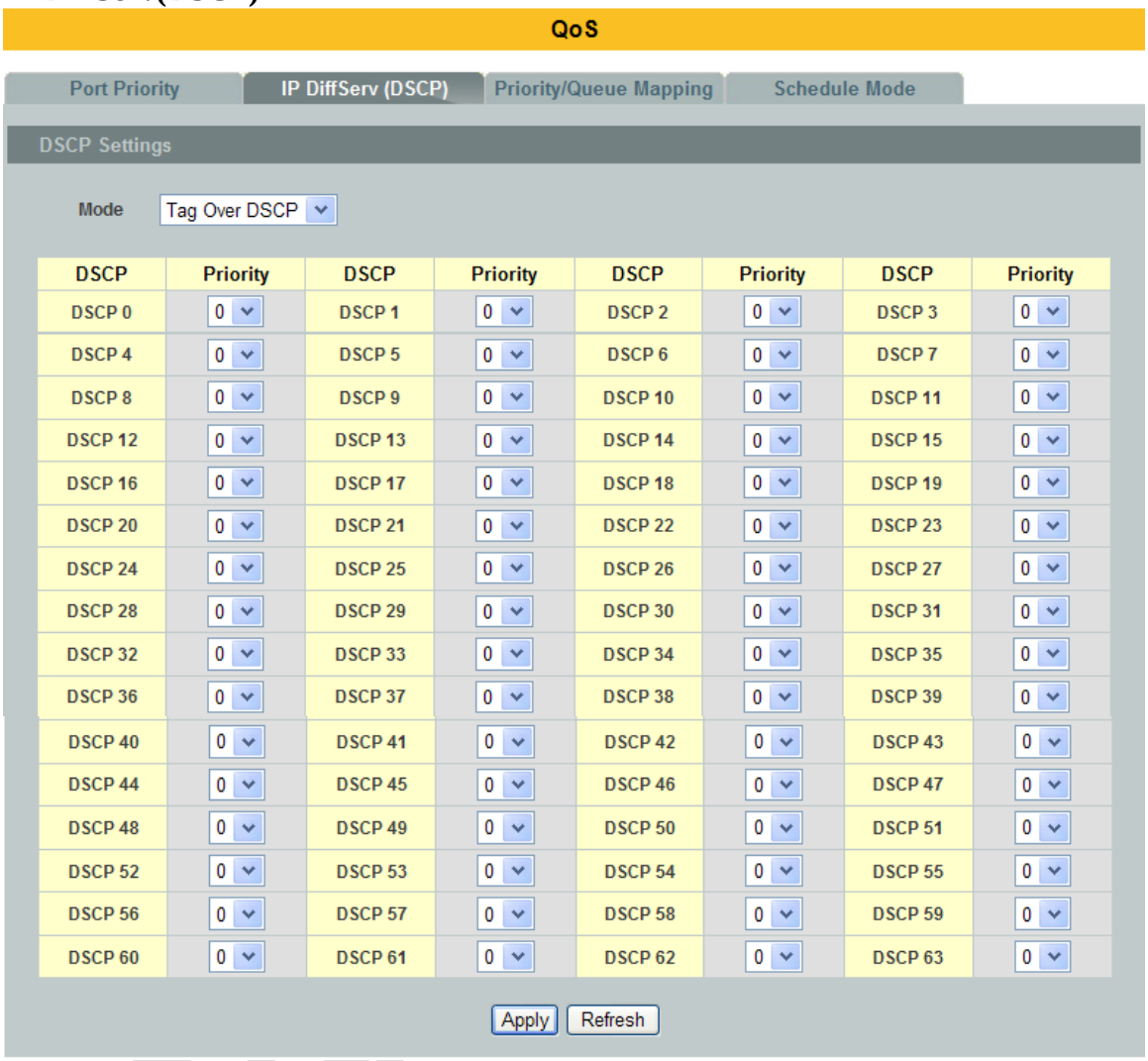
6.1.1.3. Web Configuration

Port Priority



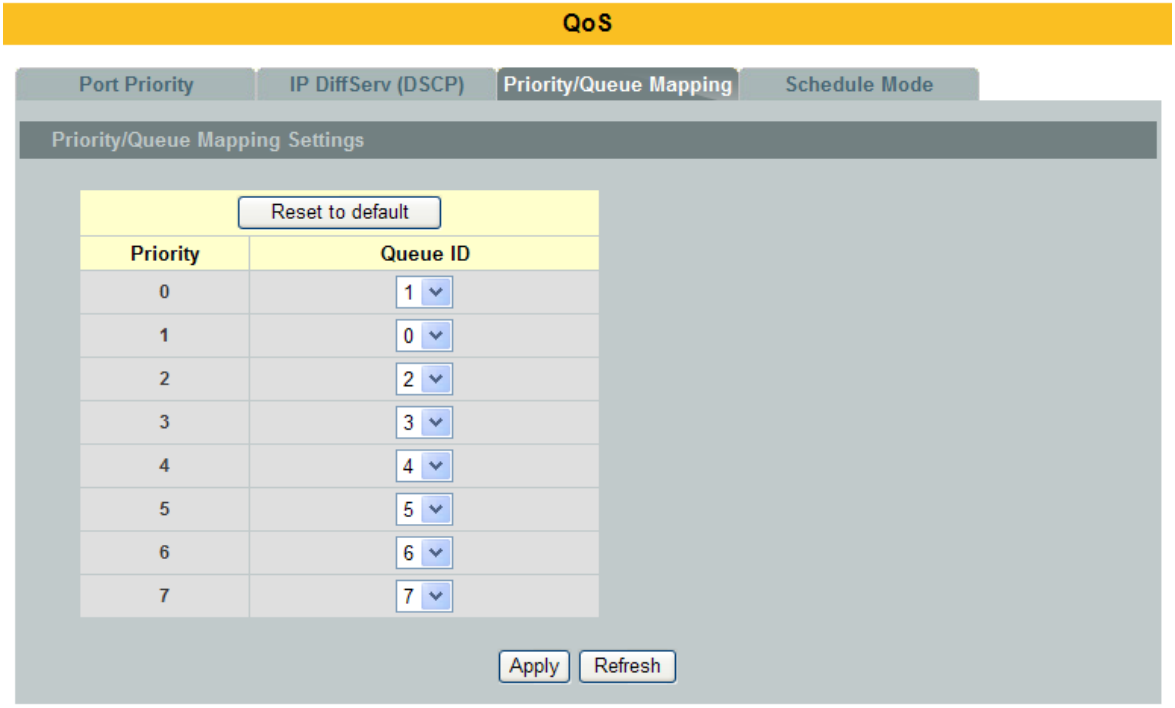
Parameter	Description
All Ports 802.1p priority	Use this field to set a priority for all ports. The value indicates packet priority and is added to the priority tag field of incoming packets. The values range from 0 (lowest priority) to 7 (highest priority).
Port	This field displays the number of a port.
802.1p Priority	Select a priority for packets received by the port. Only packets without 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)



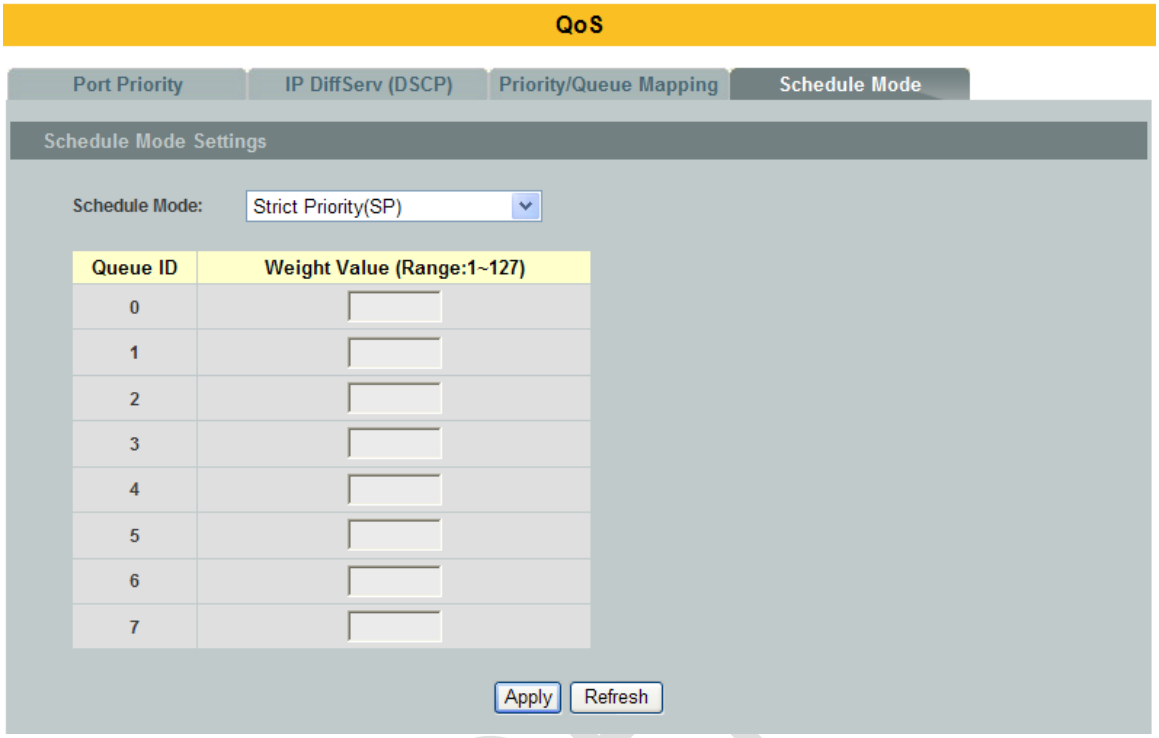
Parameter	Description
Mode	“Tag Over DSCP” or “DSCP Over Tag”. “Tag Over DSCP” means the 802.1p tag has higher priority than DSCP.
Priority	This field displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority).
Apply	Click Apply to take effect the settings.
Refresh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

Priority/Queue Mapping



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



Parameter	Description
Schedule Mode	Select **Strict Priority** (SP) or **Weighted Round Robin** (**WRR**) or **Weighted Fair Queuing** (**WFQ**). Note: Queue weights can only be changed when **Weighted Round Robin** is selected. **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.
Queue ID	This field indicates which Queue (0 to 7) you are configuring. Queue 0 has the lowest priority and Queue 7 the highest priority.
Weight Value	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. 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**.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

6.1.2. Rate Limitation

6.1.2.1. Storm Control

6.1.2.1.1. Introduction

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 : pps.

Default Settings

Broadcast Storm Control : 300pps.
Multicast Storm Control : None.
DLF Storm Control : 300pps.

6.1.2.1.2. CLI Configuration

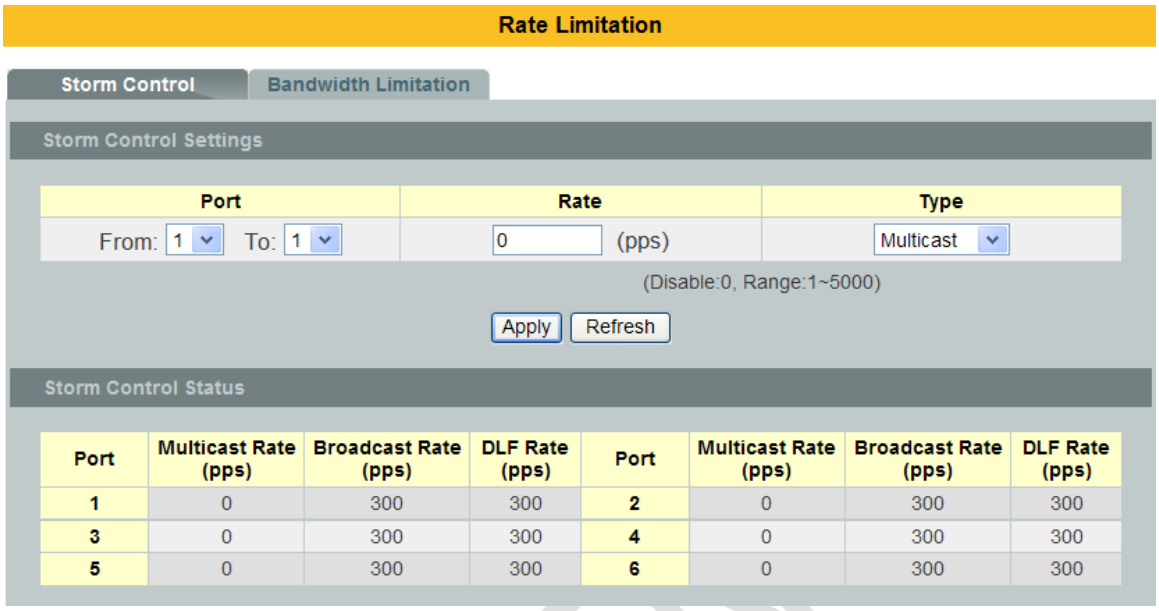
Node	Command	Description
enable	show storm-control	This command displays the current storm control configurations.
configure	storm-control rate RATE_LIMIT type (bcast | mcast | DLF | bcast+mcast | bcast+DLF | mcast+DLF | bcast+mcast+DLF) ports PORTLISTS	This command enables the bandwidth limit for broadcast 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 1-4
L2SWITCH(config)#storm-control rate 1 type multicast ports 1-4
```

L2SWITCH(config)#storm-control rate 1 type DLF ports 1-4

6.1.2.1.3. Web Configuration



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.

6.1.2.2. Bandwidth Limitation

6.1.2.2.1. Introduction

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

Rate Limitation unit: 16Kbs.
Default Setting: All ports' Ingress and Egress rate limitation are disabled.

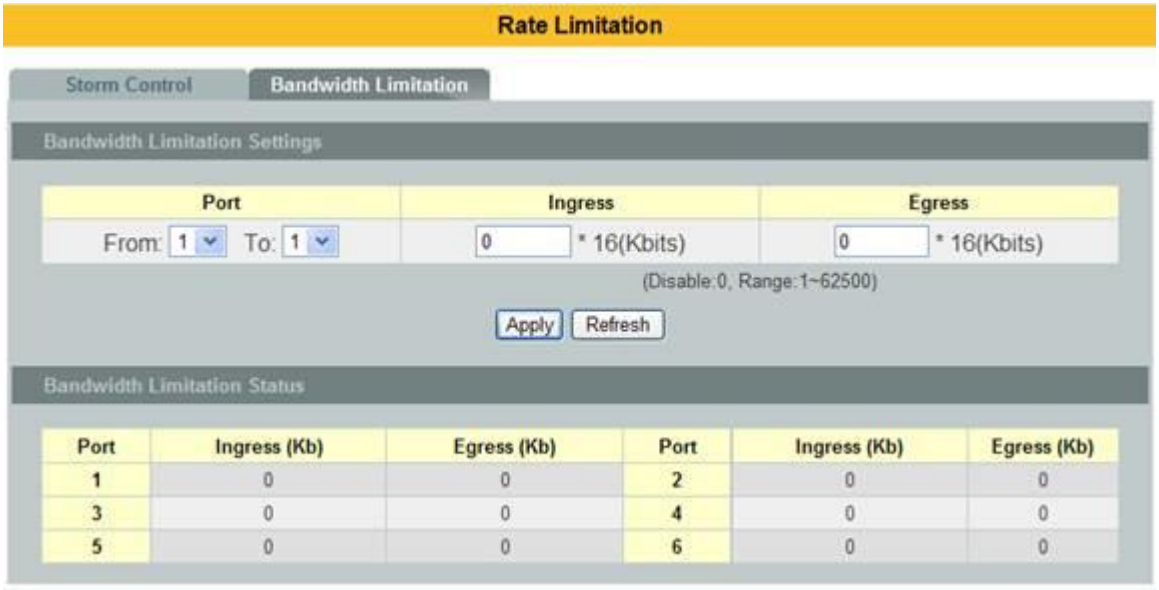
6.1.2.2.2. CLI Configuration

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 1-4
L2SWITCH(config)#bandwidth-limit ingress 1 ports 1-4
```

6.1.2.2.3. Web Configuration



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.

6.2. IGMP Snooping

6.2.1. IGMP Snooping

6.2.1.1. Introduction

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.

6.2.1.2. CLI Configuration

Node	Command	Description
enable	show igmp-snooping	This command displays the current IGMP snooping configurations.
enable	show igmp-snooping querier	This command displays the current IGMP Queriers and the querier configurations.
enable	show igmp-counters (port|vlan)	This command displays the current IGMP snooping counters per port or per vlan.
enable	show multicast	This command displays the multicast group in IP format.
configure	clear igmp-snooping counters	This command clears all of the IGMP snooping counters.
configure	igmp-snooping (disable | enable)	This command disables / enables the IGMP snooping on the switch.
configure	igmp-snooping vlan VLANLISTS	This command enables the IGMP snooping function on a VLAN or range of VLANs.
configure	no igmp-snooping vlan VLANLISTS	This command disables the IGMP snooping 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. *drop:* Drop all of the unknown multicast packets.
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 port.
interface	no igmp-immediate-leave	This command disables the IGMP Snooping immediate leave function for the specific port.
interface	igmp-snooping group-limit VALUE	This command configures the maximum groups for the specific port.
interface	no igmp-snooping group-limit	This command removes the limitation of the maximum groups for the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	igmp-immediate-leave	This command enables the IGMP Snooping immediate leave function for the specific ports.
if-range	no igmp-immediate-leave	This command disables the IGMP Snooping immediate leave function for the specific ports.

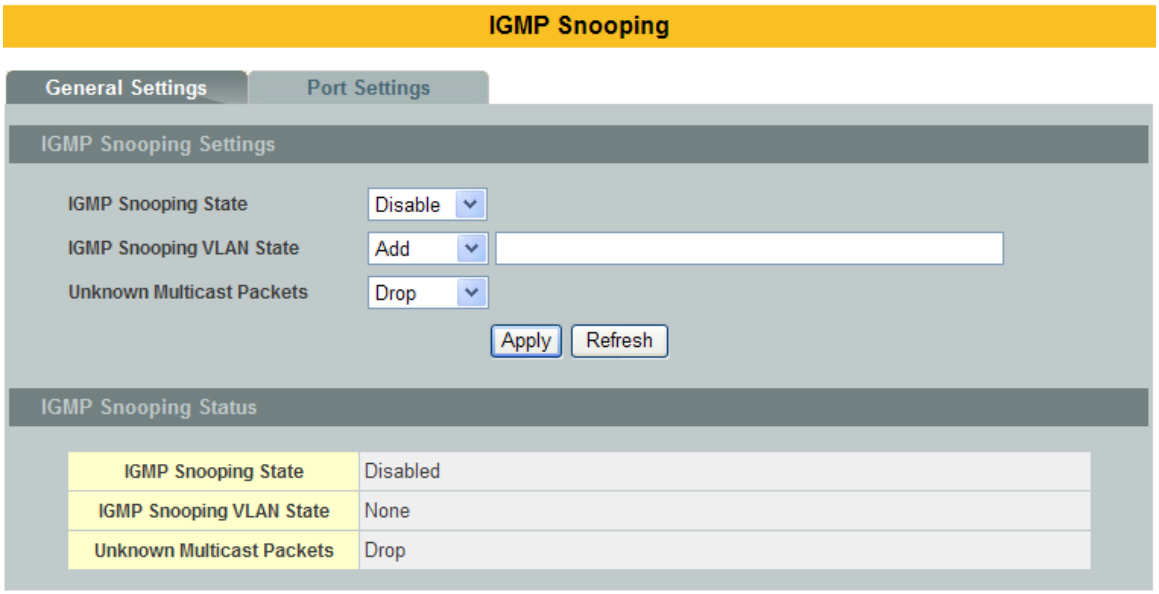
if-range	igmp-snooping group-limit VALUE	This command configures the maximum groups for the specific ports.
if-range	no igmp-snooping group-limit	This command removes the limitation of the maximum groups for the specific ports.
if-range	igmp-querier-mode (auto|fixed|edge)	This command specifies whether or not and under what conditions the ports 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)

Example:

L2SWITCH(config)#*igmp-snooping enable*
L2SWITCH(config)#*igmp-snooping vlan 1*
L2SWITCH(config)#*interface 1/0/1*
L2SWITCH(config-if)#*igmp-immediate-leave*
L2SWITCH(config-if)#igmp-querier-mode fixed
L2SWITCH(config-if)#igmp-snooping group-limit 20

6.2.1.3. Web Configuration

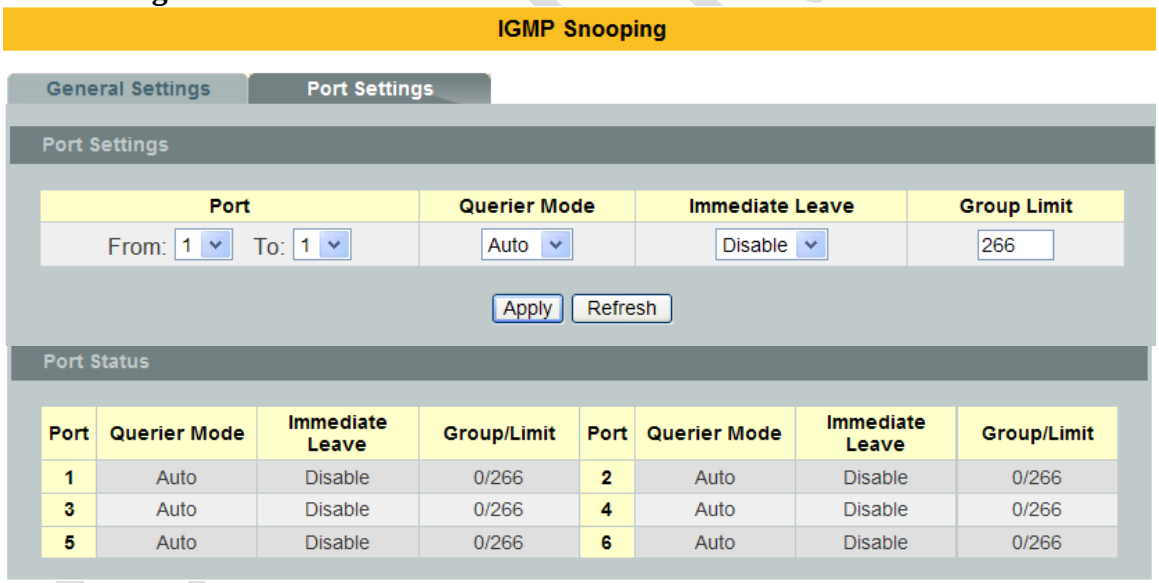
General Settings



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.
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 setting.
IGMP Snooping State	This field displays whether IGMP snooping is globally 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



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.

6.2.2. Multicast Address

6.2.2.1. Introduction

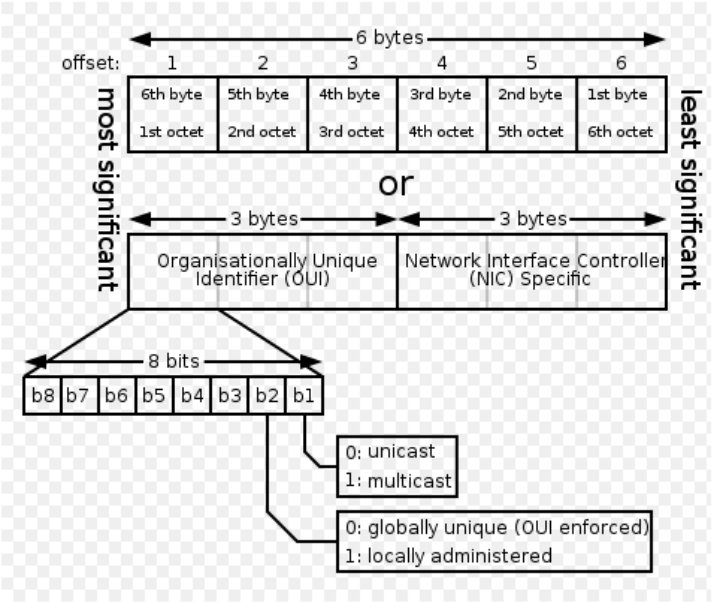
A multicast address is associated with a group of interested receivers. According to RFC 3171, addresses 224.0.0.0 to 239.255.255.255, the former Class D addresses, are designated as multicast addresses in IPv4.

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.



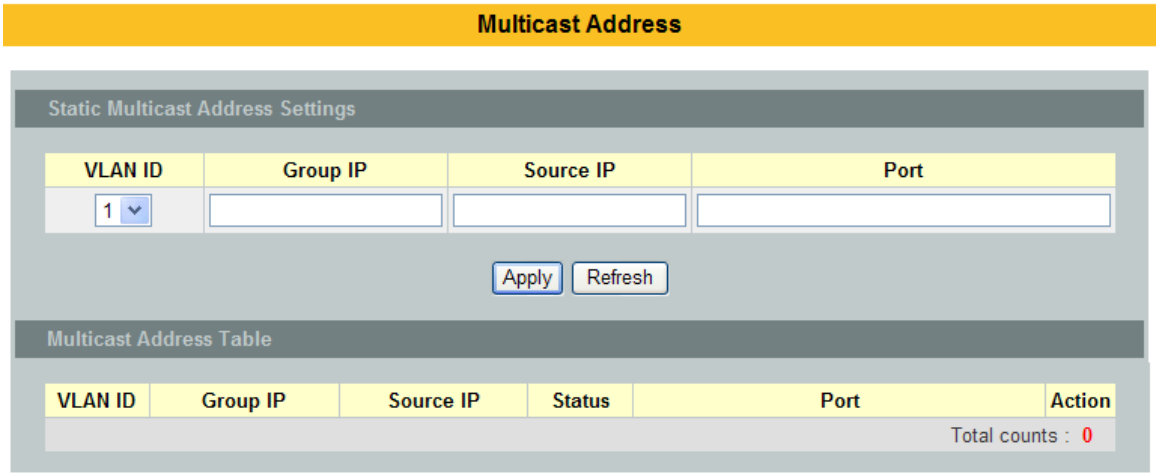
IP multicast address	Description
224.0.0.0	Base address (reserved)
224.0.0.1	The All Hosts multicast group that contains all systems on the same network segment
224.0.0.2	The All Routers multicast group that contains all routers on the same network segment
224.0.0.5	The Open Shortest Path First (OSPF) 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 RIP 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

6.2.2.2. CLI Configuration

Node	Command	Description
enable	show mac-address-table multicast	This command displays the current static/dynamic multicast address entries.
enable	show mac-address-table multicast vlan <1-4094>	This command displays the current static/dynamic multicast address entries with a specific vlan.
configure	mac-address-table multicast MACADDR vlan <1-4094> 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.

6.2.2.3. Web Configuration



Parameter	Description
VLAN ID	Configures the VLAN that you want to configure.
Group IP	Configures the multicast group IP.
Source IP	Configures the multicast server IP.
Port	Configures the member port for the multicast group.

Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
Multicast Address Table	
VLAN ID	The VLAN ID for the multicast group.
Group IP	The multicast group IP.
Source IP	The multicast server IP.
Status	The status of the multicast group.
Port	The member ports for the multicast group.
Action	Click the Delete button to delete this multicast group.

6.3. VLAN

6.3.1. Port Isolation

6.3.1.1. Introduction

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).

Port	Egress Port 0 1 2 3 4 5 6	Port	Egress Port 0 1 2 3 4 5 6
1	VVVVVVV	2	VVVVVVV
3	VVVVVVV	4	VVVVVVV
5	VVVVVVV	6	VVVVVVV

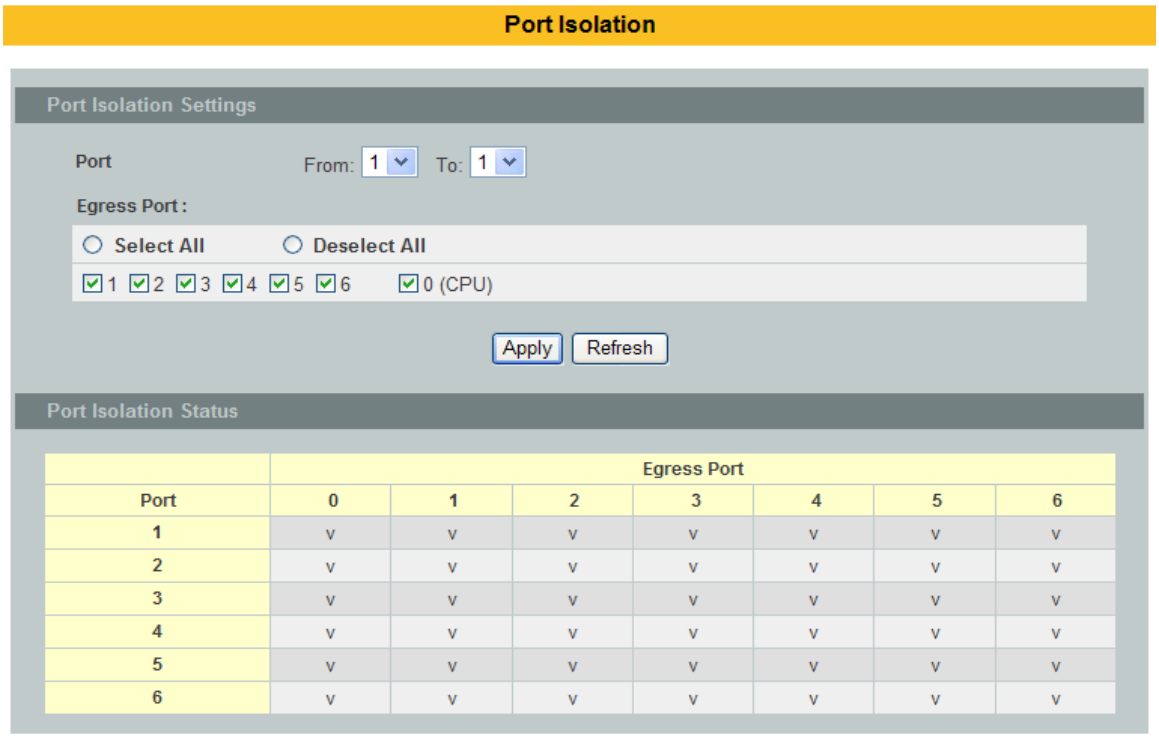
6.3.1.2. CLI Configuration

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 1-3
```

6.3.1.3. Web Configuration



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 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.

6.3.2. 802.1Q VLAN

6.3.2.1. Introduction

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.

6.3.2.2. CLI Configuration

Node	Command	Description
enable	show vlan <1-4094>	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	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 name	This command configures the vlan name to default. Note: The default vlan name is "VLAN"+vlan_ID, VLAN1, VLAN2,…
vlan	add PORTLISTS	This command add a port or a range of ports to the vlan.
vlan	fixed PORTLISTS	This command assigns ports for permanent member of the vlan.
vlan	no fixed PORTLISTS	This command removes all fixed member from the vlan.
vlan	tagged PORTLISTS	This command assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the vlan.
vlan	no tagged PORTLISTS	This command removes all tagged member from the vlan.
vlan	untagged PORTLISTS	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the vlan.
vlan	no untagged PORTLISTS	This command removes all untagged member from the vlan.
interface	acceptable frame type (all|tagged|untagged)	This command configures the acceptable frame type. all - acceptable all frame types. tagged - acceptable tagged frame only. untagged – acceptable untagged frame only.
interface	pvid <1-4094>	This command configures a VLAN ID for the port default VLAN ID.
interface	no pvid	This command configures 1 for the port default VLAN ID.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	pvid <1-4094>	This command configures a VLAN ID for the port default VLAN ID.
if-range	no pvid	This command configures 1 for the port default VLAN ID.
configure	vlan range STRINGS	This command configures a range of vlans.
configure	no vlan range STRINGS	This command removes a range of vlans.
vlan-range	add PORTLISTS	This command adds a port or a range of ports to the vlans.

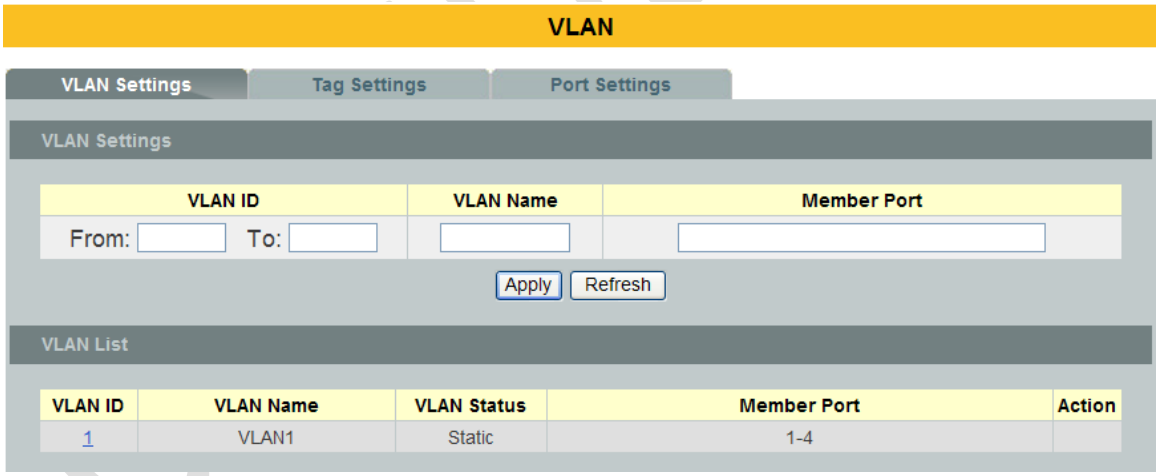
vlan-range	fixed PORTLISTS	This command assigns ports for permanent member of the VLAN group.
vlan-range	no fixed PORTLISTS	This command removes all fixed member from the vlans.
vlan-range	tagged PORTLISTS	This command assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the vlans.
vlan-range	no tagged PORTLISTS	This command removes all tagged member from the vlans.
vlan-range	untagged PORTLISTS	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the vlans.
vlan-range	no untagged PORTLISTS	This command removes all untagged member from the vlans.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#vlan 2
L2SWITCH(config-vlan)#fixed 1-4
L2SWITCH(config-vlan)# tagged 1-3
```

6.3.2.3. Web Configuration

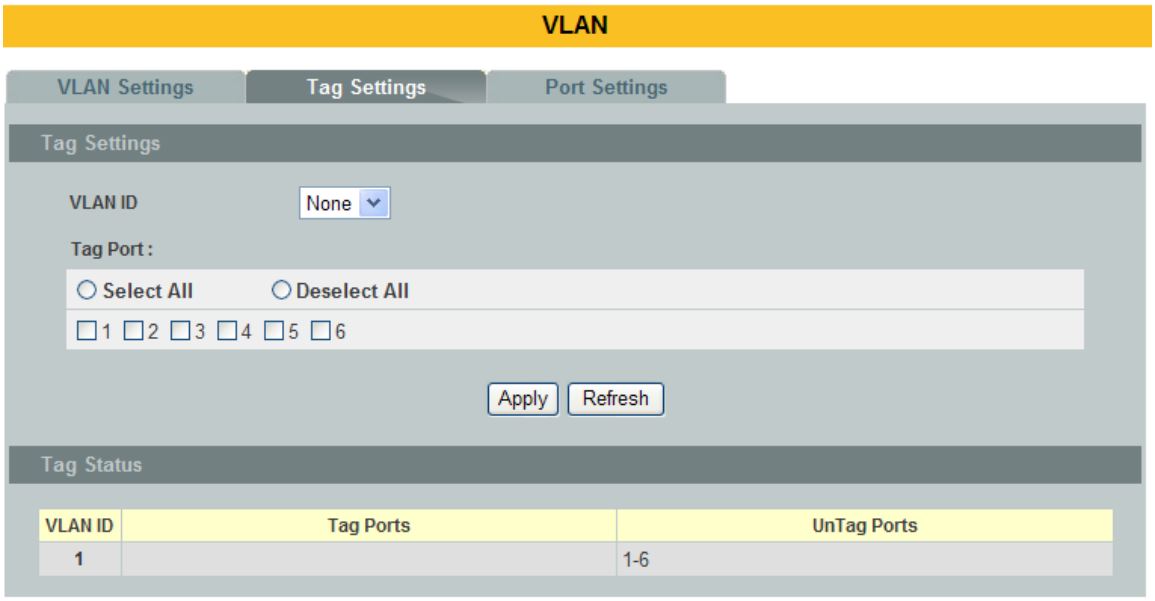
VLAN Settings



Parameter	Description
VLAN ID	Enter a range of VLAN ID which you want to configure; 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.

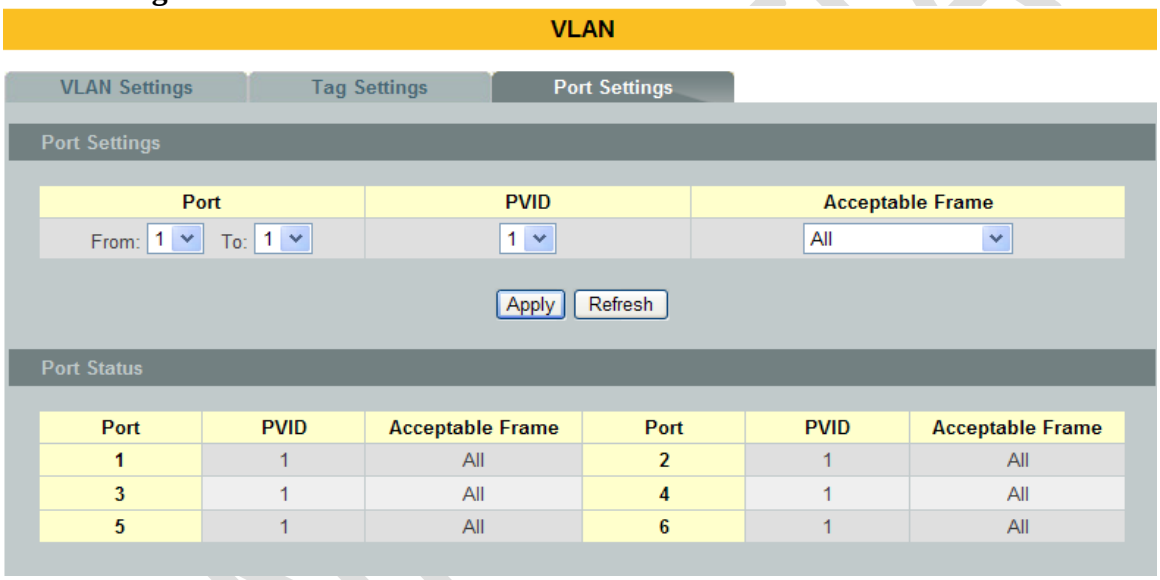
Tag Settings



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



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.**

6.3.3. MAC-based VLAN

6.3.3.1. Introduction

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, 00:01:02 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: 00:01:02, VLAN=23, Priority=2.

The packets with SA=00:01:02:xx:xx:xx will be forwarded to VLAN 22 member ports.

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

6.3.3.2. CLI Configuration

Node	Command	Description
enable	show mac-vlan	This command displays the all of the mac-vlan configurations.
configure	mac-vlan STRINGS vlan <1-4094> 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.

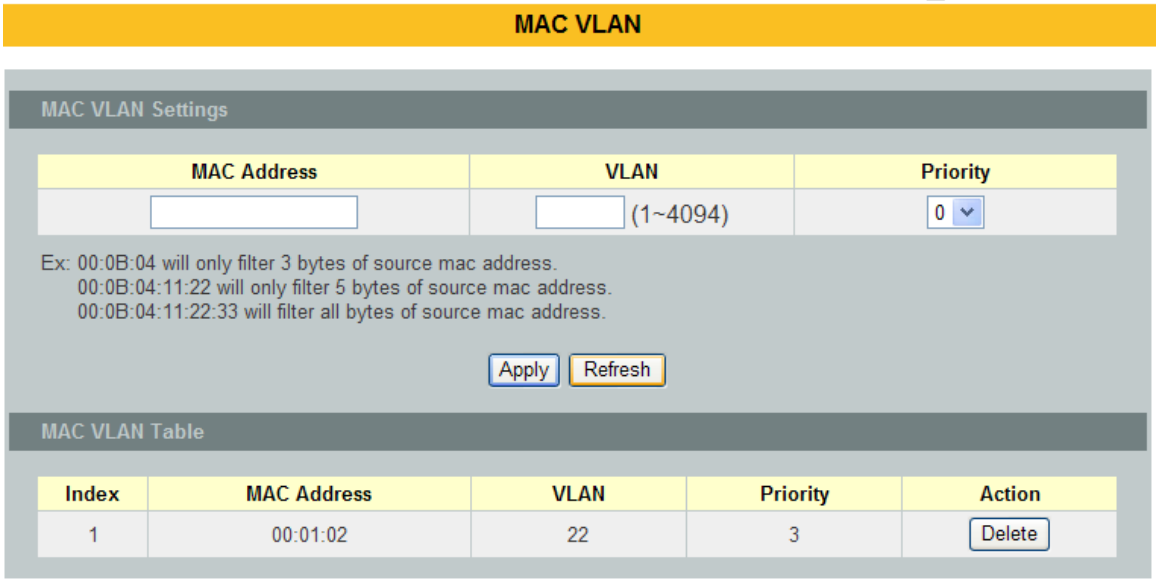
Where the STRINGS is the leading three or more bytes of the mac address.
For example:

00:01:02
00:01:02:11
00:01:02:11:22

00:01:02:11:22:33

Example:
L2SWITCH(config)#vlan 22
L2SWITCH(config-vlan)#fixed 1-4
L2SWITCH(config-vlan)#exit
L2SWITCH(config)#mac-vlan 00:01:02:11:22 vlan 22 priority 1

6.3.3.3. Web Configuration



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.

6.4. Dual Homing

6.4.1. Introduction

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, the device will replace primary connection by secondary connection. 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 Global status: Enabled

Configurations for all groups:

Dual-Homing Group Status : Disabled.
Primary Channel : None.
Secondary Channel : None.

Notices

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

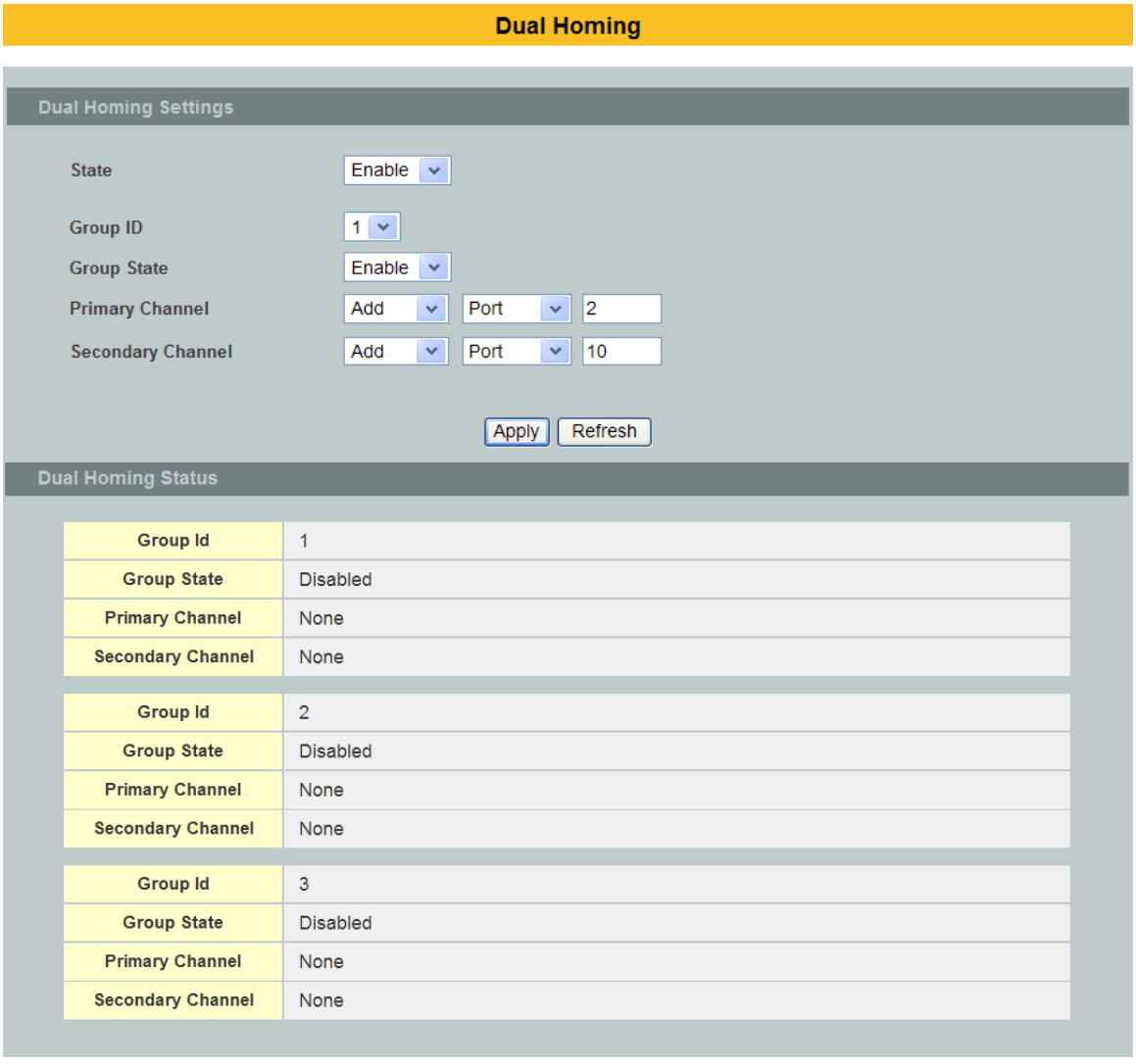
6.4.2. CLI Configuration

Node	Command	Description
enable	show dual-homing	This command displays the dual-homing configurations of all groups.
configure	dual-homing (disable | enable)	This command disables / enables the dual-homing function for the system.
configure	dual-homing <1-3> (disable | enable)	This command disables / enables a group of dual-homing function for the system.
configure	dual-homing group <1-3> primary-channel (port|trunk) VALUE	This command sets the dual-homing primary channel for a group. The channel can be a single port or a trunk group.
configure	no dual-homing group <1-3> primary-channel	This command resets the dual-homing primary channel for a group.
configure	dual-homing group <1-3> secondary-	This command sets the dual-homing secondary channel for a group.

	channel (port|trunk) VALUE	The channel can be a single port or a trunk group.
configure	no dual-homing <1-3> secondary-channel	This command resets the dual-homing secondary channel for a group.

- L2SWITCH(config)# dual-homing group 1 primary-channel port 2
- L2SWITCH(config)# dual-homing group 1 secondary -channel trunk 1
- L2SWITCH(config)# dual-homing group 1 enable
- L2SWITCH(config)# dual-homing enable

6.4.3. Web Configuration



Parameter	Description
State	Enables / disables the Dual-Homing for the Switch.

Group ID	Selects a group which you want to configure.
Group State	Enables / disables the Dual-Homing for a group.
Primary channel	Configures / Resets the primary channel for a group. The channel can be single port or a trunk group.
Secondary channel	Configures / Resets the secondary channel for a group. The channel can be single port or a trunk group.
Dual Homing Status	
Group ID	The group number.
Group State	The state of the group.
Primary Channel	The primary channel configurations and current link status for a group.
Secondary Channel	The secondary channel configurations and current link status for a group.

6.5. EEE (Energy Efficient Ethernet)

6.5.1. Introduction

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.

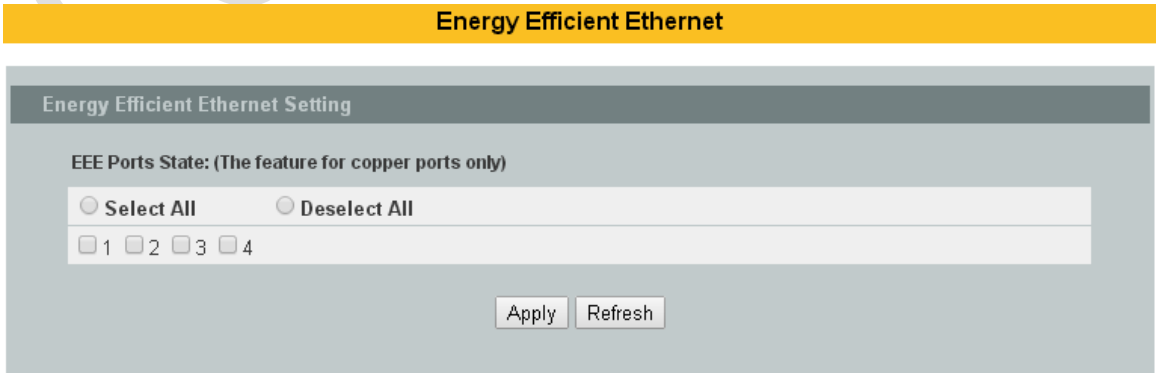
6.5.2. CLI Configuration

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

6.5.3. Web Configuration



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 setting.

6.6. Link Aggregation

6.6.1. 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 : 3.
- Maximum port in link aggregation group : 4.

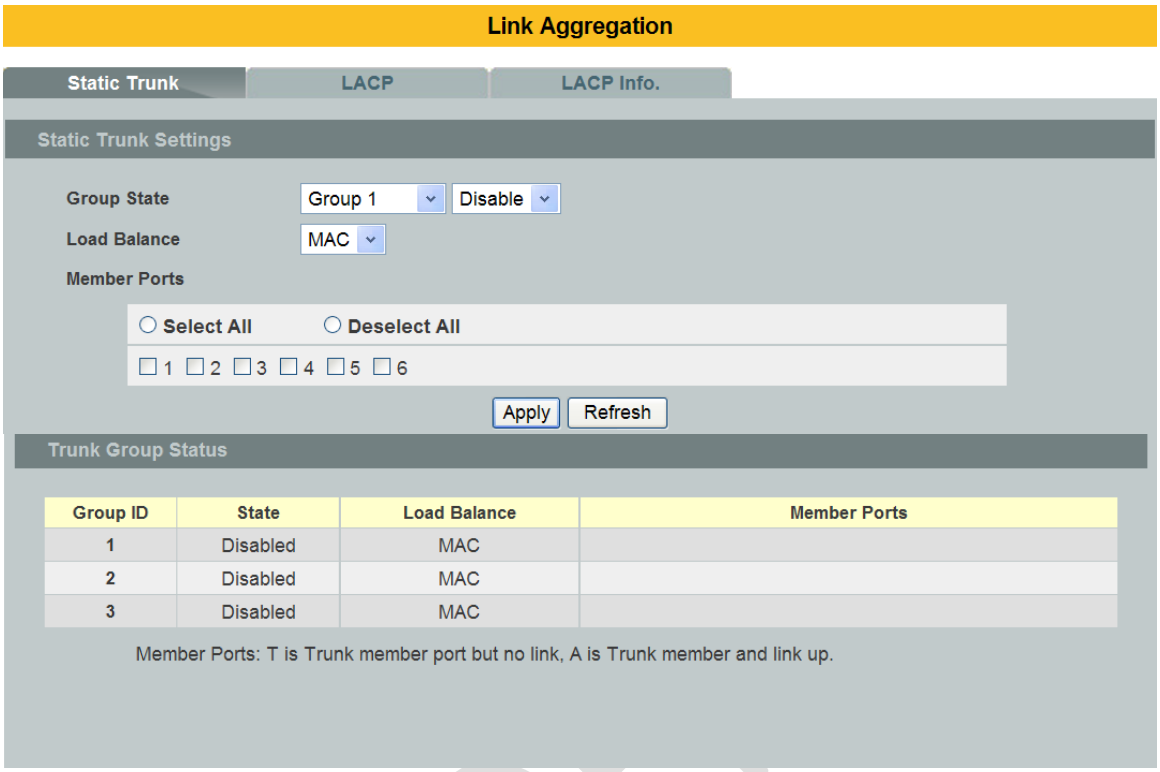
6.6.1.1. CLI Configuration

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.

Example:

L2SWITCH#*configure terminal*
L2SWITCH(config)#*link-aggregation 1 enable*
L2SWITCH(config)#*link-aggregation 1 ports 1-4*

6.6.1.2. Web Configuration



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.
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 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.
Member Ports	This field displays the assigned ports that comprise the static trunk group.

6.6.2. 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, and 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.

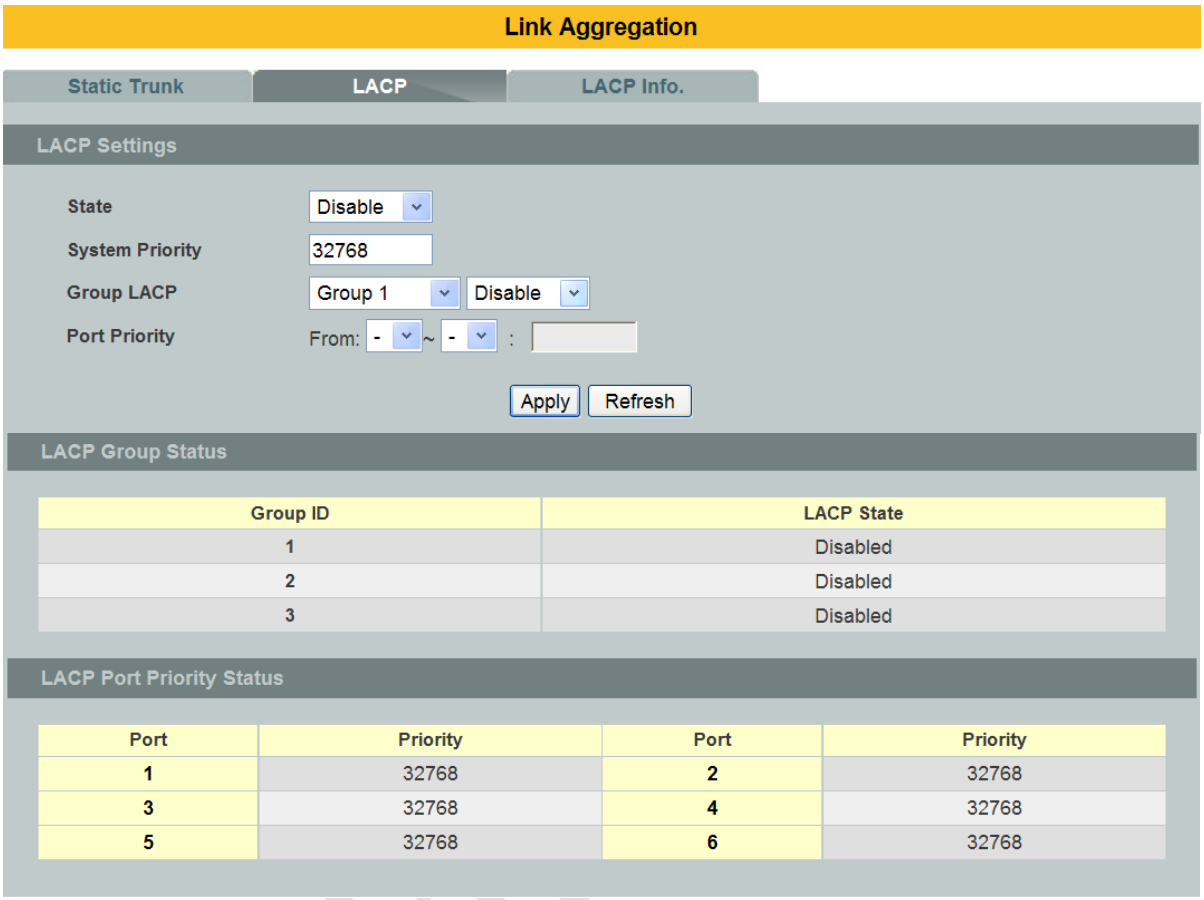
6.6.2.1. CLI Configuration

Node	Command	Description
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 c 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.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	lacp port_priority <1-65535>	This command configures the priority for the specific ports. Note: The default value is 32768.
if-range	no lacp port_priority	This command configures the default for the priority for the specific ports.

6.6.2.2. Web Configuration

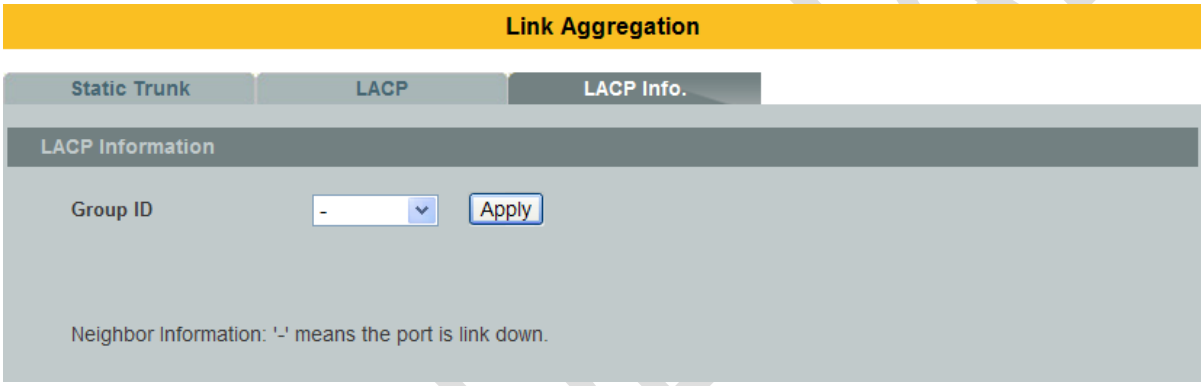
LACP Settings



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 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.



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.

6.7. Link Layer Discovery Protocol (LLDP)

6.7.1. Introduction

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.

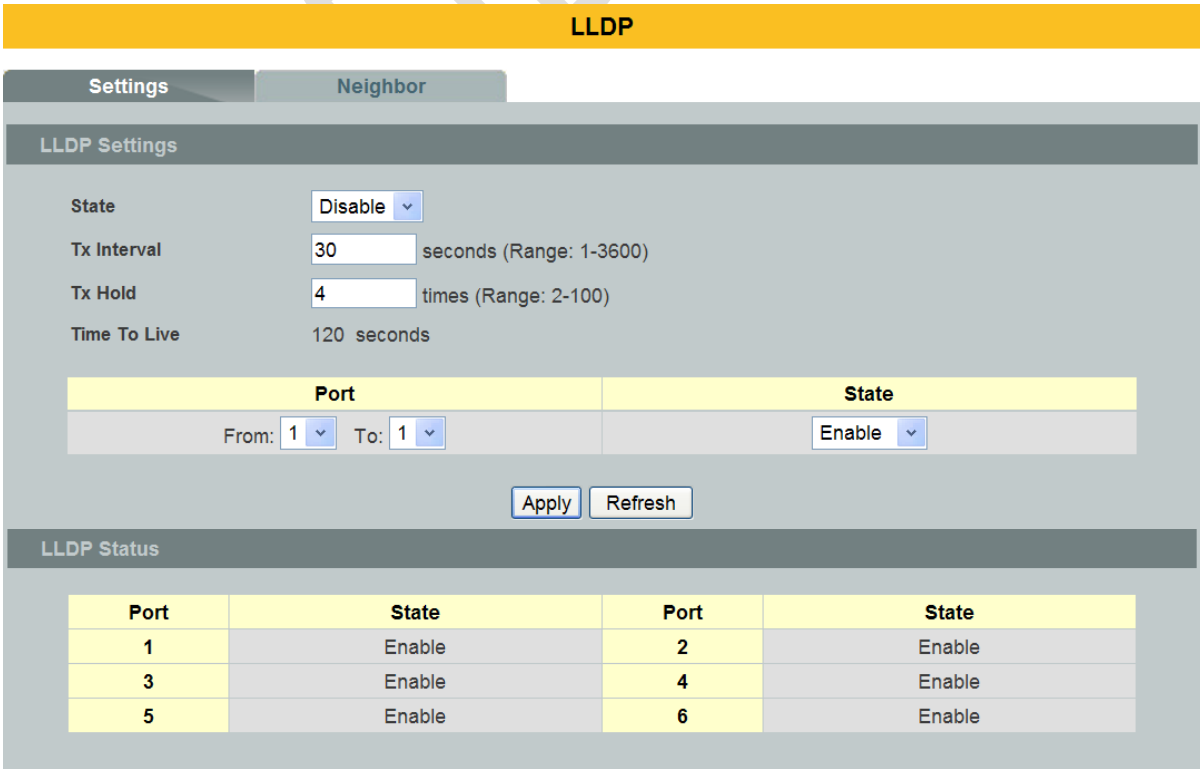
Port	Status	Port	Status
1	Enable	2	Enable
3	Enable	4	Enable
5	Enable	6	Enable

6.7.2. CLI Configuration

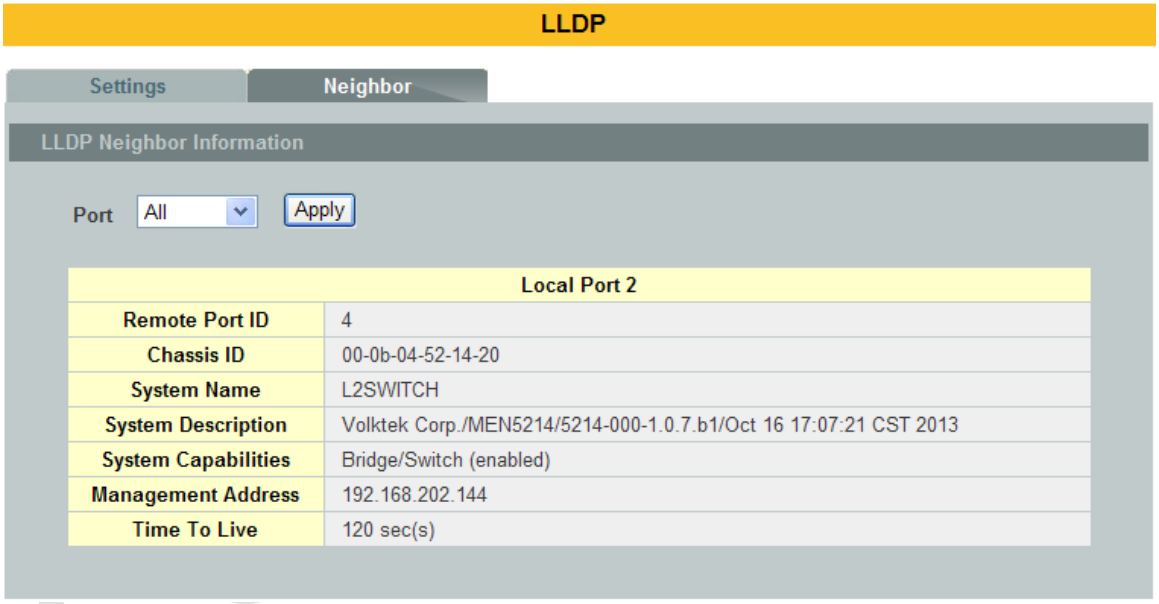
Node	Command	Description
enable	show lldp	This command displays the LLDP configurations.
enable	show lldp neighbor	This command displays all of the ports' neighbor information.
configure	lldp (disable|enable)	This command globally enables / disables the LLDP function on the Switch.

configure	lldp tx-interval <1-3600>	This command configures the interval to transmit the LLDP packets.
configure	lldp tx-hold <2-100>	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.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	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.

6.7.1. Web Configuration



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.



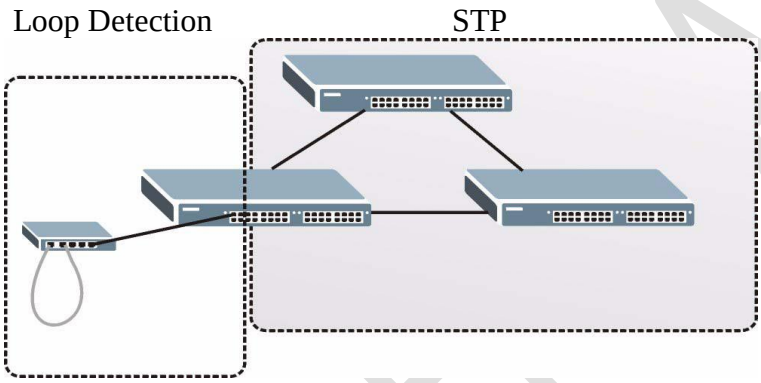
Parameter	Description
Port	Select the port(s) which you want to display the port's neighbor information.
Local Port	The local port ID.
Remote Port ID	The connected port ID.
Chassis ID	The neighbor's chassis ID.
System Name	The neighbor's system name.

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.

6.8. 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 State	Recovery Time	Port	State	Status	Recovery State	Recovery 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

6.8.1. 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 port.
interface	no shutdown	This command enables the 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 <1-60>	This command configures the recovery period time.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	loop-detection (disable | enable)	This command disables / enables the loop detection on the ports.
if-range	loop-detection recovery (disable | enable)	This command enables / disables the recovery function on the port.

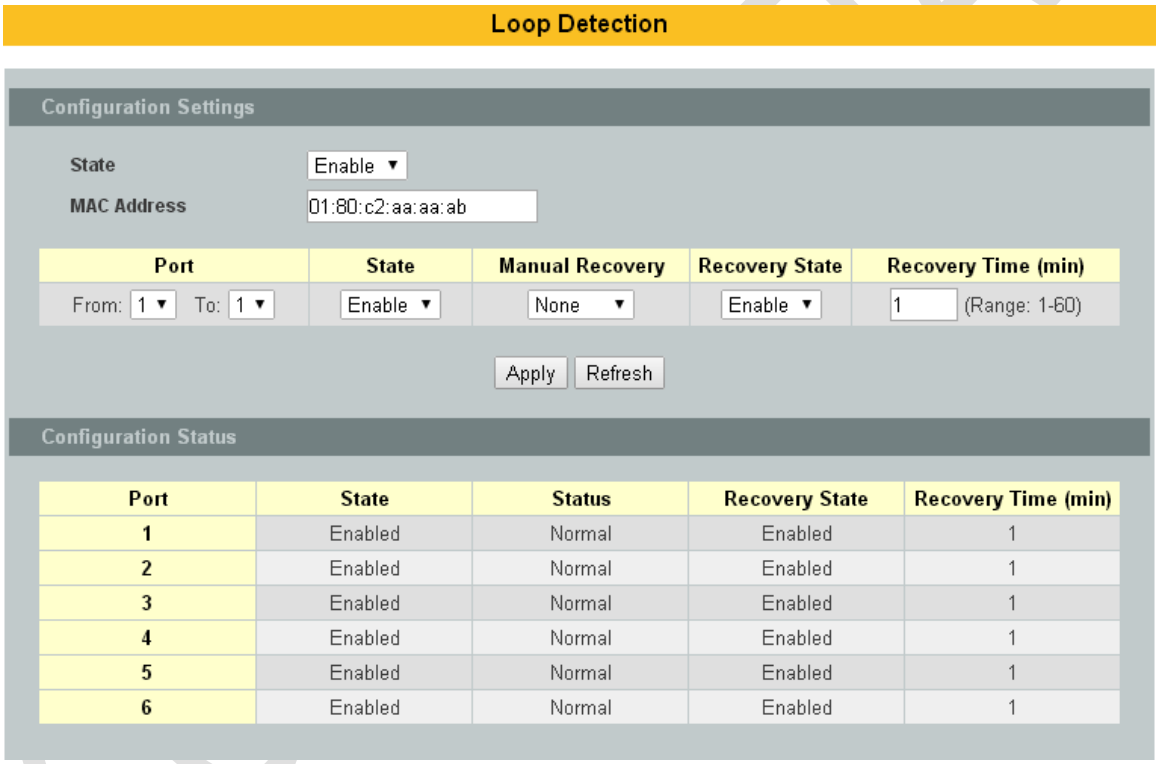
if-range	loop-detection recovery time <1-60>	This command configures the recovery period time.

Example: The procedures to enable the Loop Detection on port 1

✓ To enable the global Loop Detection.
L2SWITCH(config)#loop-detect enable

✓ To select the port 1 you want to configure.
L2SWITCH(config)#interface gigabitethernet1/0/1

6.8.2. Web Configuration



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. **The MAC should be a valid multicast MAC.**
Port	Select a port on which to configure loop guard protection.
State	Select **Enable** to use the loop guard feature on the Switch.

Manual Recovery	Select **Unblock** to enable the port.
Recovery State	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.
Configuration 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.
Recovery State	This field displays if the loop recovery feature is enabled.
Recovery Time (min)	This field displays the recovery time for the loop recovery feature.

6.9. PoE (Power over Ethernet)

6.9.1. PoE

6.9.1.1. Introduction

Power over Ethernet or **PoE** technology describes a system to pass electrical power safely, along with data, on Ethernet cabling. PoE requires category 5 cable or higher for high power levels, but can operate with category 3 cable for low power levels. Power can come from a power supply within a PoE-enabled networking device such as an Ethernet switch or can be injected into a cable run with a midspan power supply.

The original **IEEE 802.3af-2003** PoE standard provides up to 15.4 W of DC power (minimum 44 VDC and 350 mA) to each device. Only 12.95 W is assured to be available at the powered device as some power is dissipated in the cable.

The updated **IEEE 802.3at-2009** PoE standard also known as **PoE+** or **PoE plus**, provides up to 25.5 W of power. Some vendors have announced products that claim to comply with the 802.3at standard and offer up to 51 W of power over a single cable by utilizing all four pairs in the Cat.5 cable. Numerous non-standard schemes had been used prior to PoE standardization to provide power over Ethernet cabling. Some are still in active use.

PSE: Power sourcing equipment (PSE) is a device such as a switch that provides ("sources") power on the Ethernet cable.

PD: A powered device (PD) is a device such as an access point or a switch, that supports PoE (Power over Ethernet) so that it can receive power from another device through a 10/100Mbps Ethernet port.

Standard PoE parameters and comparison

Property	**802.3af**	**802.3at**
Power available at PD	12.95 W	25.50 W per mode
Maximum power delivered by PSE	15.40 W	30 W per mode
Voltage range (at PSE)	44.0 - 57.0 V	50.0 - 57.0 V
Voltage range (at PD)	37.0 - 57.0 V	42.5 - 57.0 V
Maximum current	350 mA	600 mA per mode
Maximum cable resistance	20 Ω (Category 3)	12.5 Ω (Category 5)
Power management	Three power class levels negotiated at initial connection	Four power class levels negotiated at initial connection or 0.1W steps negotiated continuously
Derating of maximum cable ambient operating temperature	None	5℃ with one mode (two pairs) active

Supported cabling	Category 3 and Category 5	Category 5
Supported modes	Mode A (endspan), Mode B (midspan)	Mode A, Mode B, Mode A and Mode B operating simultaneously

Power Devices

Class	Usage	Power levels available: Classification current [mA]	Power range [Watt]	Class description
0	Default	0 - 4	0.44 - 12.94	Classification unimplemented
1	Optional	9 - 12	0.44 - 3.84	Very Low power
2	Optional	17 - 20	3.84 - 6.49	Low power
3	Optional	26 - 30	6.49 - 12.95	Mid power
4	Reserved	36 - 44	12.95 - 25.50	High power

For IEEE 802.3at (type 2) devices class 4 instead of Reserved has a power range of 12.95 - 25.5 W.

PoE Specification Functions

The port 1 ~ 4 supports the PoE function.
Total-power: The maximum power which the switch can support to the PDs.

Schedule: The Switch allows user to arrange a week schedule to enable or disable the PoE for the specific ports.

Default Settings

State : Disabled
Total Power(W) : 0

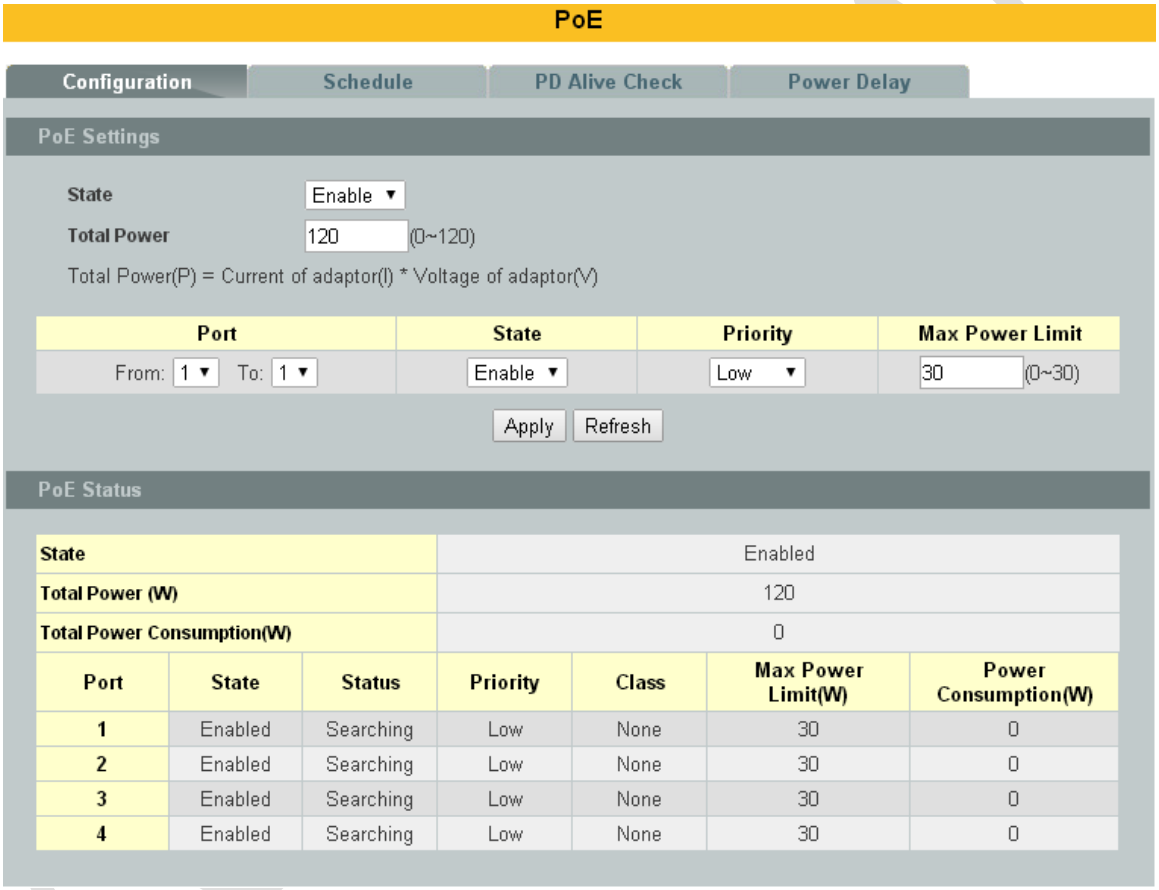
Port	State	Status	Priority
1	Disabled	Disabled	High
2	Disabled	Disabled	High
3	Disabled	Disabled	High
4	Disabled	Disabled	High

6.9.1.2. CLI Configuration

Node	Command	Description
enable	show poe	This command displays the PoE configurations and status.
enable	show poe schedule port PORT_ID	This command displays the PoE port schedule configurations.
configure	poe (disable | enable)	This command disables or enables the global PoE for the Switch.

configure	poe total-power	This command configures the total power which the Switch can support.
interface	poe (disable|enable)	This command enables or disables the PoE function on the specific port.
interface	poe priority (critical|high|low)	This command configures the priority of the PoE function for the specific port. ● critical : The highest priority. ● high : The middle priority. ● low : The lowest priority.

6.9.1.3. Web Configuration



Parameter	Description
PoE Mode	Selects the PoE mode, classification or consumption. **Classification** - Allocated power according to class (0 to 4). **Consumption** - Allocated power according to the actual need of each PD.
Port	Selects a port or a range of ports that you want to configure the PoE function.
State	Selects **Enable** to enable the PoE function on the specific port. Selects **Disable** to disable the PoE function on the specific port.

Priority	Selects **Critical / High / Low** priority for the specific port.
Max Power Limit	Configure the maximum power for the port.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
PoE Status	
State	Displays the global state for the Switch.
Total Power(W)	Displays the total power that the Switch supports.
Total Power Consumption	Displays the total consuming power for all of the PDs.
Port Status	
Port	Display the Port No.
State	Displays the PoE state for the specific port.
Status	Displays the current PoE state machine.
Priority	Displays the PoE priority for the specific port.
Class	Displays the class mode which the PSE negotiate with the PD on the specific port.
Max Power Limit(W)	Displays the maximum power for the specific port.
Consuming Power(mW)	Displays the consuming power for the specific port.

6.9.2. PoE Schedule

6.9.2.1. Introduction

The function has a global state configuration. If the global state configuration is disabled. The Switch will not perform the schedule function. If the global state is enabled, the Switch will check every port's configurations.

If the port's check configuration is NO for a specific day, the Switch will not perform action for the specific port. If the port's check configuration is YES for a specific day, the Switch will check the Start time and End Time. If the current time is in the interval between Start time and End Time, the Switch will perform the action configuration. If the action is ENABLE, the Switch will send power to the port. If the current time is not in the interval between Start time and End Time, the Switch will not send power to the port.

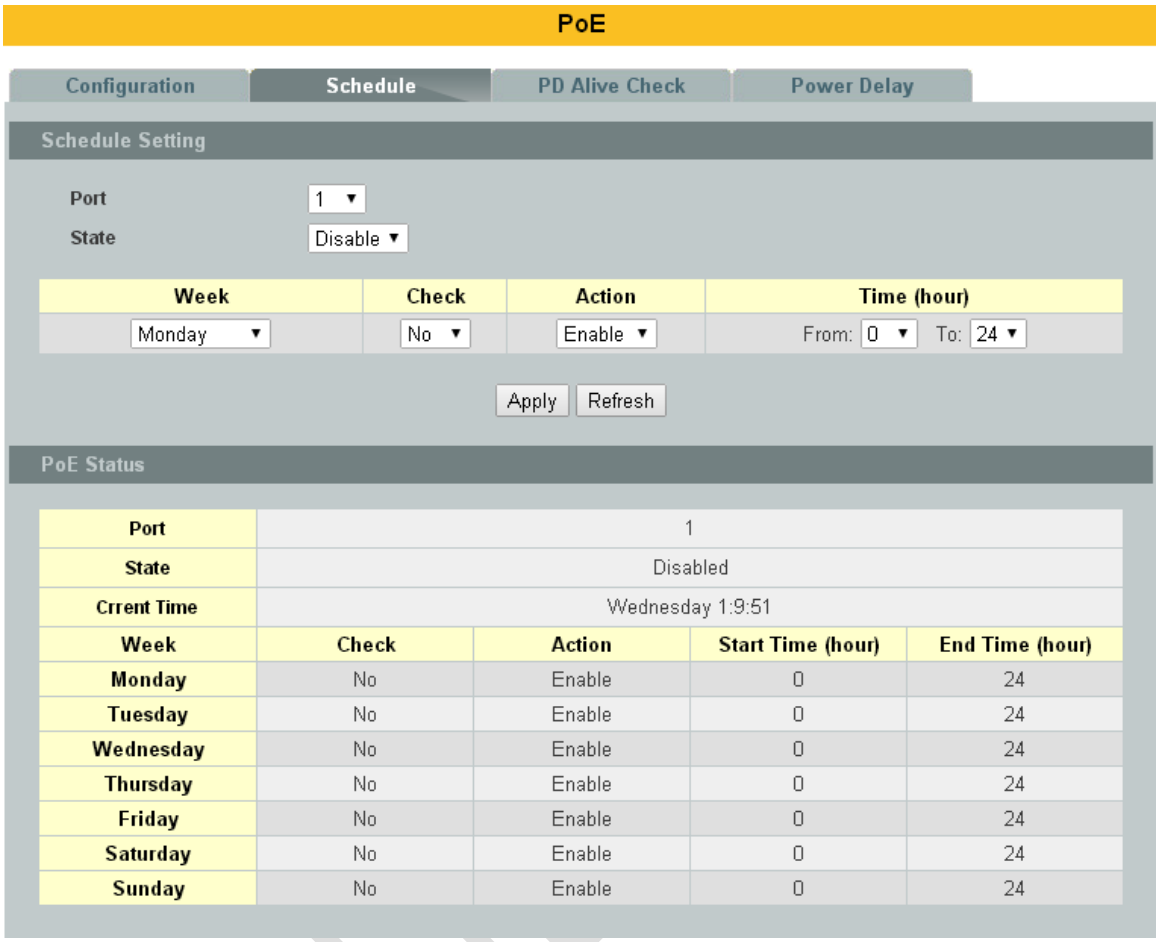
Port : 1
Schedule State: Disabled

Week	Check	Action	Start Time(hour)	End Time(hour)
Monday	No	Enable	0	24
Tuesday	No	Enable	0	24
Wednesday	No	Enable	0	24
Thursday	No	Enable	0	24
Friday	No	Enable	0	24
Saturday	No	Enable	0	24
Sunday	No	Enable	0	24

6.9.2.2. CLI Configuration

Node	Command	Description
enable	show poe schedule port PORT_ID	This command displays the PoE port schedule configurations.
interface	poe schedule (disable|enable)	This command disables or enables the PoE schedule on the specific port.
interface	poe schedule week (Sun|Mon|Tue|Wed|Thu|Fri|Sat) check (yes|no)	This command enables or disables the PoE schedule on the specific day.
interface	poe schedule week (Sun|Mon|Tue|Wed|Thu|Fri|Sat) start-time VALUE end-time VALUE action (enable|disable)	This command configures the PoE schedule start-time and end-time on a specific day on the specific port. Users can enable or disable the PoE on the time period.

6.9.2.1. Web Configuration



Parameter	Description
Port	Selects a port that you want to configure the PoE schedule function.
State	Select **Enable/Disable** to enable/disable the schedule function on the specific port.
Week	Select a week day that you want to configure the schedule.
Check	Enables or Disables the PoE schedule on the specific port for a defined time period.
Action	Enables or Disables the PoE function for a defined time period.
Time (Hour)	Configures the time period.

6.9.3. PD Alive Check

6.9.3.1. Introduction

The function has a global state configuration. If the global state configuration is enabled.

The Switch will check the configurations of every port.

If the port's state is enabled, the Switch will send keep-a-live probe packet every interval time. If the host cannot respond when the keep-a-live probe packet count is over the retry times, the Switch performs the action, reboot/alarm/all to the Power Device, depending on the port's configuration.

Power OFF Time (sec):
When PD has been rebooted, the PoE port restored power after the specified time.
Default:15, range: 3-120 sec.

Start up Time (sec):
When PD has been start up, the Switch will wait Start up time to do PoE Auto Checking.
Default: 60, range: 30-600 sec.

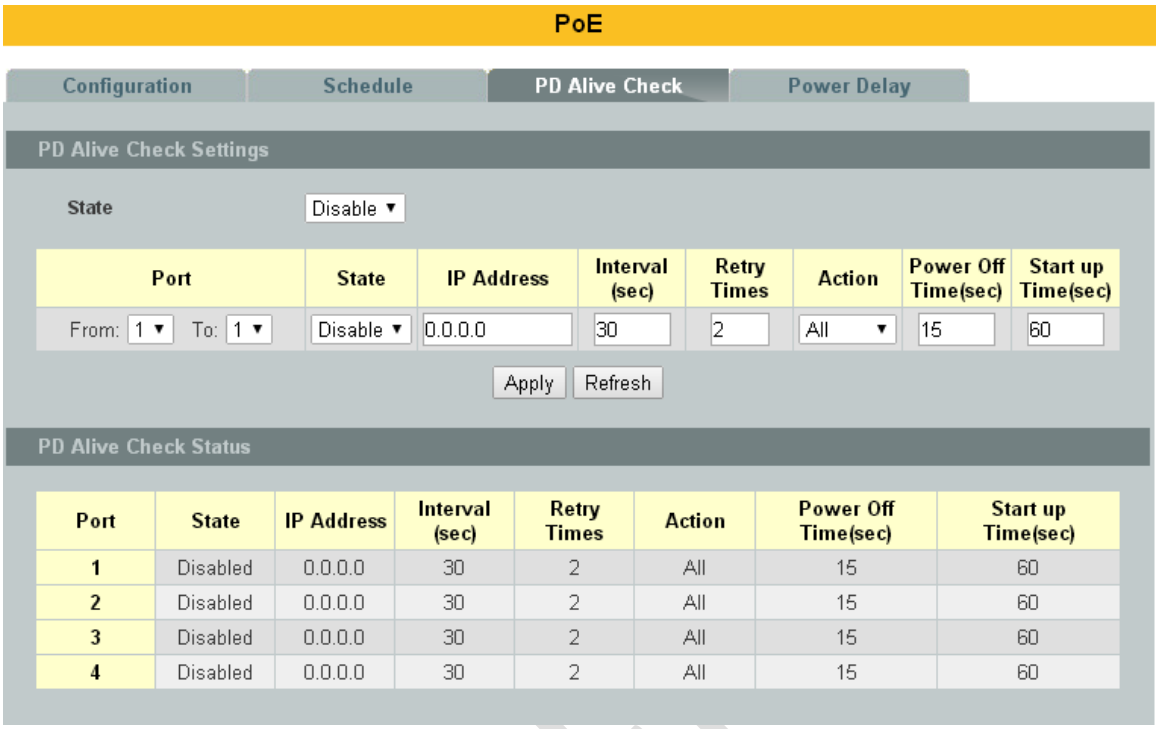
Interval Time (sec):
Device will send checking message to PD each interval time.
Default: 30, range: 10-120 sec.

Failure Action:
The action when the third fail detection.
Nothing: Keep Ping the remote PD but does nothing further.
Reboot Remote PD: Cut off the power of the PoE port, make PD rebooted.

6.9.3.2. CLI Configuration

Node	Command	Description
enable	show pd-alive	This command displays the configuration of the PD Alive Check.
configure	pd-alive (disable|enable)	This command disables or enables the global PD Alive Check for the Switch.
Interface	pd-alive action (reboot|alarm|all)	This command configures the action when the system detects that the host cannot respond the keep-a-live probe packet
Interface	pd-alive interval VALUE	This command configures the interval to send the keep-a-live probe packets to check if the host is still alive for the specific port.
Interface	pd-alive ip IP_ADDR	This command configures the Host IP address which connects to the specific port.
Interface	pd-alive reboot-time VALUE	This command configures the time which the host needs to reboot the system.
Interface	pd-alive retry-time VALUE	This command configures the retry times when no response from the host for the keep-a-live probe packet for the specific port.

6.9.3.3. Web Configuration



Parameter	Description
State	Enables/Disables the PD Alive Check.
Port	Selects a port or a range of ports which you want to configure.
State	Enables/Disables the PD Alive Check for the specific port(s).
IP Address	Specifies the Host IP address which connects to the port.
Interval	The interval to send the packet probes to check if the host is still alive.
Retry Times	The retry times when no response from the host for the keep-a-live probe packet.
Action	The action to the Power Device when the system detects that the Power Device cannot respond the keep-a-live probe packet. The options have Reboot / Alarm / All.
Reboot Time	The time which the host needs to reboot the system.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

6.9.4. Power Delay

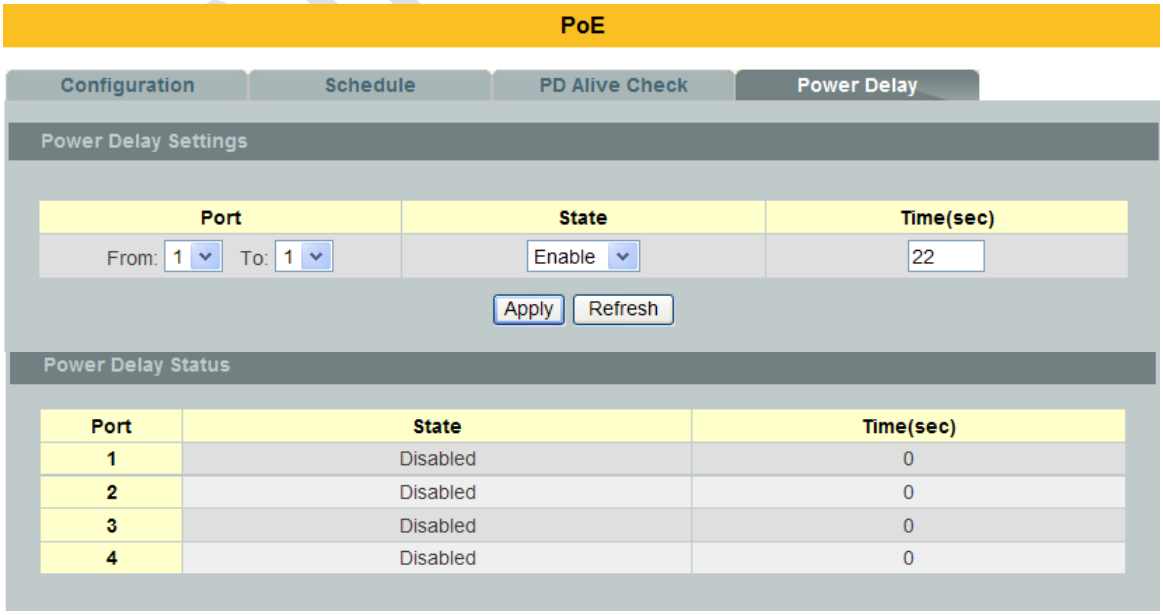
6.9.4.1. Introduction

The Power Delay allows the user to setting the delay time of power providing after device rebooted.

6.9.4.2. CLI Configuration

Node	Command	Description
enable	show poe power-delay	This command displays the PoE power delay configurations.
interface	poe power-delay (enable|disable)	This command enables / disables of the Power Delay function for the specific port.
interface	poe power-delay time VALUE	This command configures the delay time of the Power Delay for the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	poe power-delay (enable|disable)	This command enables / disables of the Power Delay function for the range of ports.
if-range	poe power-delay time VALUE	This command configures the delay time of the Power Delay for the range of ports.

6.9.4.3. Web Configuration



Parameter	Description
Port	Selects a port or a range of ports which you want to configure.
State	Enables/Disables the PoE Power Delay for the specific ports.
Time	The delay time for the specific ports.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Power Delay Status	
Port	The port ID.
State	The PoE power delay state for the port.
Time	The PoE power delay time for the port.

7. Security

7.1. 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.

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

7.1.1. 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 actives 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	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 MACADDR	This command configures the source AMC and mask for the profile.
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 <1-4094>	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

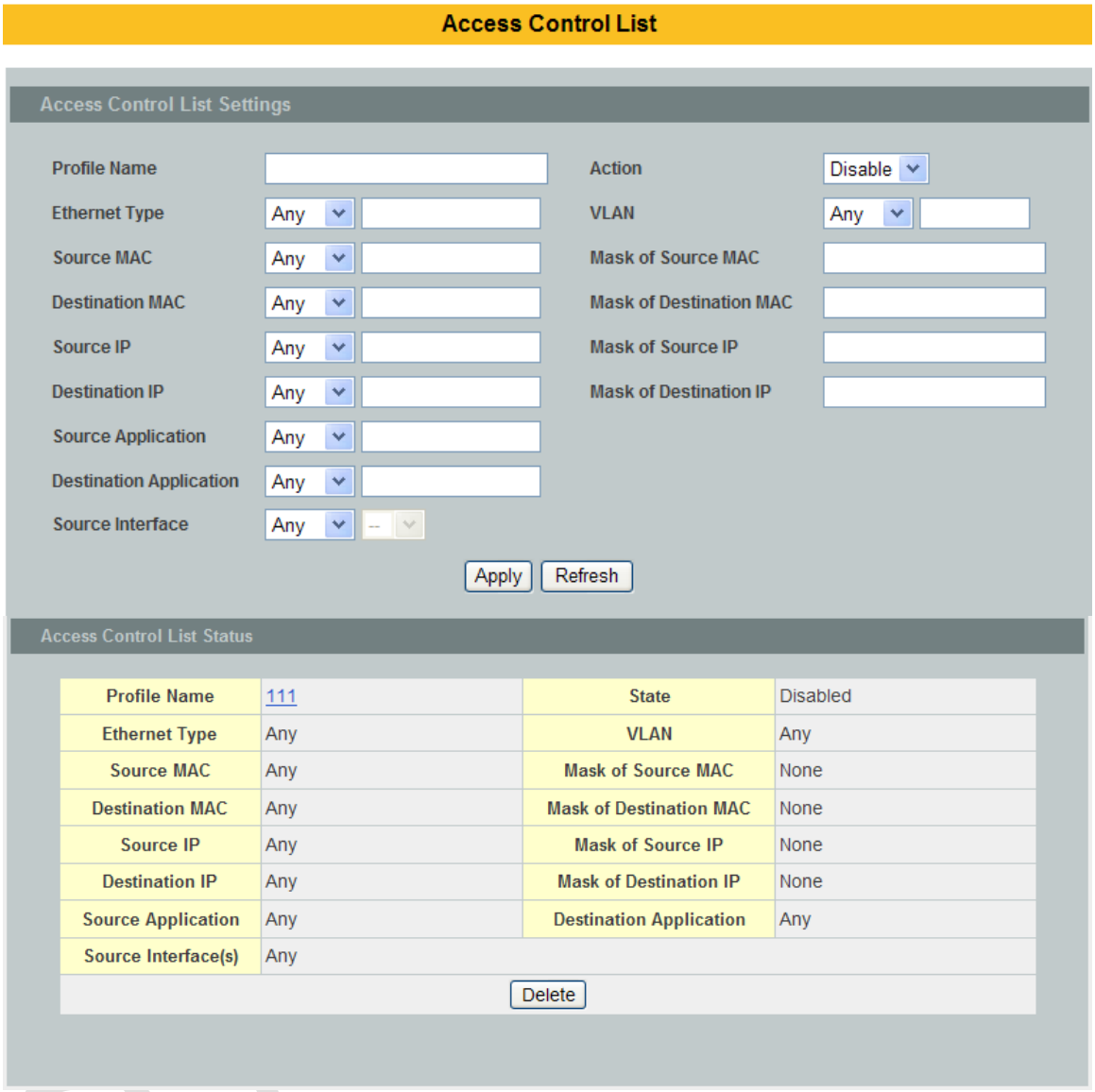
➔ The command will filter source IP range from 172.20.0.0 to 172.20.255.255

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

7.1.2. Web Configuration



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.

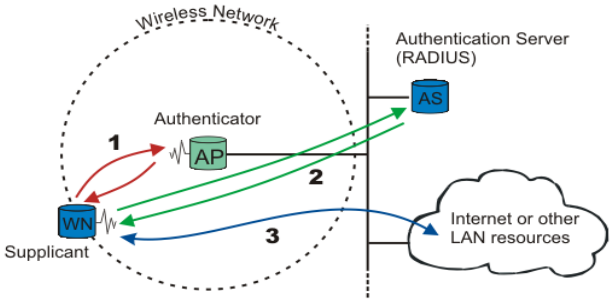
	If the Source MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured in Source MAC field.
Destination MAC	Configures the destination MAC of the packets that you want to filter.
Mask of Destination MAC	Configures the bitmap mask of the destination 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 rage 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.

7.2. 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).

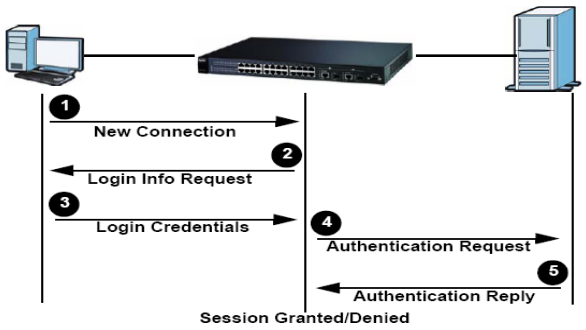
802.1X provides port-based authentication, which involves communications between a supplicant, authenticator, and authentication server. The supplicant is often software on a client device, such as a laptop, the authenticator is a wired Ethernet switch or wireless access point, and an authentication 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 an 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.



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 20 seconds for all ports.
The default port Supp timeout is 30 seconds for all ports.
The default port Server timeout is 16 seconds for all ports.

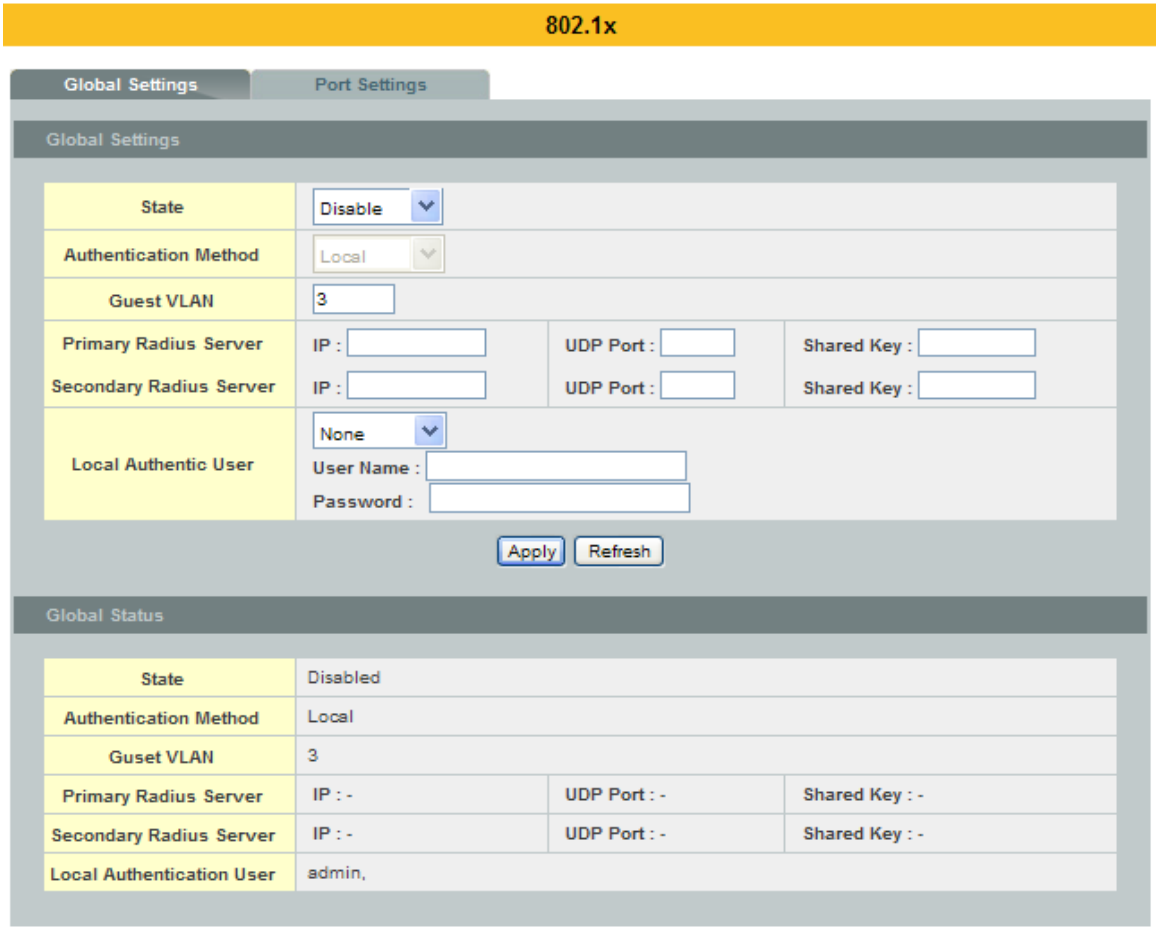
7.2.1. CLI Configuration

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 accounting-record	This command displays the local accounting 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 VLANID	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.

7.2.2. Web Configuration

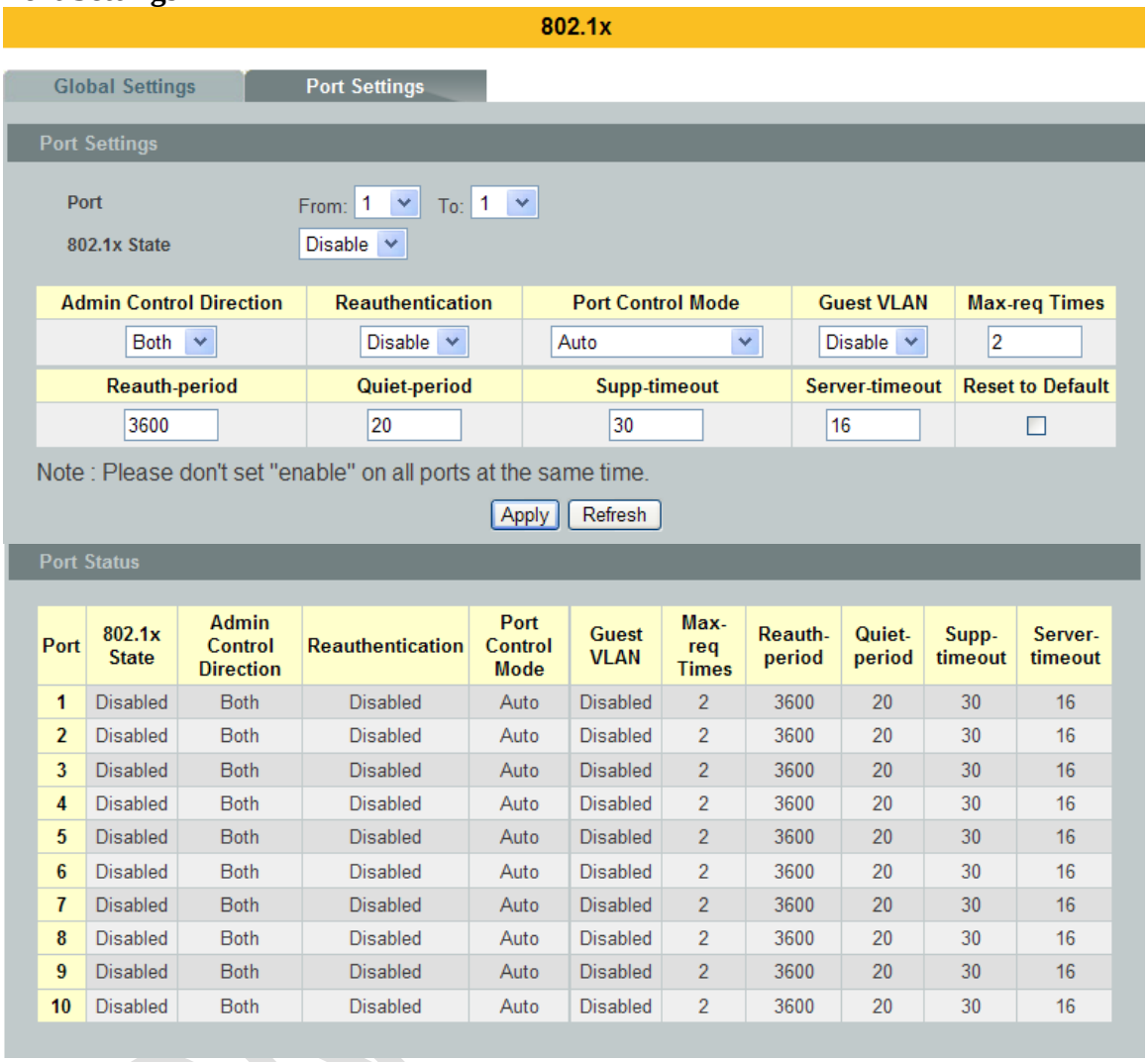
Global Settings



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 Method	Select whether to use **Local** or **RADIUS** as the authentication method. The **Local** method of authentication uses the "guest" and "user" user groups of the user account database on the Switch itself to authenticate. However, only a certain number of accounts can exist at one time. **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.
Guest VLAN	Configure the guest vlan.

Primary Radius Server	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 Radius Server	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 Radius Server	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



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.
Re-authentication	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.
Re-authentication	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.

7.3. 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 used MAC table to check it. The static MAC addresses are included for the limit.

Notice: 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 port state of the port security is disabled.
- ✓ The Maximum MAC per port is 5.

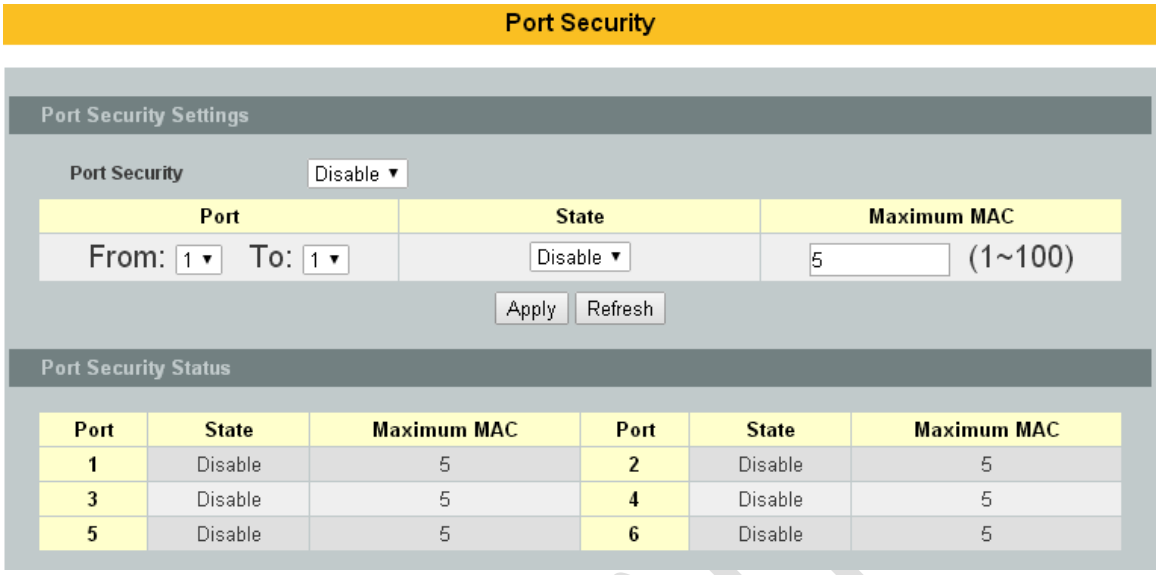
7.3.1. CLI Configuration

Node	Command	Description
enable	show port-security	This command displays the current port security configurations.
configure	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 <1-100>	This command configures the maximum MAC entries on the specific port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	port-security (disable|enable)	This command enables / disables the port security function for the specified ports
if-range	port-security limit <1-100>	This command configures the maximum MAC entries for the specified ports.

Example:

L2SWITCH#*configure terminal*
L2SWITCH#*port-security enable*
L2SWITCH#interface 1/0/1
L2SWITCH#*port-security limit 10*
L2SWITCH#*port-security enable*

7.3.2. Web Configuration



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

8. Monitor

8.1. Alarm

8.1.1. Introduction

The feature displays if there are any abnormal situation need process immediately.

Notice:

The Alarm DIP Switch allow users to configure if send alarm message when the corresponding event occurs.

For Example:

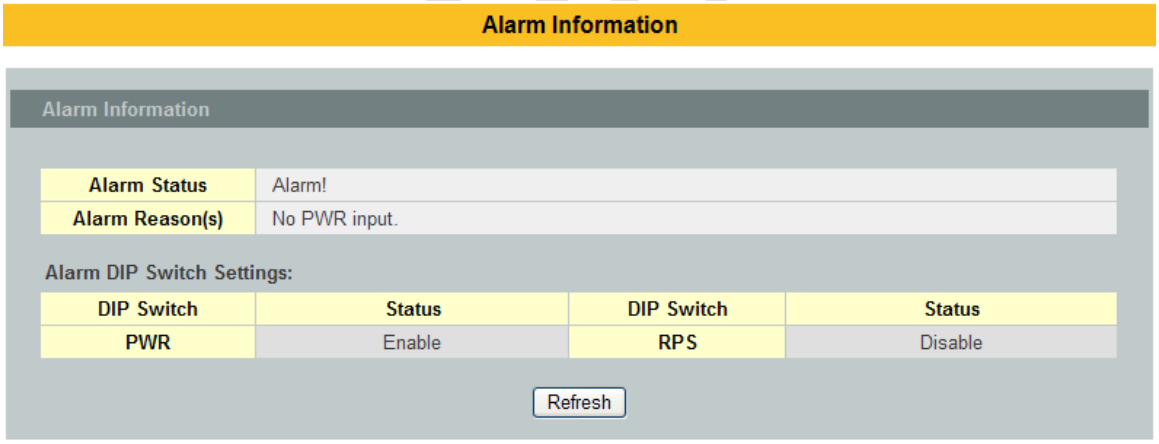
PWR: ON, The Switch will send alarm message when the main power supply disconnect.

RPS: ON, The Switch will send alarm message when the redundant power supply disconnect.

8.1.2. CLI Configuration

Node	Command	Description
enable	show alarm-info	This command displays alarm information.

8.1.3. Web Configuration



Parameter	Description
Alarm Information	
Alarm Status	This field indicates if there is any alarm events.
Alarm Reason(s)	This field displays all of the detail alarm events.
Alarm DIP Switch Settings	
DIP Switch	The field displays the DIP Switch name.

Status	The field indicates the DIP Switch current status.

8.2. Port Statistic

8.2.1. Introduction

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

8.2.2. CLI Configuration

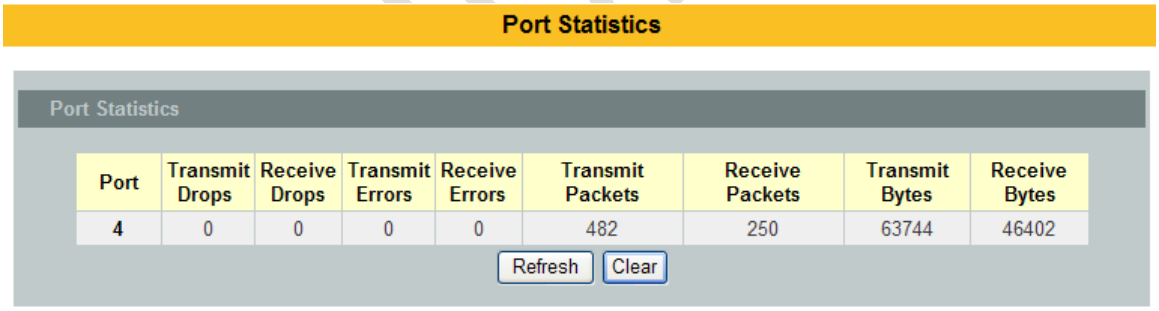
Node	Command	Description
enable	show port-statistics	This command displays the link up ports' statistics.

Example:

```
L2SWITCH#show port-statistics

          Packets                 Bytes                   Errors                  Drops
Port      Rx          Tx          Rx          Tx          Rx          Tx          Rx          Tx
----      --------    --------    ----------  --------    --------    --------    --------    --------
 5        1154        2           108519      1188        0           0           0           0
```

8.2.3. Web Configuration



Parameter	Description
Port	Select a port or a range of ports to display their statistics.
Rx Packets	The field displays the received packet count.
Tx Packets	The field displays the transmitted packet count.
Rx Bytes	The field displays the received byte count.
Tx Bytes	The field displays the transmitted byte count.
Rx Errors	The field displays the received error count.
Tx Errors	The field displays the transmitted error count.

Rx Drops	The field displays the received drop count.
Tx Drops	The field displays the transmitted drop count.
Refresh	Click this button to refresh the screen quickly.

8.3. Port Utilization

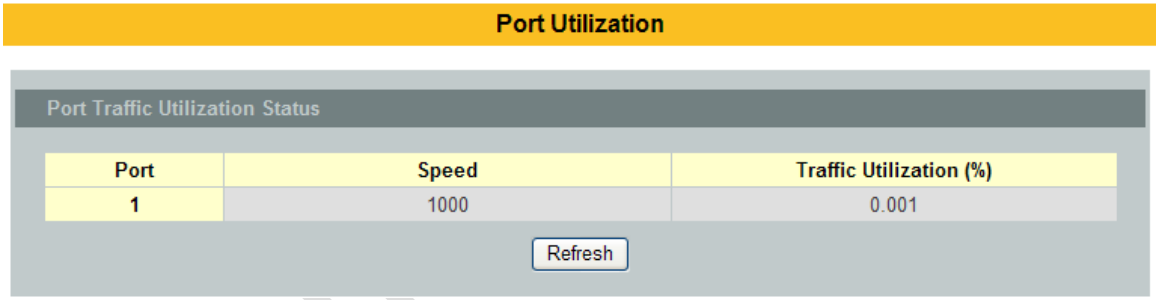
8.3.1. Introduction

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

8.3.2. CLI Configuration

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

8.3.3. Web Configuration



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.

8.4. RMON Statistics

8.4.1. Introduction

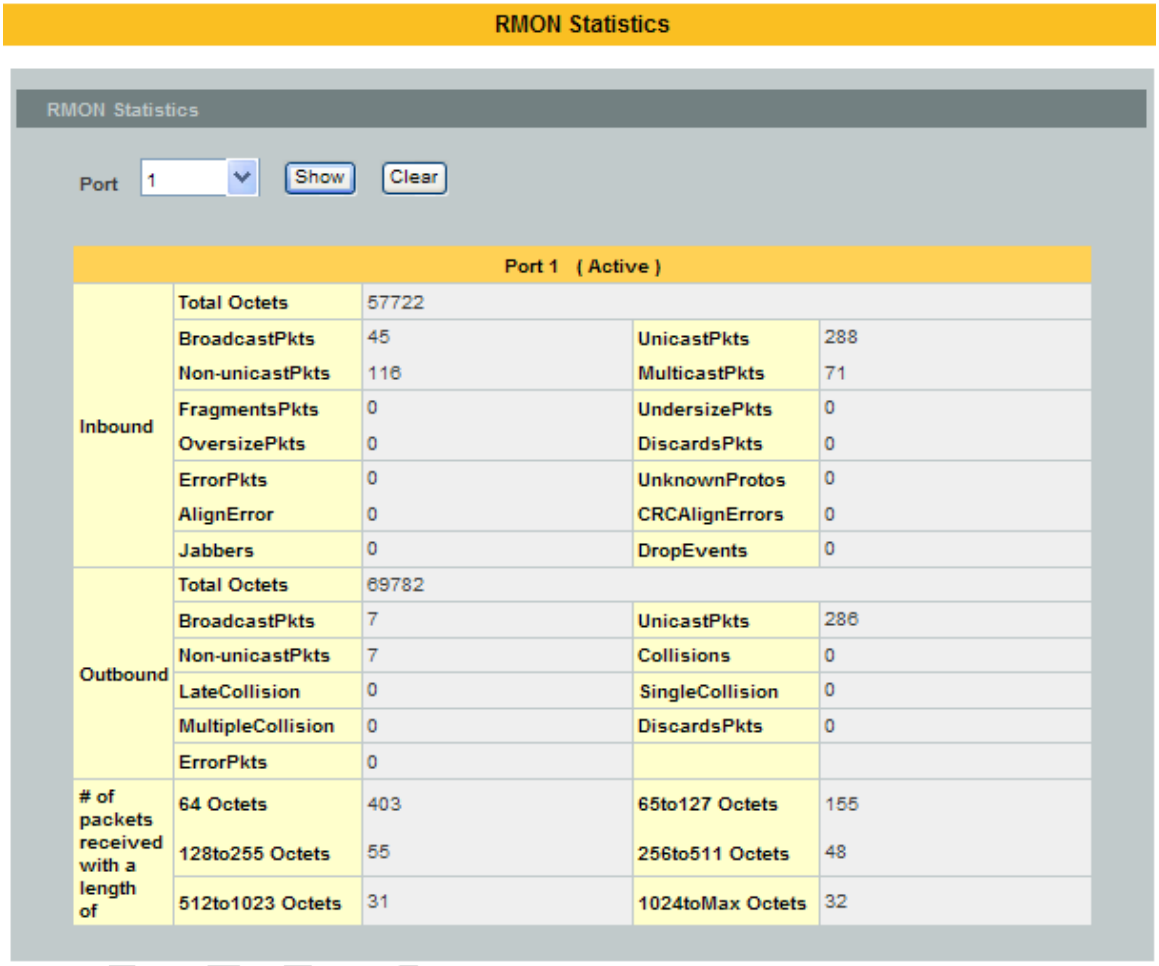
This feature helps users to monitor or clear the port's RMON statistics.

8.4.2. 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.

8.4.3. Web Configuration



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.

8.5. SFP Information

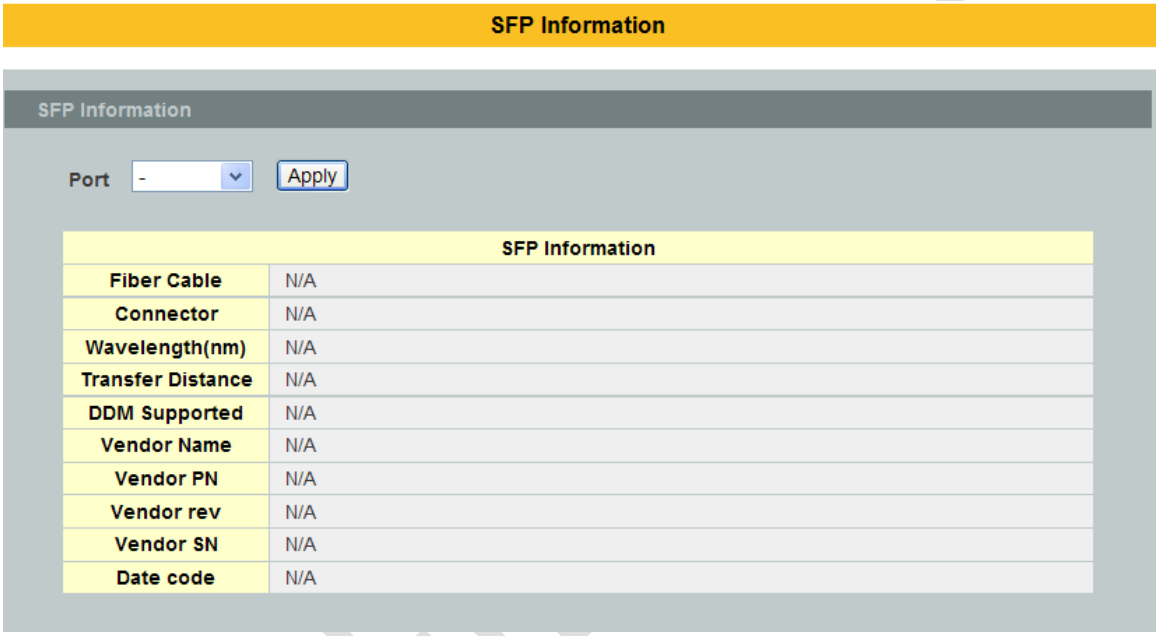
8.5.1. Introduction

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 function.

8.5.2. 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.

8.5.3. Web Configuration



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.

8.6. Traffic Monitor

8.6.1. Introduction

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

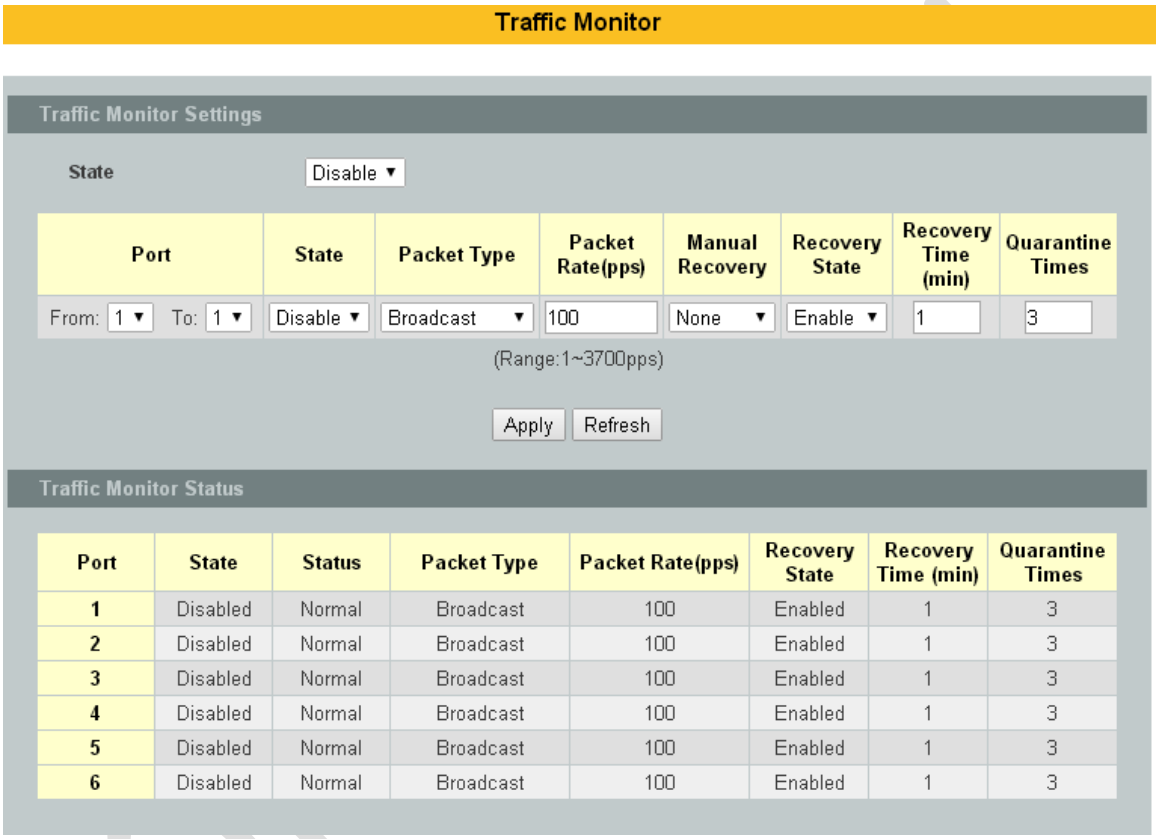
Port	State	Status	Packet Type	Packet Rate(pps)	Recovery State	Recovery Time(min)
1	Disabled	Normal	Bcast	1000	Enabled	1
2	Disabled	Normal	Bcast	1000	Enabled	1
3	Disabled	Normal	Bcast	1000	Enabled	1
4	Disabled	Normal	Bcast	1000	Enabled	1
5	Disabled	Normal	Bcast	1000	Enabled	1
6	Disabled	Normal	Bcast	1000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

8.6.2. 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 (disable|enable)	This command enables / disables the traffic monitor on the port.
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 port. bcast – Broadcast packet. mcast – Multicast packet.
interface	traffic-monitor recovery (disable|enable)	This command enables / disables the recovery function for the traffic monitor on the port.
interface	traffic-monitor recovery time <1-60>	This command configures the recovery time for the traffic monitor on the port.
configure	interface range gigabitethernet1/0/ PORTLISTS	This command enters the interface configure node.
if-range	traffic-monitor (disable|enable)	This command enables / disables the traffic monitor on the port.
if-range	traffic-monitor rate RATE_LIMIT type (bcast|mcast|bcast+m	This command configures the packet rate and packet type for the traffic monitor on the port. bcast – Broadcast packet.

	cast)	mcast – Multicast packet.
if-range	traffic-monitor recovery (disable|enable)	This command enables / disables the recovery function for the traffic monitor on the port.
if-range	traffic-monitor recovery time <1-60>	This command configures the recovery time for the traffic monitor on the port.

8.6.3. Web Configuration



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)

9. Management

9.1. SNMP

9.1.1. SNMP

9.1.1.1. Introduction

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.

9.1.1.2. CLI Configuration

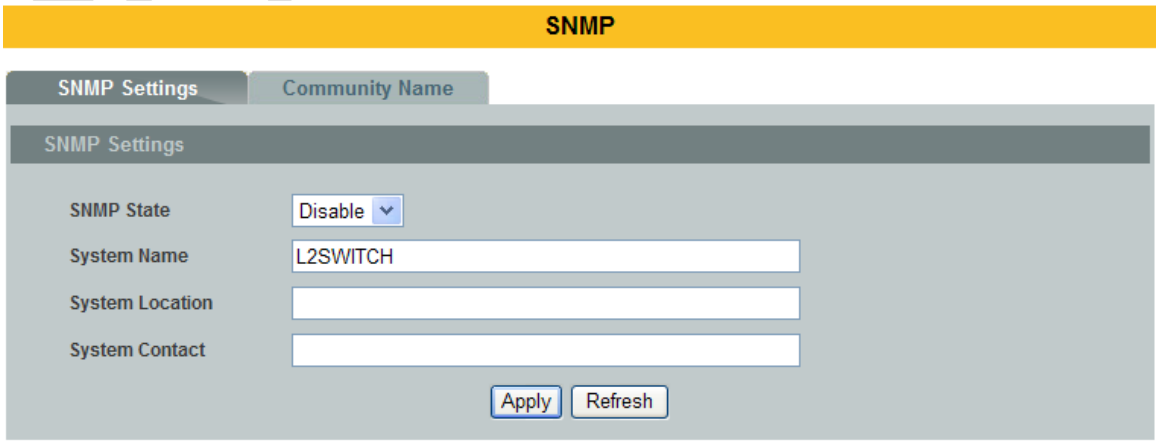
Node	Command	Description
enable	show snmp	This command displays the SNMP configurations.
configure	snmp community STRING (ro|rw) trusted-host IPADDR	This command configures the SNMP community name.
configure	snmp (disable|enable)	This command disables/enables the SNMP on the switch.
configure	snmp system-contact 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 Branch-Office
```

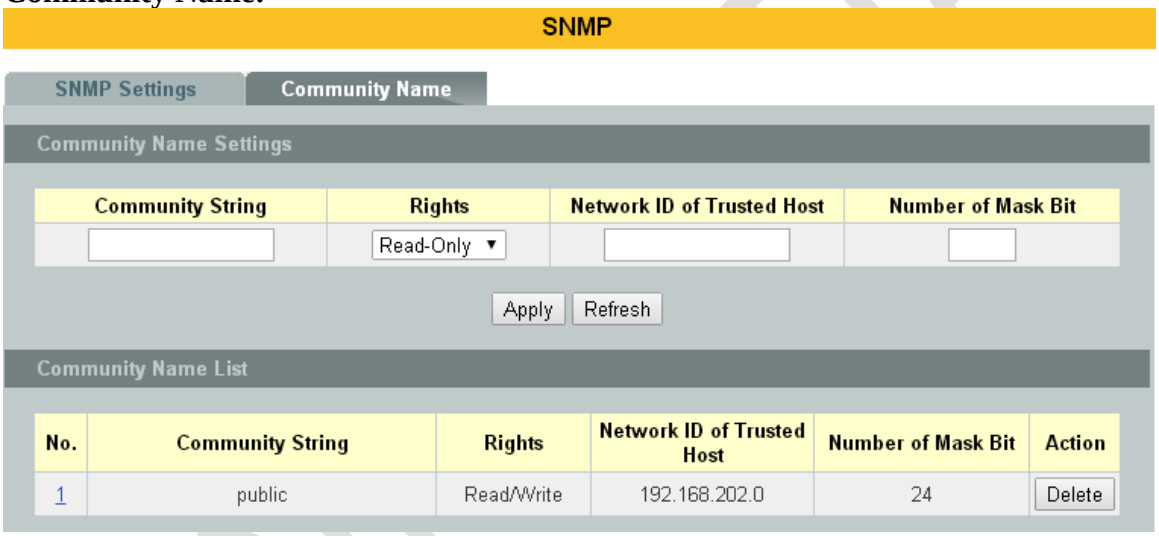
9.1.1.3. Web Configuration

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 button to reset the fields to the last setting.

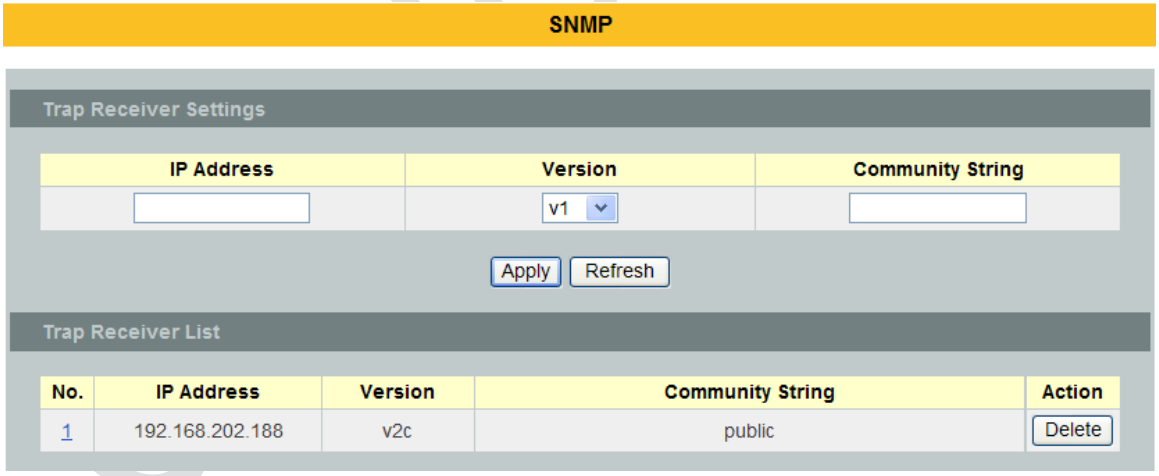
Community Name:



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.

Number of Mask Bit	The bit count of the subnet mask for the IP address of the remote SNMP management station.
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.
Number of Mask Bit	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.

9.1.2. SNMP Trap Receiver



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.

9.2. Auto Provision

9.2.1. Introduction

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: DIS-200G-06WPT***_Autoprovision.txt***

The contents of the file are listed below:

```
AUTO_PROVISION_VER=1
Firmware_Upgrade_State=1
Firmware_Version= DIS-200G-06WPT-100-1.1.0.S0
Firmware_Image_File= DIS-200G-06WPT-100-1.1.0.S0.fw
Firmware_Reboot=1
Global_Configuration_State=0
Global_Configuration_File= DIS-200G-06WPT-100-1.1.0.S0.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 "INS-8648P***_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:

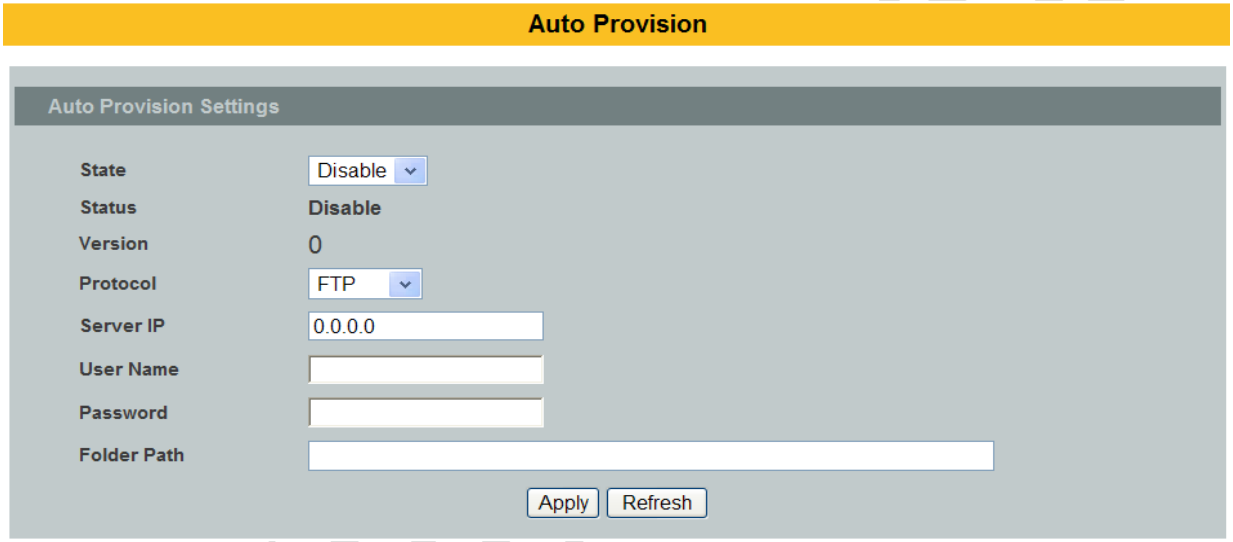
Active	: Disable
Version	: 0
Protocol	: FTP
FTP user/pwd	: /
Folder	:
Server address	:

9.2.2. CLI Configuration

Node	Command	Description
enable	show auto-provision	This command displays the current auto provision configurations.
configure	auto-provision	This command enters the auto-provision node.
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	no folder	The command configurations the folder to default.
auto-provision	no FTP-user	The command configurations the username and password to default.

9.2.3. Web Configuration



9.3. Mail Alarm

9.3.1. Introduction

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

- System Reboot : The system warn 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.

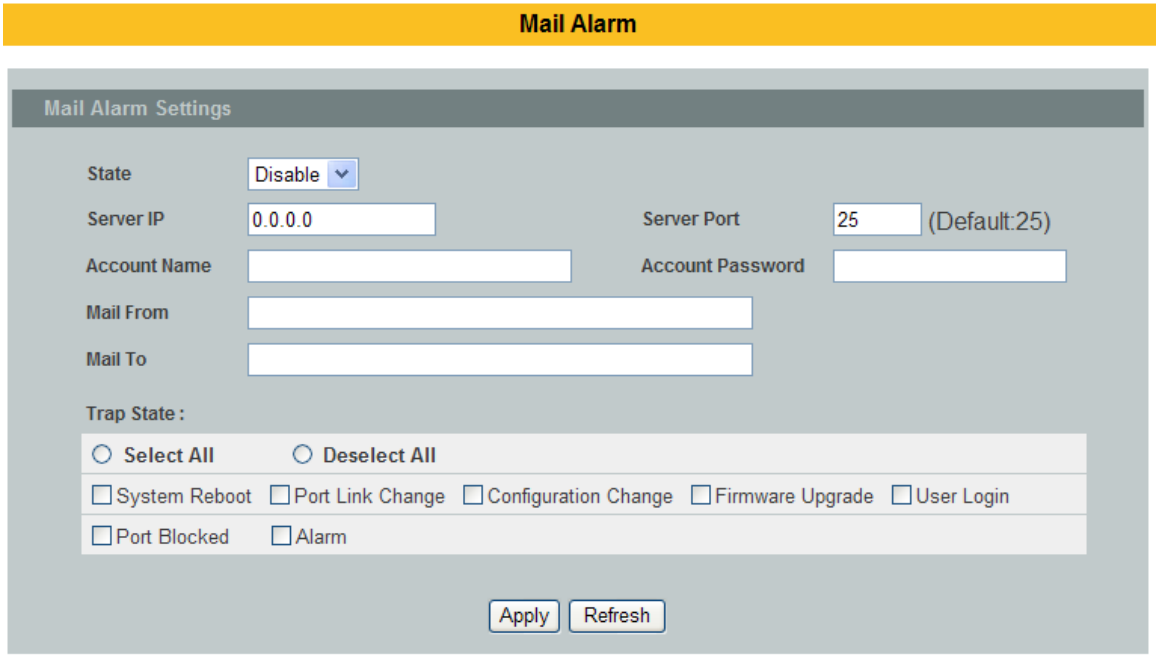
9.3.2. Reference

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	Server:	Authentication:	Port:
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	Server:	Authentication:	Port:
SMTP Server (Outgoing Messages)	smtp.live.com	StartTLS	587
POP3 Server (Incoming Messages)	pop3.live.com	SSL	995
Yahoo Mail	Server:	Authentication:	Port:
SMTP Server (Outgoing Messages)	smtp.mail.yahoo.com	SSL	465
POP3 Server (Incoming Messages)	pop.mail.yahoo.com	SSL	995
Yahoo Mail Plus	Server:	Authentication:	Port:
SMTP Server (Outgoing Messages)	plus.smtp.mail.yahoo.com	SSL	465
POP3 Server (Incoming Messages)	plus.pop.mail.yahoo.com	SSL	995

9.3.3. 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 IPADDR server-port VALUE	This command configures the mail server IP 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.

9.3.4. Web Configuration



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.

9.4. Maintenance

9.4.1. Configuration

9.4.1.1. 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:

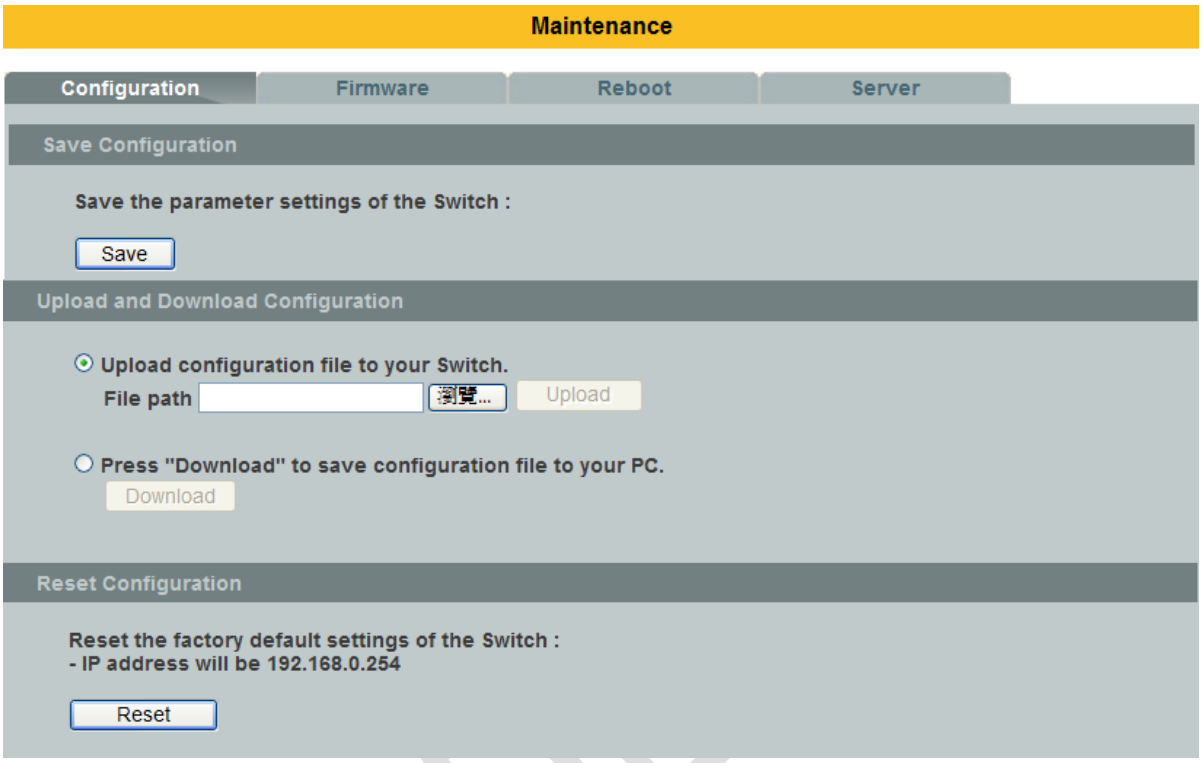
L2SWITCH#*configure terminal*
L2SWITCH(config)#*interface eth0*
L2SWITCH(config-if)#*ip address 172.20.1.101/24*
L2SWITCH(config-if)#*ip address default-gateway 172.20.1.1*
L2SWITCH(config-if)#*management vlan 1*

Enable the DHCP client function for the switch.

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

9.4.1.2. Web Configuration

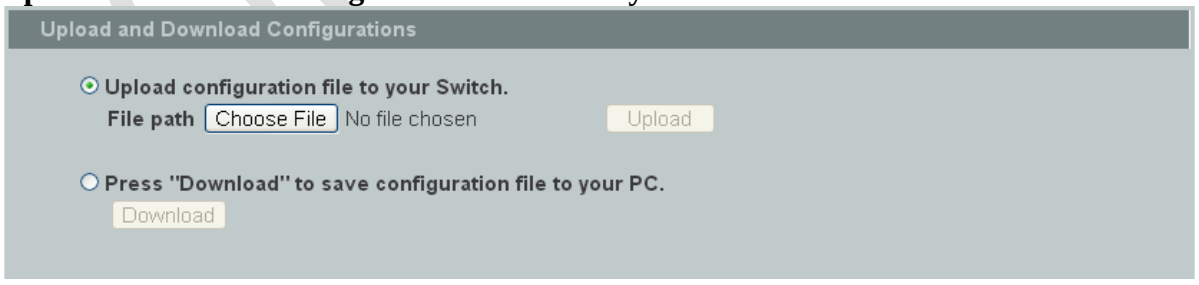
Configuration



Save Configurations

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

Upload / Download Configurations to /from a your server



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

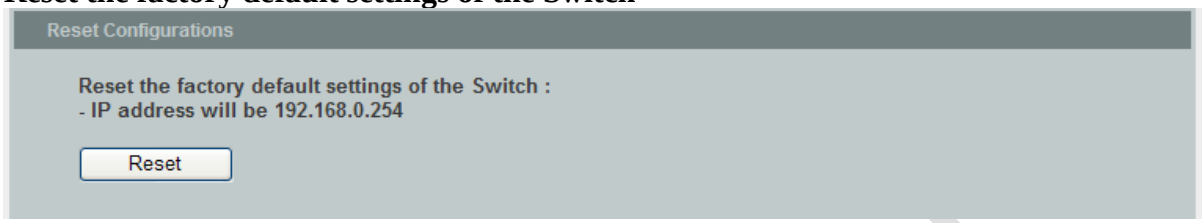
- Select the “Press “Download” to save configurations file to your PC”.
- Click the “Download” button to start the process.

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.

The configuration status

Display the configuration status of recorded in the NV-RAM.

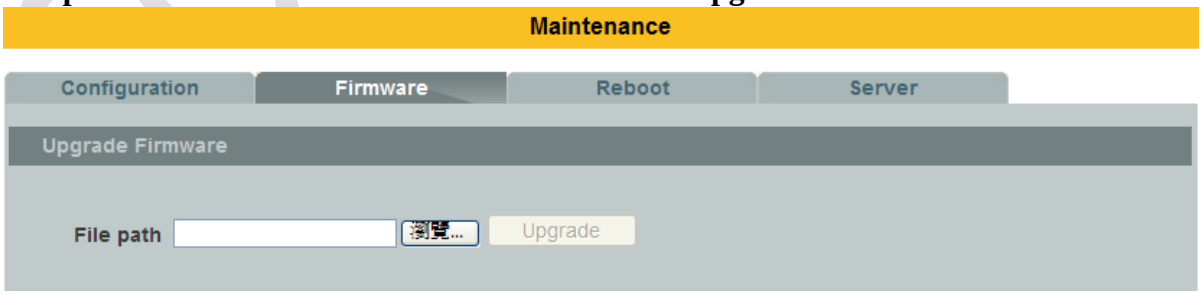
Notice:
If the user has changed any configurations, the message display “The configurations have been modified!”; otherwise, The message “The configurations are default values.”

There are two conditions will change message from “The configurations have been modified!” to “The configurations are default values.”:

1. Click “Reset configuration” in web management or do cli command, reload default-config.
2. Click “Upload configuration” in web management or do cli command, “archive download-config xxx”.

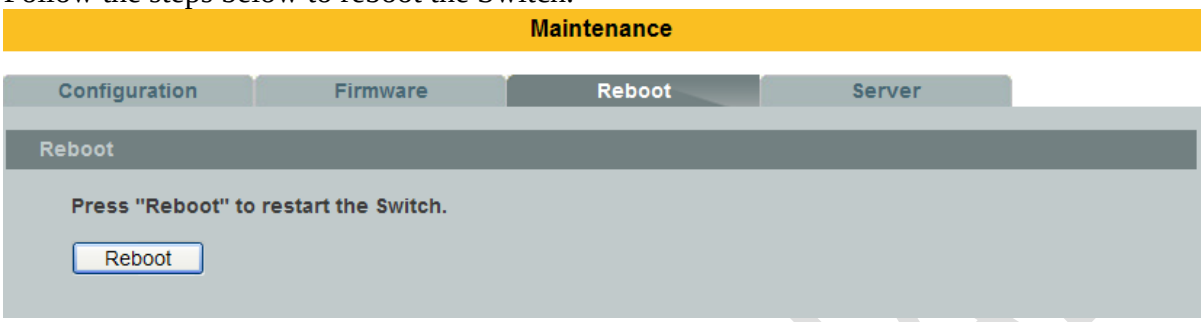
9.4.2. Firmware

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.

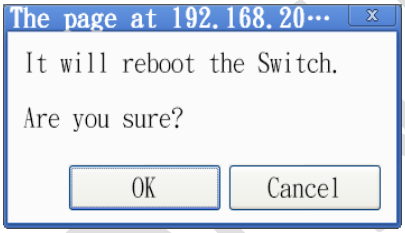


9.4.3. Reboot

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.

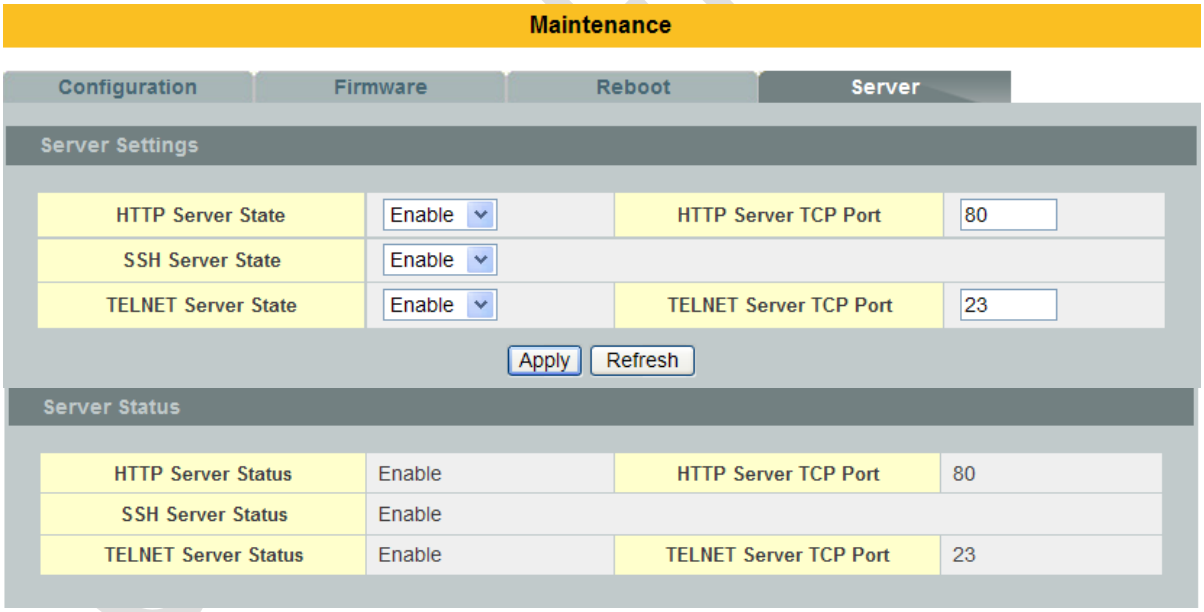
9.4.4. Server Control

The function allows users to enable or disable the SSH or Telnet or Web service individual using the CLI or GUI.

9.4.4.1. CLI Configuration

Node	Command	Description
enable	show server status	This command displays the current server status.
configure	http server	This command enables the http on the Switch.
configure	http server port VALUE	This command configures the TCP port for the HTTP server.
configure	no http server	This command disables the http on the Switch.
configure	ssh server	This command enables the ssh on the Switch.
configure	no ssh server	This command disables the ssh on the Switch.
configure	telnet server	This command enables the telnet on the Switch.
configure	no telnet server	This command disables the telnet on the Switch.
configure	telnet server port VALUE	This command configures the TCP port for the TELNET server.

9.4.4.2. Web Configuration



Parameter	Description
Server Settings	
HTTP Server State	Selects Enable or Disable to enable or disable the HTTP service.
HTTP Server TCP Port	Configures the TCP port for the HTTP service.
SSH Server State	Selects Enable or Disable to enable or disable the SSH service.

Telnet Server State	Selects Enable or Disable to enable or disable the Telnet service.
TELNET Server TCP Port	Configures the TCP port for the Telnet service.
Apply	Click Apply to configure the settings.
Refresh	Click this button to reset the fields to the last setting.
Server Status	
HTTP Server Status	Displays the current HTTP service status.
HTTP Server TCP Port	Displays the current TCP port of the HTTP server.
SSH Server Status	Displays the current SSH service status.
Telnet Server Status	Displays the current Telnet service status.
TELNET Server TCP Port	Displays the current TCP port of the TELNET server.

9.5. System log

9.5.1. Introduction

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.

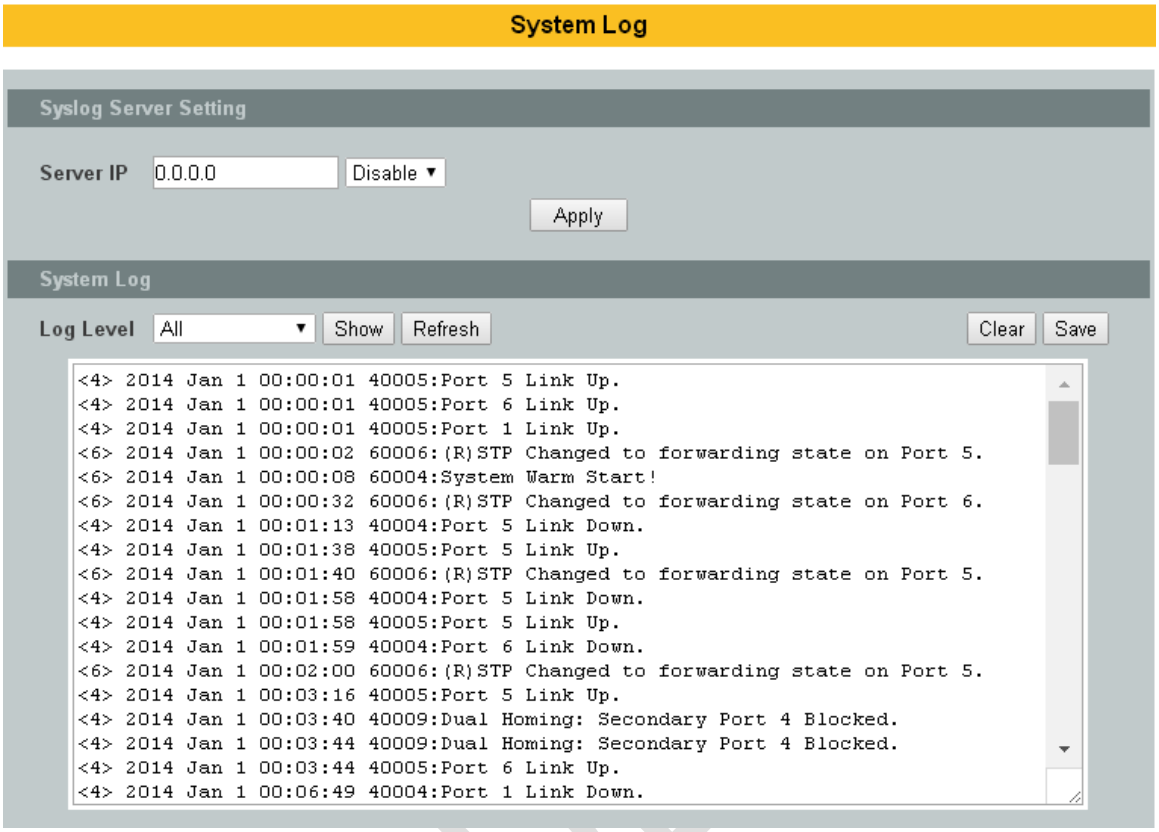
9.5.2. CLI Configuration

Node	Command	Description
enable	show syslog	The command displays all of log message recorded in the Switch.
enable	show syslog level <1-6>	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-server (disable|enable)	The command disables / enables the syslog function.
configure	syslog-server 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
```

9.5.3. Web Configuration



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.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Log Level	Select **Alert/Critical/Error/Warning/Notice/Information** to choose which log message to want see.
Clear	Click Clear to clear all of log message.
Save	Click Save to save all of log message into NV-RAM.

9.6. User Account

9.6.1. Introduction

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.

9.6.2. 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.

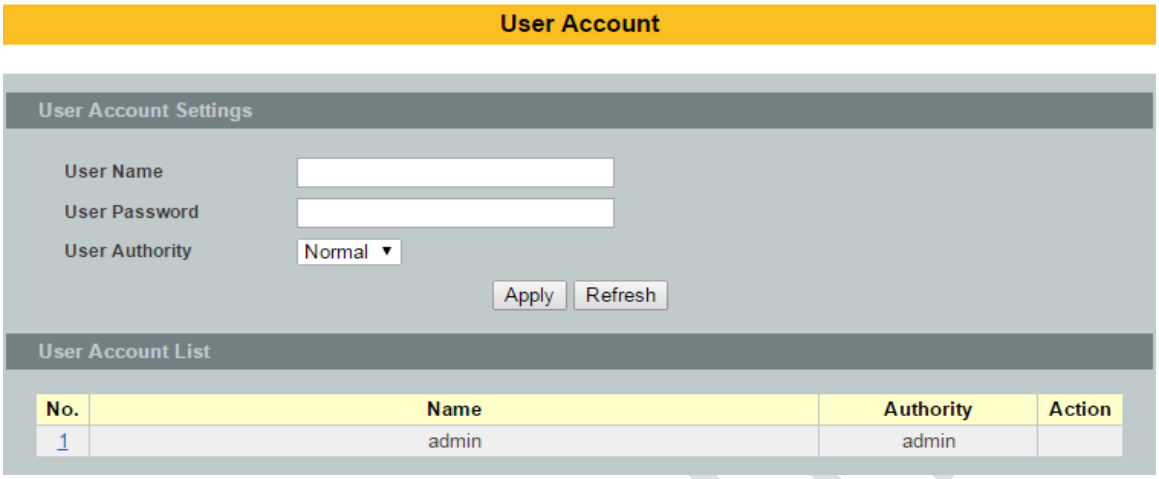
The procedures to configure a user account.

✓ To enter the configure node.
L2SWITCH#configure terminal
L2SWITCH(config)#

✓ To configure a user account.
L2SWITCH(config)#add user w w admin

✓ To remove a management host.
L2SWITCH(config-if)#no management host 192.168.200.106

9.6.3. Web Configuration



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 INS-8624P or any other Volktek product, please 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	*support@volktek.com.tw*
Website	www.volktek.com

ISO 9001 Certified